Introduction to internet of things

Prof. Sudip Misra

DEPARTMENT OF COMPUTER SCIENCE
AND ENGINEERING
IIT KHARAGPUR

INDEX

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 01
Introduction to IoT-Part – 1

So, the first lecture is going to be on the Basics of Internet of Things. So, in this lecture we are going to get introduced to the different fundamental concepts behind IoT and the basic technologies connectivity devices that are required and an overall understanding about how IoT's are made. So, we are going to have in this lecture an understanding about all of these concepts, but first let us get motivated about why IoT is required.

So, it has been anticipated that very soon all the different things that are going that we are seeing around us and that we have around us are all going to be internet worked. They are all going to be interconnected. So, at present what we enjoy as services, as internet based services is basically a connection of different computers and computing devices. So, basically this capital I internet that all of us use is basically a global network or an internet work of different computers and computing devices.

Now, what internet of things says is that the scope of this internet is going to be expanded. So, it is going to be expanded beyond computing and computer devices being connected. It is going to interconnect different things that physical objects that we see around us, the different objects such as the lighting system in a room, the lights, the fans, the air conditioners and anything and everything including things such as the toothbrush, the microwave oven, the refrigerator and so on so forth and not only in our homes, but also in our businesses such as internet working different machines, internet working different equipments and so on. So, each and everything that we see around us that we use at our home in businesses, in workplaces, everything being internet worked. So, this is the whole vision of internet work of things, internet of things.

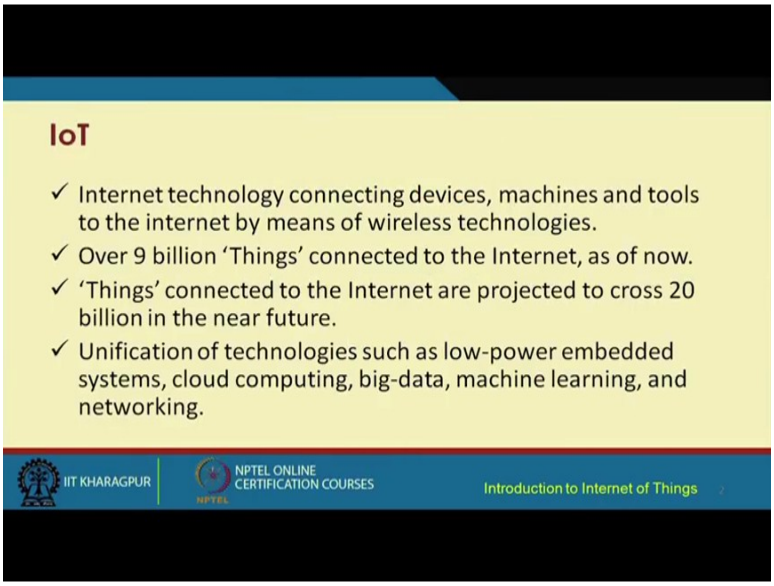
Now, there are several challenges that are going to arise if we want to do it, but before that let us also discuss about why it is going to be required, why internet of things has become so popular, why it is going to be required? The reason is that IoT is envisaged to be able to provide advanced level of service to the society to the business and so on. So, advanced levels of services can be offered with the help of IoT based technology.

So, what is going to happen is, these different things, the chairs, the tables, these lighting system, you know the watch or anything and everything that you can think of, all of these are going to be fitted with embedded systems, embedded electronics and information technology, so that they have some basic computing platform in them, attached to them and then, they are going to be acting as different nodes of that particular internet, the IoT internet of things, right.

So, what is going to happen is these systems, these things are going to be all equipped with embedded systems and these embedded systems along with embedded electronics, embedded processor, embedded communication systems and so on. So, they are going to help in connecting different other things that are around them and depending on the application requirements, depending on the specific goals of the business and then, a big internet is going to be formed which is much bigger than the current internet of computers and that is the internet work internet of things IoT.

Now, IoT is one of the building blocks that is considered to be of use for developing smart homes and smart cities. So, at present not only in our country, but throughout the world there is a lot of interest on developing smart cities and smart homes. So, IoT is one of the enabling technologies to make the city smart, to mix make the home smart. So, how it is going to be done, that is going to be more evident as we proceed through the different lectures and the different intricacies that are going to be there in building this complex internet of things is going to be evident through different lectures that we are going to go through in this particular course.

(Refer Slide Time: 05:48)



So, going forward Internet Technology that we have as I have already said it is going to expand beyond the connection of simple computers. So, we are going to connect or internet work different machines, different tools typically, but not necessarily using wireless technologies, such as Wi-Fi cellular technologies, Bluetooth Zigbee and different other wireless technologies that are available to us.

Now, in order to be able to do it, what is going to happen is because the number of things is very large, much larger than the number of computers that are available, so it is going to increase the number of nodes in this particular network. So, IoT in other words is going to have large number of nodes, the IoT internetwork is going to have large number of nodes and each node corresponding to the different distinct objects or different things that exist in the physical world.

So, the things basically are going to explode the number of connected things, are going to explode in time with time. So, the things that are connected to the internet are going to be projected to cross the 20 billion figure in the near future. This is what has been predicted. So, a large number of things, billions and in fact, billions and trillions of things are going to be connected to the internetwork of things.

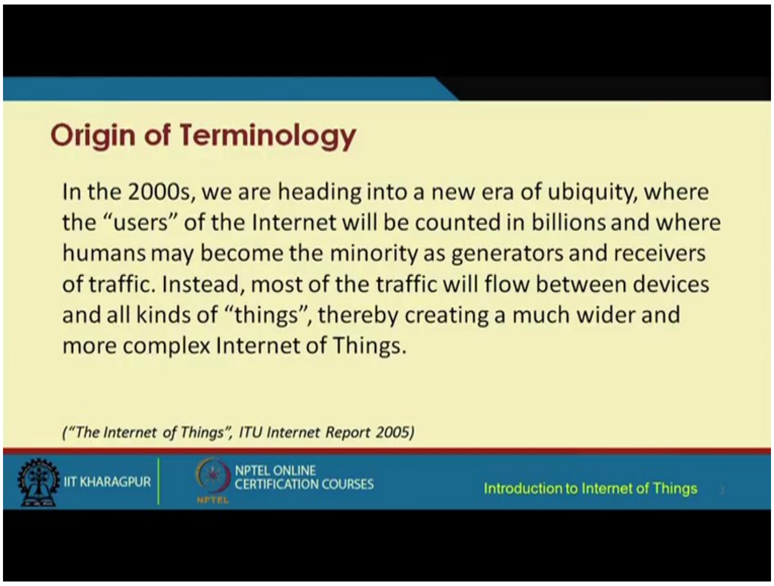
So, at this point I should also mention one more thing that this internetwork of things can be construed to be built in two different ways. One way is to expand the scope of the current internet. That means, the internet of computers this is one way, so you expand.

So, essentially what is going to happened using this particular approach is all these different things are going to be connected to the existing internet.

So, this internet is going to be expanded further. It is going to become much bigger than what it is at present with only the computers connected. This is the first approach. The other approach is to build a separate internetwork of these physical objects from scratch. So, one is basically expanding the existing internet and the other one is a separate internetwork which is going to be built from scratch. So, irrespective of which one we adopt, each of these approaches has its own separate challenges that have to overcome.

So, going back we have the unification of different technologies that becomes very much mandatory we have. So, internetwork of things is not a single technology. Physical devices can be of different types of physical devices having different configurations, different specifications and so on. Each of these supported through different other systems such as cloud technology, big data machine, learning networking computer vision, you name it and all these different technologies from electrical sciences and some from even mechanical sciences are required in order to build IoT.

(Refer Slide Time: 09:40)

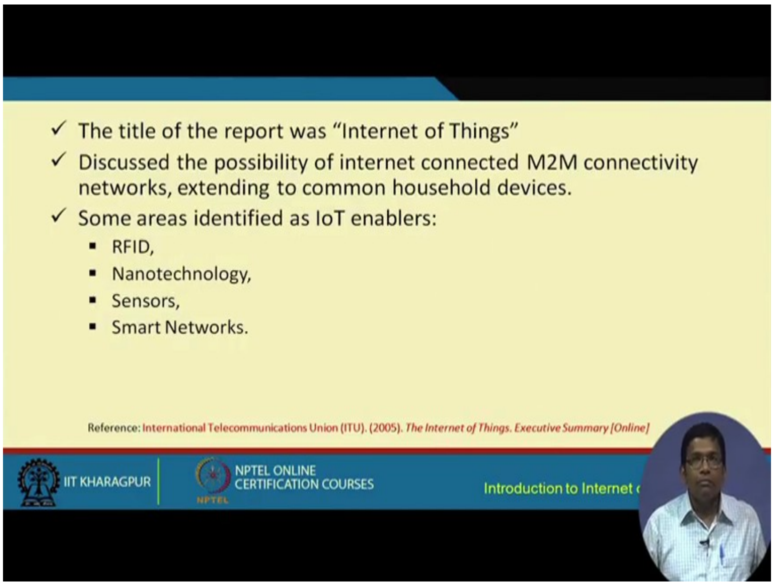


So, talking about the origin of IoT. So, in the 2000, what we are going to witness is a new era of ubiquity. So, in this era of ubiquity, what is going to happen is not only that we are going to have anywhere, any place, that means any place any time connectivity or services relating to connectivity. That means, internet or network connectivity of different types, but also the service of connecting anything. So, anytime anyplace anything, connectivity is what is going to be observed in this new era of ubiquity. So, that is going to result in billions and trillions of things. Humans, everybody being connected and consequently what is going to happen is the number of humans that are on the earth that is going to this number, this figure is going to be outnumbered very soon with the number of things that are connected to the internetwork of things internet of things and consequently what is going to happen is, all these different devices, all these different things, they are going to send lot of data.

This data has to be handled properly, this data have to be analyzed and this is what we are going to cover in one of the next lectures. So, what is going to happen is this internetwork, the new internetwork that we are talking about, the internet of things is going to be very complex network with much wider scope than the current internet and with many more complexities and this is currently the vision of internet of things and all these lectures that we are going to go through in this particular course. All the other lectures that we are going to go through, they are going to cover the different challenges and how there are different tools that are available in order to, what are the different tools that are available in order to address these different challenges.

So, we are going to go and we are going to get introduced to all these different challenges and the different tools that are available in this particular course. We are going to mostly understand the different concepts that are behind them and typically because it is an introductory course, we are not going to go through each of these different technologies that are available to us in too much of detail, but at a level that will help us to understand the basic concepts for that are required for designing internet of things. So, there are different enabling technologies for internet of things.

(Refer Slide Time: 12:39)

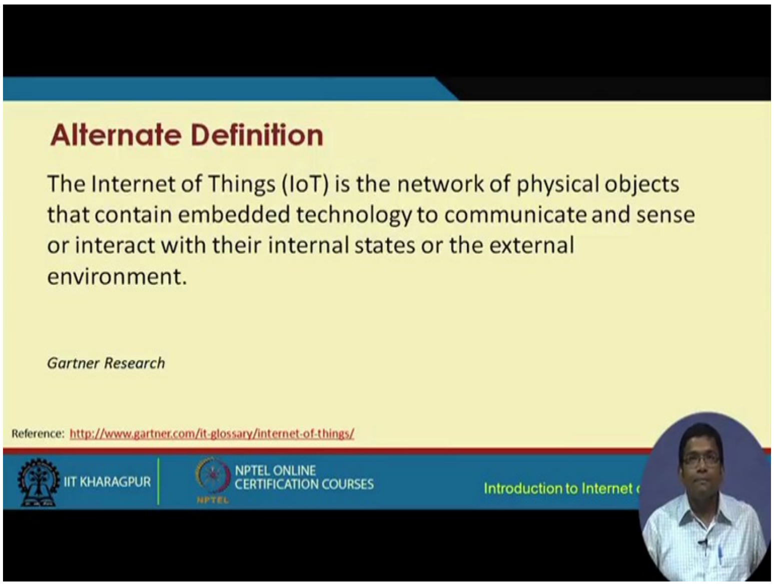


RFID is one we know at present in the market places and different places in the society you know and wherever we go, we see that RFID technology being used RFID tags, RFID readers are being used. So, RFID based devices are required for building internet of things.

Sensors is another one which is according to me one of the most important enabling device or enabling technology for building internet of things. Sensors and actuators are what we are going to cover in one of the next lectures very shortly and the other things are different networking devices, different connectivities, different communication paradigms and so on. So, these are also required in order to connect these different sensors, RFIDs and different other physical devices that have to be internetwork to form the IoT. Finally, I would like to mention that at present there is lot of interest in the nanotechnology domain. So, people are talking about building internet of nano things, internet of nano sensors and so on.

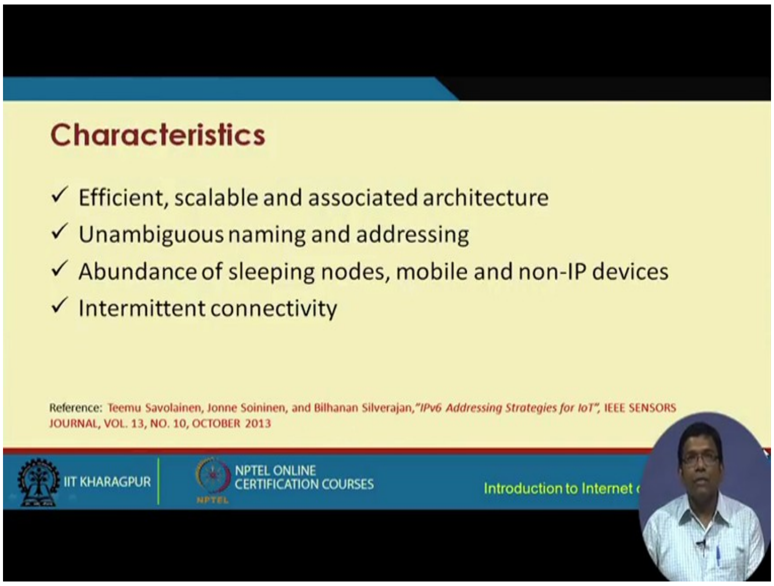
So, you know what is going to happen is there are going to be very small sized nano size nano in the order of nano sized devices that are going to be used for different purposes. For example, there could be these nano capsules which can be consumed and finally, which are going to be excreted after you know after they have performed their functions. So, these nano devices are going to be used, they are going to be swallowed and consumed and then you know once that is done in the form of capsules, they are going to be internetwork. These different nano devices, these nano capsules are going to talk to each other. So, these nano devices, nano communication devices are being conceptualized. At present people are thinking about building these nano devices that can be used to form the internet of nano things. So, once we have this internet of nano things, the horizon of internet of things is going to be expanded much further.

(Refer Slide Time: 15:22)



So, we already have seen that when we are talking about IoT, it is mostly about networking of physical objects and these physical objects are embedded with you know the different embedded electronics that communicate and sense and interact with the internal states or with the external environment in which they are operating. So, either they are interacting with each other, they change their different states or they are interacting with the inter external environment in which they are operating.

(Refer Slide Time: 15:57)



There are different characteristics, there are different characteristics of IoT. So, first of all this IoT that we develop that has to be efficient. It has to serve efficiently the requirements of the applications for which they are deployed. They have to be scalable because we have already seen that in IoT systems, we are talking about large number of things, we are talking about not simply millions of things, but in several billions and trillions, we are talking about the scalability is very important, consideration is very important issue that has to be addressed.

So, even if the number of sensors and the sensing devices IoT devices are going to increase, the overall network performance should not be compromised. So, you know this is challenge in terms of the network. So, from a networking perspective, it is a challenge that has to be worked on. There has to be unambiguous meaning and addressing architecture. So, this is very important. So, all these different devices already we have witnessed that addressing in the IPV4 context in the regular existing internet context is a big issue.

So, we are talking about naming and addressing different mechanisms of naming and addressing with the help of IP technology, DNS etcetera etcetera. We already have seen that these can be used in order to you know address these problems of addressing and naming in the context of the present internet and now, when we are expending this internet in this large scale. So, what is going to happen is, we are going to run into a bigger problem with naming and addressing.

So, we need a new mechanism for naming and addressing of the different nodes, these physical nodes, the physical objects that are fitted with embedded systems. So, another thing is that in terms of the resource requirements, each of these nodes are typically very low power. They have very low resources and they have to be you know whenever they are not required, they have to be put to the sleeping mode, they have to go through a sleep cycle.

So, that means whenever they are not being used, they are not being active. They have to be put in a sleep state and whenever it is required, they have to be made active. These devices can be mobile, they can move. For example, a smartwatch you know whoever is wearing the smartwatch, when they move, this node also moves, the smartwatch also moves. So, mobility like this becomes a very important problem in the context of IoT networks. Mobility of the devices and the mobility of the sub networks also is possible.

So, part of the network becomes mobile and in extreme cases even larger network can also become mobile. So, IP based addressing may not be always very suitable in this sort of scenario. So, what are the different alternatives? There are different people, different researchers globally who are working on how IoT technology, how naming can be a different form of, naming can be designed in order to support this IoT technology and intermittent connectivity is another characteristic that is typical of IoT. These devices, they move, they get the network and the subnetworks get partitioned. One device which is in connectivity with another device at a later instant of time may not be connected.

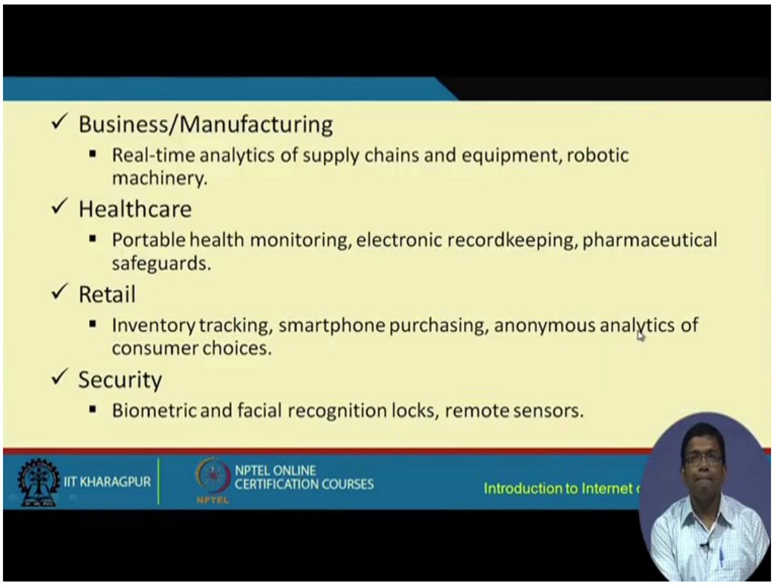
So, this is another problem that has to be taken care of. So, for example there is this opportunistic mobile networks which is a topic which can help in addressing this particular problem, this technology. The Waymond technology can help in addressing this particular problem. So, opportunistic mobile networks are useful in order to address the problems of intermittent connectivity between the different nodes in the network.

(Refer Slide Time: 20:30)

In terms of application domains, there are you know IoT is attractive in different applications, spheres application, domains spheres. For instance, manufacturing and business, healthcare, retail, security and so on. So, among all of these, it is estimated that most of the market share with IoT goes with the manufacturing at an business sector, so 40.2 percent approximately.

Next is the healthcare and third is the retail sector and fourth is the security, surveillance, safety surveillance and so on with the help of IoT based systems.

(Refer Slide Time: 21:21)



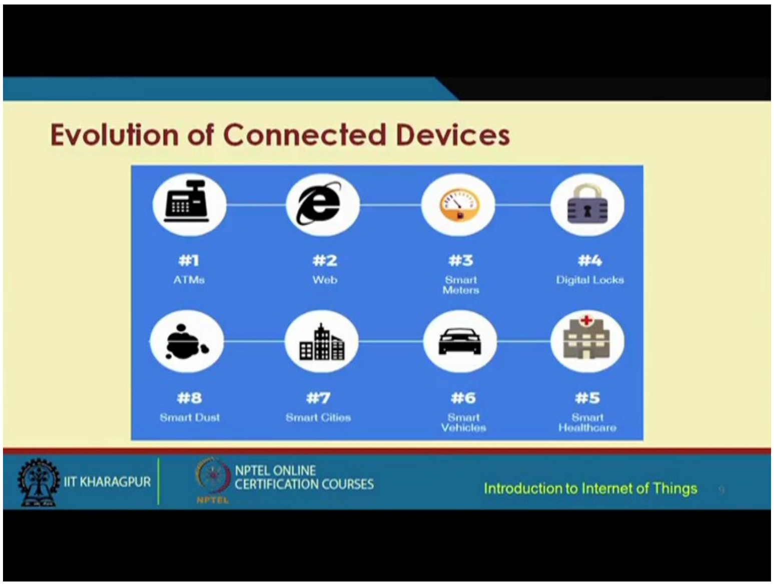
So, when we talk about business and manufacturing, we are talking about how to improve the overall supply chain, what are the different equipments that have to be introduced and different sensors and actuators can be fitted to them, the different robotic machinery can be used in order to improve the business processes.

Second is the healthcare. We are talking about portable healthcare monitoring telemedicine in a much more bigger way. That means, much remote areas can also be connected the different healthcare facilities, hospitals, nursing homes, doctors, nurses. Irrespective of where they are, they can still monitor the healthcare condition, the health condition of the patients that they are treating.

So, portable health monitoring electronic recordkeeping is another. So, automatically because you know in medical domain record keeping is a very important concern. So, electronic record keeping automatically things are the records, medical records are going to be archived. They are going to be stored, they are going to be you know maybe they can be even further analyzed to grow some meaningful conclusions from them and so on and different pharmaceutical set safeguards can had in using the IoT technology.

In the case of retail sector as well tasks, such as inventory tracking, smartphone purchasing, anonymous analytics of consumer choices, these are the different things that can be done efficiently through the use of IoT technology. Security is another biometric and facial recognition looks, then the remote sensors and so on. You know fingerprinting based or face recognition based or different eye rays recognition based you know, so these technologies can be connected and used with the help of IoT and you know this sort of security mechanisms can be developed.

(Refer Slide Time: 23:36)



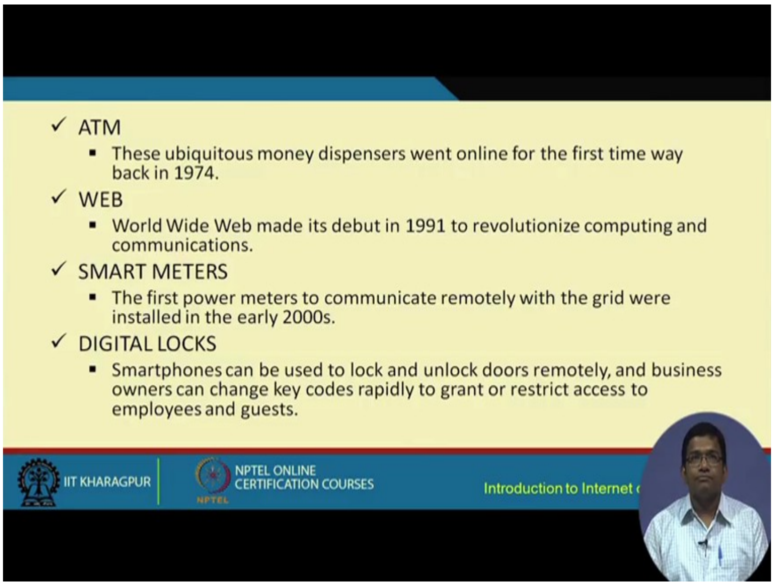
Now, when we talk about this interconnectivity of different devices, we see that this interconnection or connectivity between the different devices has evolved over the years. First it started with these individual cash machines or the ATMs being internetworked. The web became very popular.

So, you know everybody connects to the internet or the web in order to get access to different information, send emails and so on and so forth. Many different things are performed by different web users. At present smart picker meters then became popular. So, smart meters are used at different homes in a city. These smart meters, they can be programmable and they can record different things.

Even you can program the smart meters at your homes in order to do different things like load balancing, electrical load balancing, efficient use of electricity you know using electricity during non-peak hours, pricing, accordingly in the pricing mechanic choosing different options for service of electricity that is provided by the service provider and so on and then, we have digital locks. Biometric based digital locks are very popular.

We have smart healthcare, smart vehicles, smart cities and smart dusts. So, these are the different technologies that have evolved, these are different connected you know device based technologies that have evolved over the years.

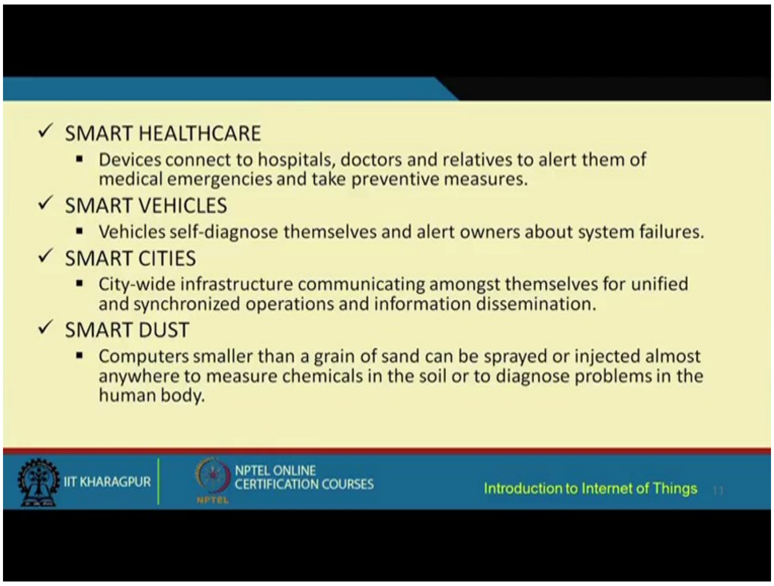
(Refer Slide Time: 25:17)



So, ATM and web are relatively old by now. One comes from 1970s and the other one from 1990s, but smart meters became very popular in the 2000s. Digital locks are very popular at present.

So, smartphones can be used as locks to lock and unlock the doors remotely at your homes or at your businesses and these locked keys and so on. They can be easily changed and one can be granted access to a particular facility. One means in a business, the employees or the different guests, they can be granted access to different facilities through the digital locks much more easily than the conventional locks.

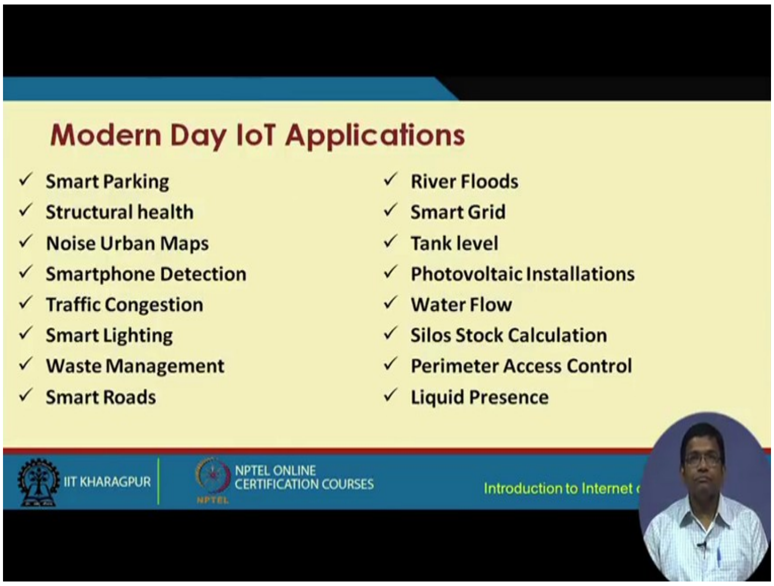
(Refer Slide Time: 26:10)



Smart healthcare connected vehicle, smart vehicles you know these are quite common smart cities as I was telling you is very popular at present not only in India, but throughout the globe. So, in smart city, people are talking about deploying smart different infrastructure. These infrastructure which can communicate with each other, they can be used by different owners and the different operations in a city and different functions of the different offices, etcetera you know.

So, all these things, offices and different other public places, all these things can be monitored and the operations can be improved much more easily and also, the information dissemination because you know all these different devices, they are typically fitted with sensors. So, these sensors are going to throw in lot of data. So, dissemination of this particular data is very important, handling of this particular data is very important. In the context of smart cities, smart dust is another thing where the computers that are smaller than a grain of sand can be spread or injected almost anywhere to measure chemicals in the soil or to diagnose problems in the human body.

(Refer Slide Time: 27:27)

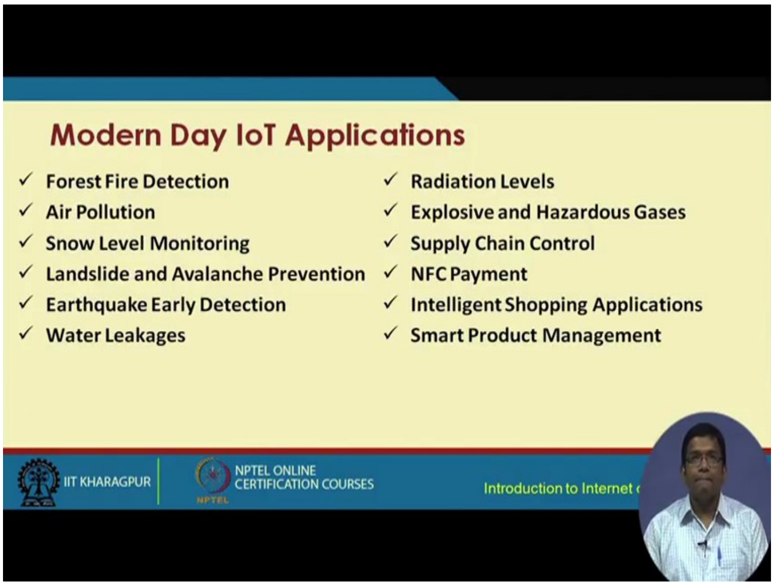


So, in the modern day IoT people are talking about different applications such as smart parking, structural health monitoring noise urban maps; that means, noise maps in a particular city or an urban environment smartphone detection traffic condition, smart lighting systems, waste management, smart roads river flood monitoring, smart grid tank monitoring, water tanks etcetera, tank level monitoring, photovoltaic installations, water flow monitoring, stock calculations, access control presence of different liquids hazardous materials and so on and so forth.

Large number of applications are envisaged. In fact, you know there are many IoT oriented systems have been built already. They have been prototyped. Some have been much more advanced than in that than a simple prototype and these can be used for serving not only these applications that I just mentioned, but also a large number of different other types of applications. For example, healthcare, space applications and so and so forth.

The number is many and you know anywhere that you see there is a problem IoT is quite likely can be used in order to improve the efficiency of the solution to that particular problem.

(Refer Slide Time: 28:59)

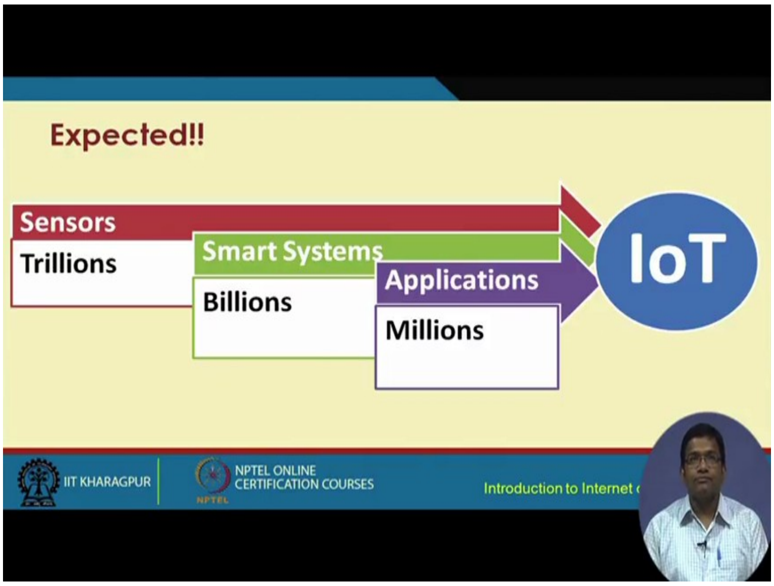


Different other applications such as forest fire detection, air pollution monitoring, snow level monitoring, landslide monitoring and avalanche prevention actually landslide monitoring in our country, there have been different institutions that have already developed systems for landslide monitoring. So, without getting into the details of it, let me proceed further.

So, we have earthquake early detection and monitoring seismic system. Seismic sensors have been developed. They can be connected, they can be internet worked and so on. Water leakage monitoring in a water delivery system, water transmission system in a city, radiation level monitoring, explosive exclusive monitoring and hazardous gas monitoring, supply chain control, NFC payment, intelligent shopping applications and smart product management.

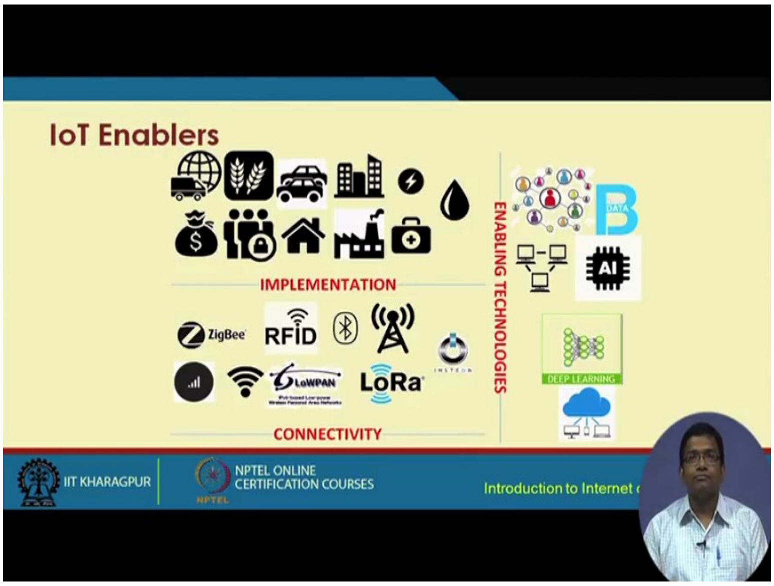
As I was telling you before you can in fact think of IoT applications in almost any sphere of the society, any sphere of life.

(Refer Slide Time: 30:02)



So, what is expected in order to build IoT is to have trillions of sensors, billions of smart systems, millions of applications, all of which are going to be internetwork. They are going to be made synchronously operated in order to form, in order to build IoT.

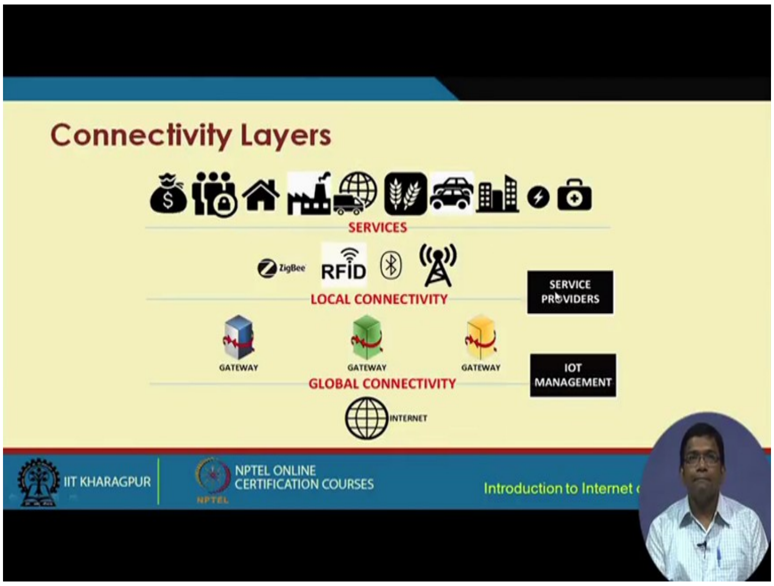
(Refer Slide Time: 30:24)



Different enablers of IoT in terms of, in terms of enabling technologies, we have from implementations perspective different technologies, such as you know smart homes, smart factories, and so on. Different sensors can be fitted and then, we also have different connectivity offering devices such as RFIDs, Zigbee, Wifi, Cellular connectivity, 6 Lowpan, Lora and so on and so forth.

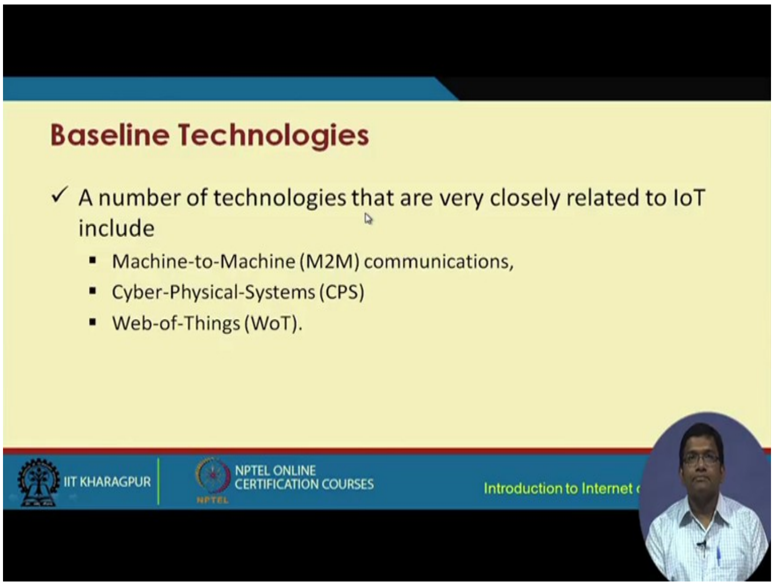
So, different connectivity offering technologies are required and in terms of implementation as I was telling you, factories homes you know banks and transportation sector, agriculture, you know healthcare and so on and so forth, all of these different technologies are required and the other enabling technology is things like big data, deep learning, artificial intelligence, sensor network, regular network, the regular wireless and wired networks. So, all of these are different enablers for buildings IoT.

(Refer Slide Time: 31:43)



In terms of connectivity, typically there are three layers of connectivity service; service layer, local connectivity and global connectivity. For global connectivity we have the internet, for local connectivity we have components such as the gateway and for service level using different communication technologies, such as these you know different services can be offered to different application areas, such as health care agriculture you know businesses, factories, plants, banks and so on.

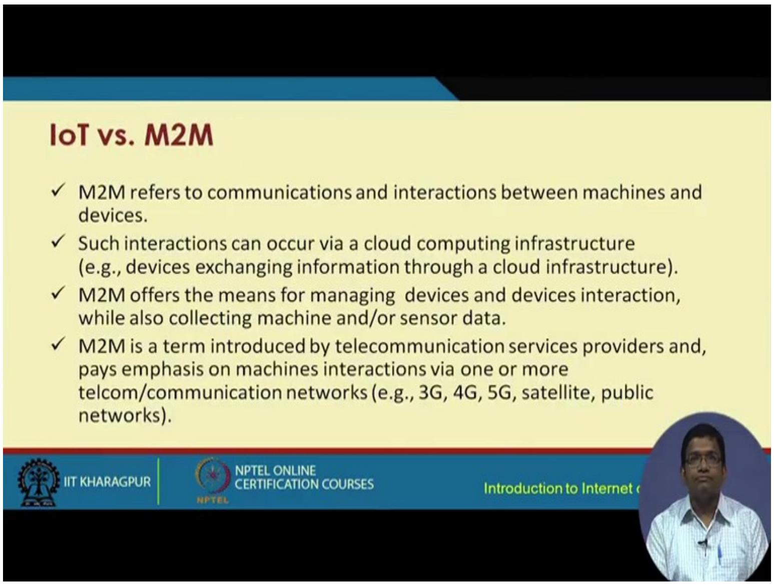
(Refer Slide Time: 32:24)



In terms of the baseline technologies, there are quite a few baseline technologies that can be used. Machine to machine communication is one. In machine to machine communication, one machine directly talks to another machine, communicates with another machine without any human intervention. We have the cyber physical systems where the cyber, the physical systems are basically equipped with computer and connectivity computational and connectivity mechanisms.

So, we have a cyber physical system which works hand in hand. Cyber 1, the cyber component of the system works hand in hand with the physical component of the system. So, we have the cyber physical system, we have web of things which is sort of like the web person of the internet of things.

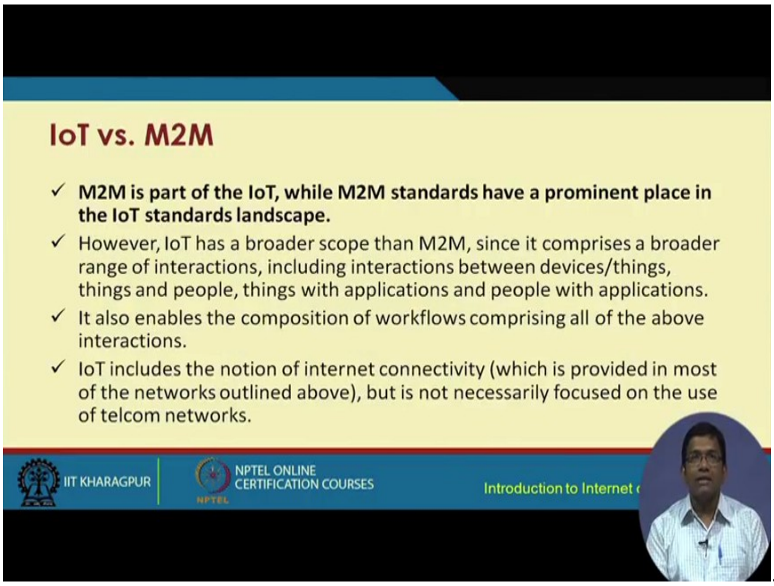
(Refer Slide Time: 33:13)



So, IoT and M2M, these go almost hand in hand, but there is a distinction whereas, M2M is just concerned about communication and interaction between two machines or two devices using technologies such as cloud regular internet and so on.

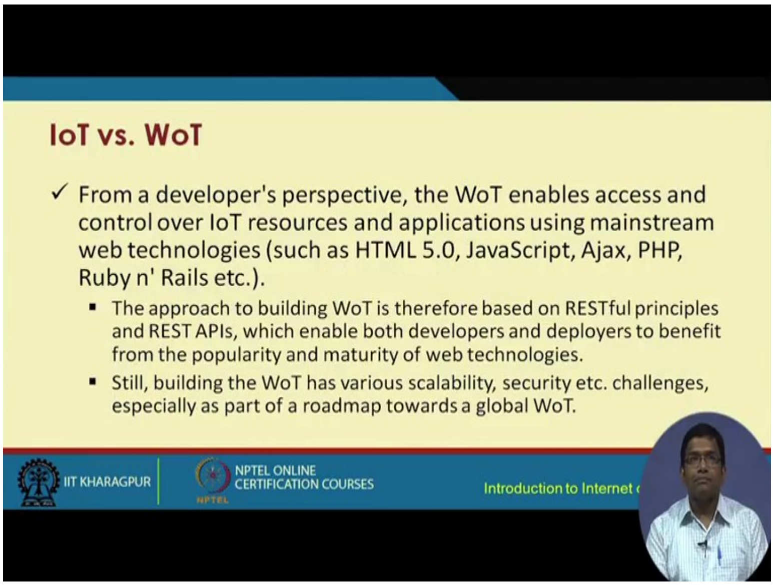
In the case of IoT, IoT the scope is much bigger. So, in IoT we are talking about not only machine to machine communication, but different other things as well.

(Refer Slide Time: 33:48)



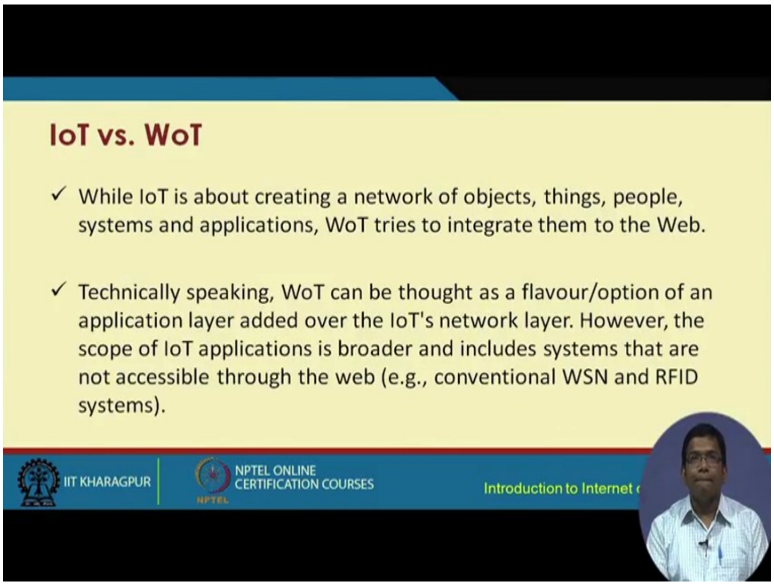
So, M2M can be construed to be a part of IoT while M2M standards have a prominent place in the IoT standard landscape, however IoT has a broader scope than M2M. So, there can be broader range of interactions and not simply machine to machine interaction. They can be interactions between not only machines and machines things and things, but also things and people, things and applications and people with applications.

(Refer Slide Time: 34:23)

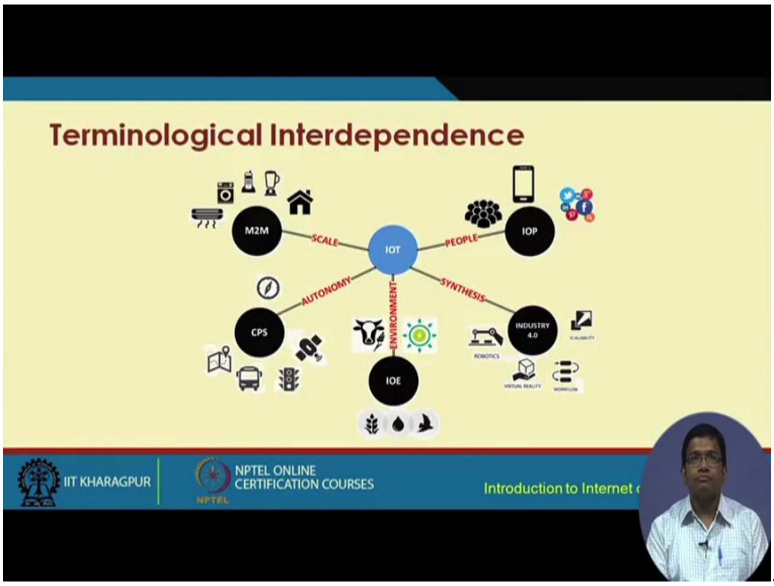


IoT and web of things, internet of things and web of things are often confused to be one and the same, but there is a distinction. The web of things basically focuses more on the use of web based technologies, such as HTML5, JavaScript, Ajax, PHP and so on and so forth.

(Refer Slide Time: 34:51)



(Refer Slide Time: 34:53)



Over the regular IoT to make IoT smarter and web accessible, there are a lot of terminological interdependence when we talk about IoT.

IoT has similarity with internet of people which has a people focus IOP from IoT different using IoT different industry oriented machines and so on can be controlled. So, we have smart factories, you know smart factories using a robots virtual reality and so on. One can have industry 4.0 which is an approach to the modern day mechanization or improvement of the current day plans and industries.

Internet of environment is another. We have CPS which is basically the Cyber Physical Systems, where these systems basically autonomously they operate and they can in fact in an IoT world what can happen is these CPS systems, these different CPS systems, they can be internetwork together in this particular internet. That means, the internet of things we have M2M machine to machine communication.

I already mentioned to you maybe what can happen in a smart home machines, such as the lighting system can talk to the cooling system directly, the cooling system can talk to, can communicate with the fans directly, the fans can communicate with a mobile phone directly or the mobile phone can communicate with a fan directly. So, as you can see that between two different machines, without any human intervention, you know communication can take place and this is known as M2M.

So, with this we come to an end of this particular lecture and we are going to continue with the introduction in the next part of the lecture as well. So far what we have understood are the basics of internet of things, the motivation behind internet of things, the different application areas, the different main points, the challenges that are involved and what we are envisioning when we are talking about building internet of things in the future.

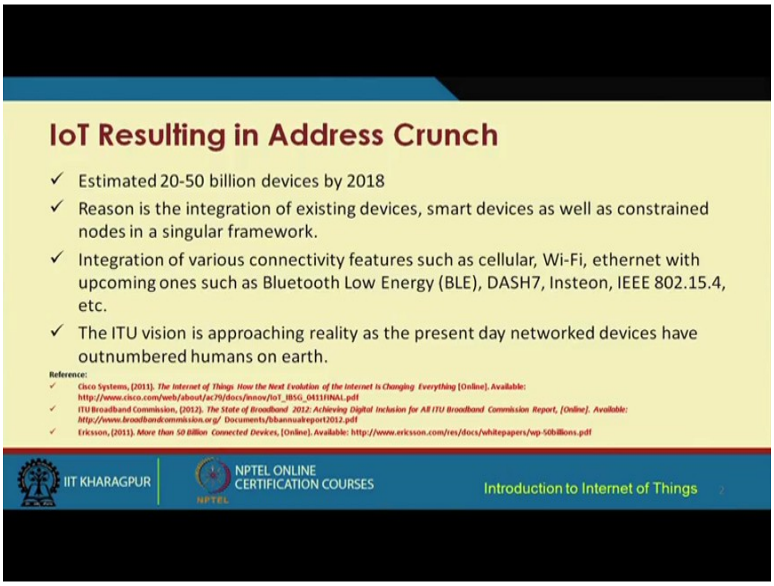
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 02
Introduction to IoT-Part- II

So, now we are going to continue in this lecture with the other basic instructions Basics of Internet of Things.

(Refer Slide Time: 00:34)



So, we have already seen that in the future, it is estimated that the number of things are going to be many, the number of internet of things that are going to be connected are going to be many. So, it is estimated as per one of the studies that by 2018, almost we are going to have 20 to 50 billion devices that are connected that are going to be internetworked.

So, many different applications, so many different devices and these devices are going to be made smart in these applications. So, that is the reason why we are going to have an explosion or in the number of these internetwork things, number of devices connected to the internet of things.

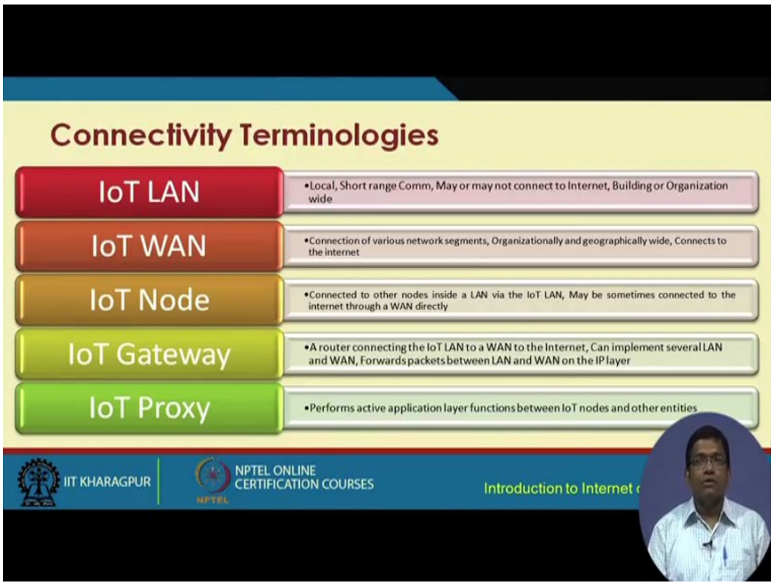
So, as we can understand that if you want to internetwork, if you want to form a network, a big network, a joint network of internet of things, that means these things being connected, then one fundamental problem that is going to happen is there is going to be an address crunch. We are going to soon run out of the number of addresses that we can assign to each of these devices, the different addresses for example the IP address and so on.

So, IPV4 is defiantly not good enough. People have explored the use of IPV6, but what is required is to come up with a completely new type of addressing scheme which can take care of these issues because of this address crunch.

The next thing is the connectivity. At present there are different various sources, different various ways of offering connectivity. Cellular is one Wi-Fi Ethernet, then Bluetooth Low Energy, Dash 7, Insteon, IEEE 802.15.4, 802.15.6, 80.2.16 so and so forth. So, many different connectivity mechanisms, connectivity standards are available.

So, this is going to be another challenge with respect to network. So, how you are going to have some kind of handshaking between each of this different isolated standards. So, this handshaking has to be, handshaking mechanism has to be devised.

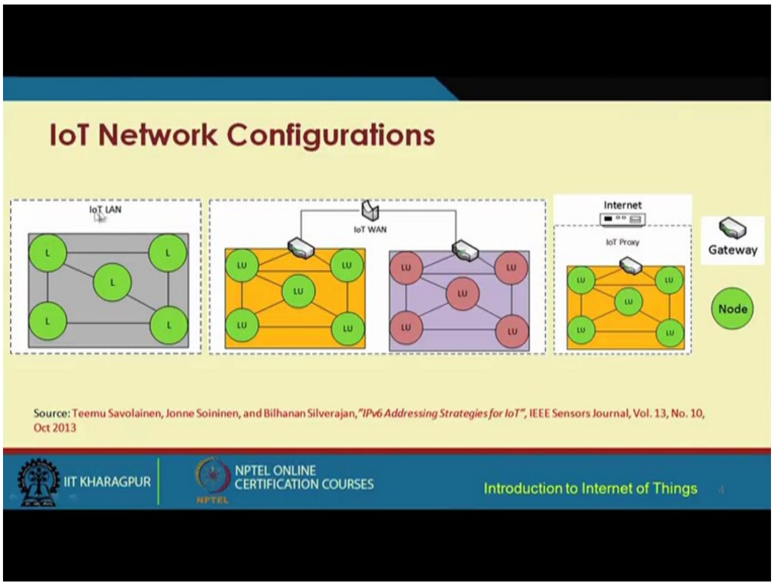
(Refer Slide Time: 03:08)



So, in terms of connectivity, we are talking about concepts called Unique Building Blocks, such as the LAN IoT, WAN IoT, Node IoT, Gateway IoT, Proxy and so on and so forth. So, all most analogist to what we have as different components of the internet, the capital I internet means the internet of computers analogously. We are also going to have these different components, the LAN, the WAN, the Node, the Gateway, the Proxy, these different components.

So, the concepts are very similar as we have in the internet. So, IoT LAN is very similar to IoT, the internet LAN. So, this is for Local Short Range communication may be building wide or campus wide and so on. IoT WAN is basically internetworking of two different LANs, you know inter connecting of two different LANs, connecting different various network segments organizationally or maybe geographically wide and these can be connected to the internet IoT Node which is the connectivity of the different Nodes inside a LAN or maybe a WAN also directly. Sometimes the LAN you know, the Nodes in the WAN can also be connected IoT. Gateway is basically sort of like you know a router or something very similar which connects to the IoT LAN. So, it is sort of like the outside world, the Gateway beyond a LAN and typically connecting to the WAN. So, we can have in WAN, you know several LANs connected to each other through the individual Gateways and Proxy very similar to what we use proxies for security proxies for sub networking and so on.

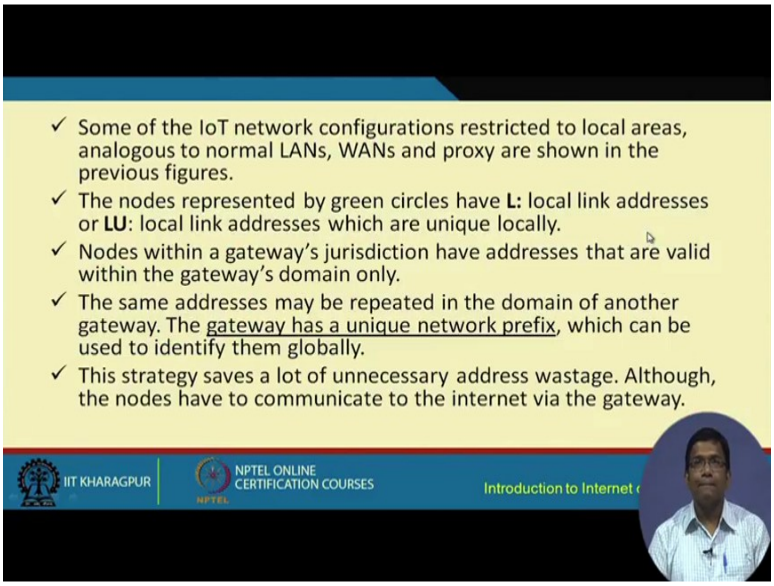
(Refer Slide Time: 05:15)



So, if you look at the first picture over here, what we see is IoT LAN. So, you know IoT LAN we have this different IoT devices and each of these devices has its own unique address, local address and these addresses are local uniquely uniquely local. So, unique that what I am trying to say over here is within a particular LAN, these addresses are unique, these local addresses are unique and similarly, within another LAN, IoT LAN these addresses are unique. So, these are locally unique addresses. So, it might so happen that a particular address might be unique to this LAN, but may be reused in another LAN.

So, the other thing is that these two different LANs, they can connect via two different Gateways. These are the Gateway Nodes and also, we have seen that there is a concept of Proxy. So, Proxy basically helps connects to connect to the external internet. So, Proxy helps to connect to the internet. So, it is beyond the Gateway and connecting to the internet that is offered by the Proxy.

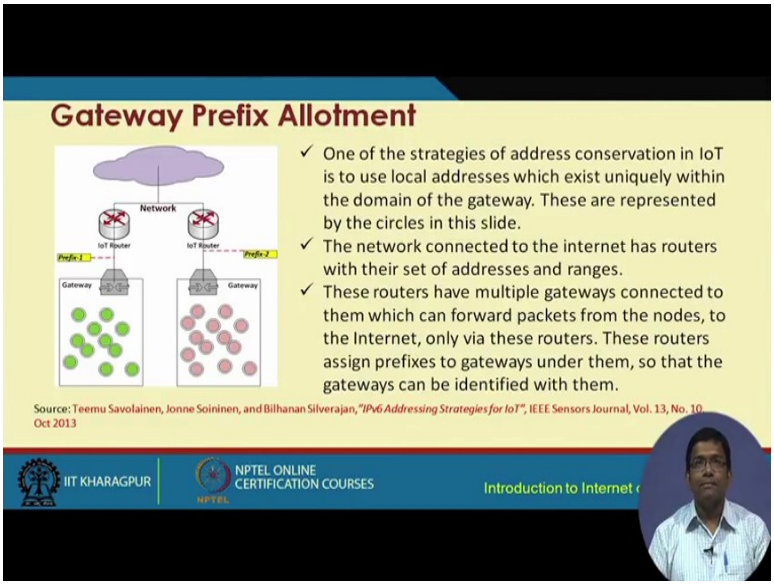
(Refer Slide Time: 06:56)



So, some of the IoT network configurations are restricted to local areas, very analogous to what we have as internet LANs, WANs and Proxy and this is what we have seen in the previous figure.

So, the Nodes that are within the Gateways jurisdiction have addresses that are valid within the Gateways domain only and the same address maybe repeated in another domain as I was telling you before in the previous slide in the previous diagram. So, the Gateway has a unique network prefix which can be used to identify them globally. So, there is a unique network prefix as well and we are going to look at it shortly. So, this strategy basically saves a lot of unnecessarily address wastage and although the Nodes have to communicate to the internet via the Gateway.

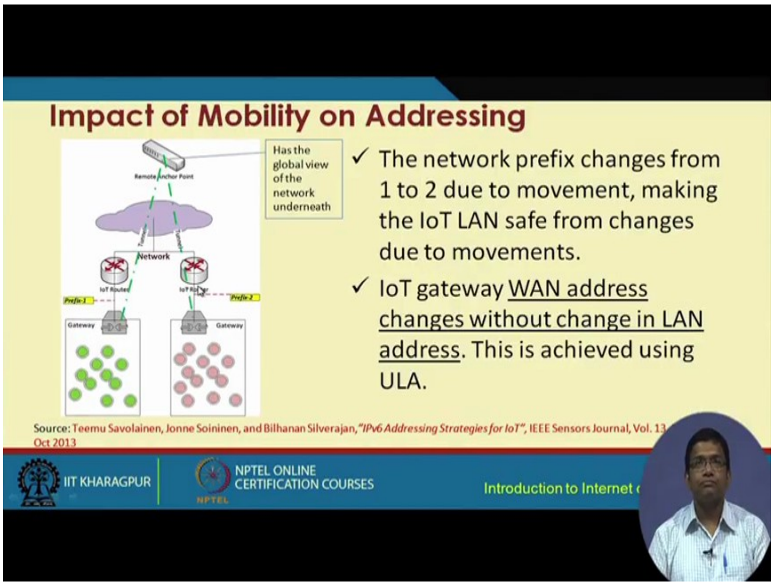
(Refer Slide Time: 07:50)



So, for address conservation as we have seen, these addresses are unique locally, but they can be reused in another domain, but these networks are connected to the internet, these IoT networks are connected to the network through the Gateway and these IoT routers the network is connected to the internet and these are connected through the routers and these have their own set of addresses and ranges and that means the address ranges.

So, these routers have multiple Gateways and they are connected to them which can forward packets from the Nodes to the internet only via these routers and these routers assign the prefixes to the Gateways that are under them. So, we have this prefix 1 and prefix 2, two different prefixes that I used that are assigned by their corresponding routers to the Gateway. So, prefix 1 is assigned by this router to this Gateway and prefix 2 is assigned by this router to this particular Gateway.

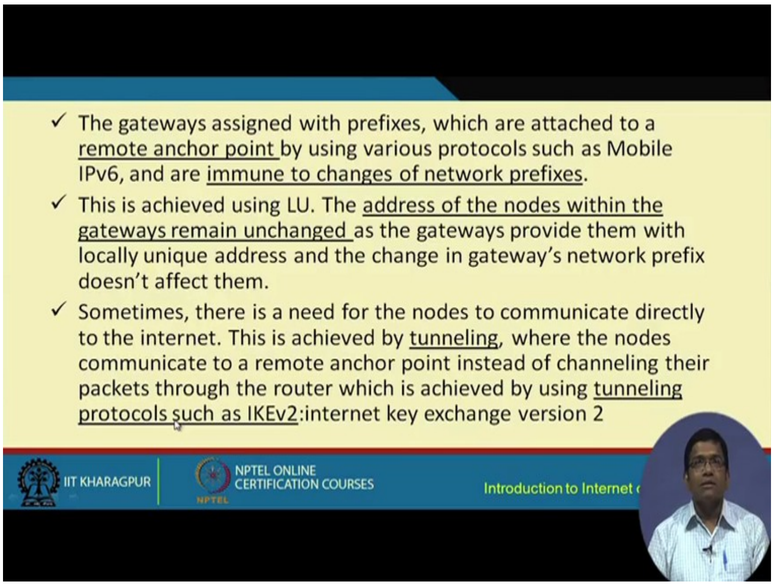
(Refer Slide Time: 09:11)



Now, this is a very important concept that has been proposed because it helps to solve the problem of mobility. So, basically what is going to happen is when a particular Node changes its position from a particular network to another network, let us say from this network is Node moves and comes to this particular network, then the prefix is also going to change from 1 to 2 and this is going to make the IoT LAN safe from changes due to mobility. So, IoT Gateway, basically the IoT Gateway WAN takes care of the address changes without change in the LAN address. So, within the LAN, the address remains the same, but with the help of assignment of this unique prefix, the WAN address changes and that is how the mobility addressing aspect of mobility is taken care of.

So, in this particular figure, we see that there is this concept of the remote anchor point and these particular entity in this network is the one which has the global view of the network that is underneath. That means, this entire network comprising of these LANs, this WAN, the Gateway, then this thing routers and so on. So, this particular entity is considered to be the one which has the unique global view of this network underneath.

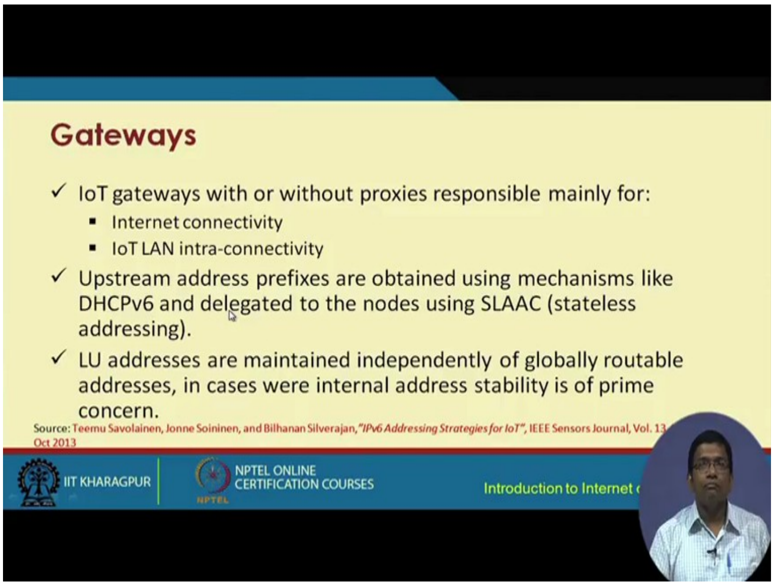
(Refer Slide Time: 10:54)



So, now let us try to understand few other concepts surrounding it. So, we have already seen that there is a remote anchor point and if there is a change in the network prefix that can be taken care of automatically and technologies or protocols, such as mobile IPV6 can come helpful in this particular scenarios assuming that IPV6 based addressing is being used.

So, within a particular LAN, the address of the Nodes remain unchanged because they are within the Gateway and so within the Gateway, there is a local unique address and the change in the Gateways network prefix does not affect them, but it might be required for the Nodes to communicate directly to the internet as well and this can be done with the help of concept of tunnelling where the Nodes can communicate to a remote anchor point instead of channelling their packets through the router. This can be done with the help of tunnelling protocol, such as IKV, IKEV2. So, this is how with the help of IKEV2, this tunnelling can be done with the help, with the remote anchor point through the Gateways. So, indirectly from the Gateway to the anchor points, the tunnels can be set up like this.

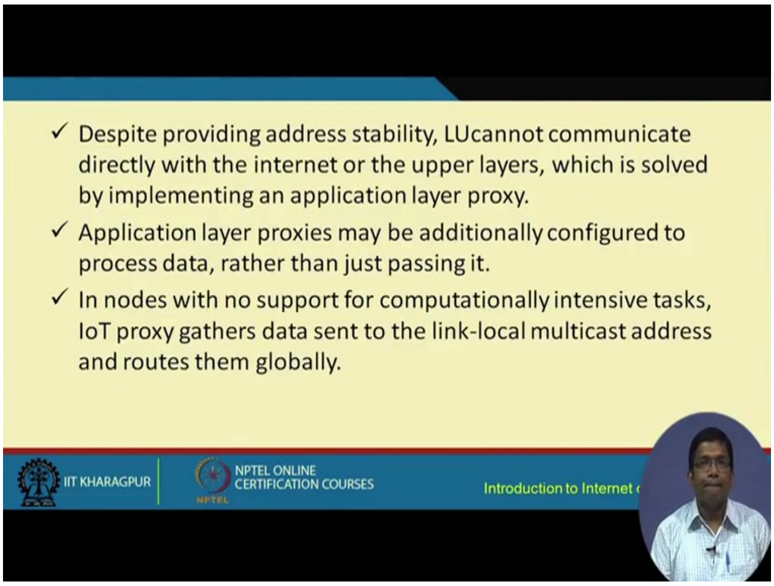
(Refer Slide Time: 12:25)



The Gateway has you know associated, they can come with or without proxies and they can offer internet connectivity or intra LAN connectivity. So, within the LAN, they can offer connectivity between the different Nodes within it so for up upstream addressing, that means beyond the Gateway.

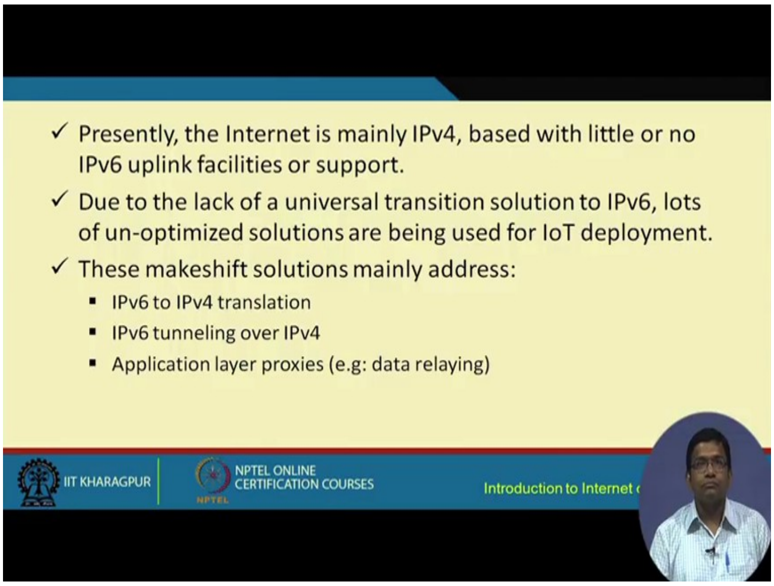
So, Gateway to the internet mechanisms, such as DHCPV6 assuming that IPV6 technology is being used, DHCPV6 for state based addressing or SLAAC for stateless addressing can be used and the locally unique addresses are maintained independently of the globally routable addresses in cases were internal address stability is of prime concern.

(Refer Slide Time: 13:21)



So, we have to keep another thing in mind that despite this mechanism of address stability, the LU cannot communicate directly with the internet or the upper layers which is solved by implementing an application layer Proxy. So, this proxies basically help in achieving connectivity to the upper layers on the internet.

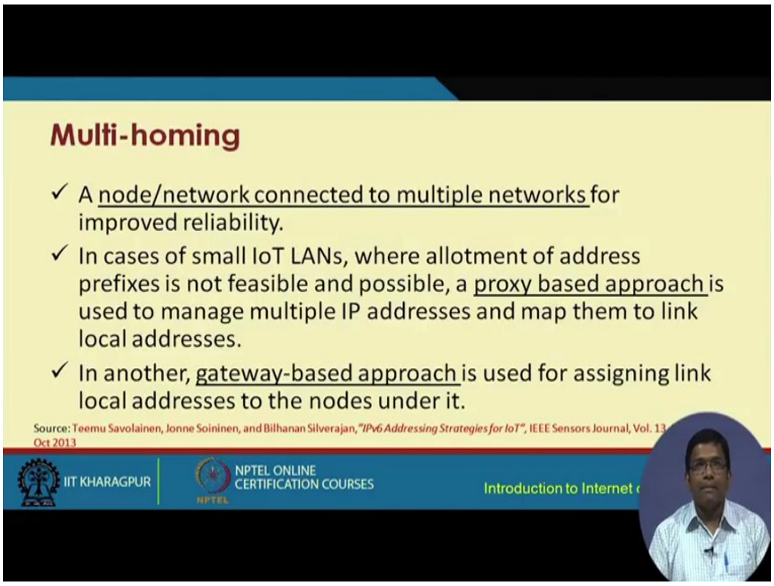
(Refer Slide Time: 13:50)



So, most of the IoT based solutions at present still are using IPV4. There are very few IPV6 implementations. So, what is going to happen is if you want to deploy, if you want to approach building IoT by expanding the existing internet, they approach one that I talked about initially as part of lecture 1 for building IoT.

So, in that particular case, what needs to happen is there are different addressing schemes that are followed IPV4 IPV6 and so on. So, something like address translation between IPV4 and IPV6 and vice versa has to happen. This is one until we have a separate addressing scheme, a new type of a addressing scheme. So, handshaking or translation of addresses from IPV4 to IPV6 or from IPV6 to IPV4 number 1, number 2 is tunnelling of IPV6 over IPV4. So, maybe some part of the network uses IPV6. So, these IPV6 PD used can be tunnelled over IPV4 PD used application layer proxies can also be used and these can help in achieving tasks such as data relaying.

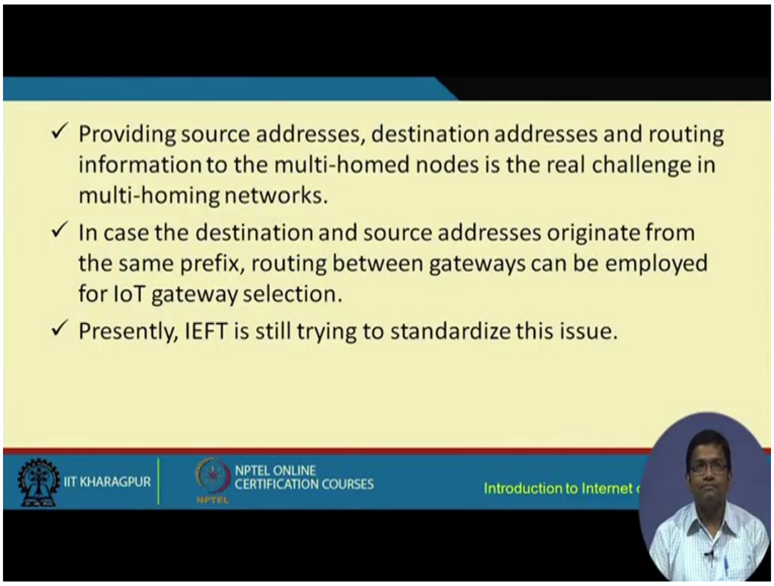
(Refer Slide Time: 15:21)



Finally, I would like to mention that there is a concept of multi-homing, where a particular Node or an IoT device or the sub network, IoT sub network can be connected multiple networks for improving the reliability. So, basically multi-homing is a concept that is used for improving the overall liability of the network in that way. So, in the same state if some component of the network or maybe a Node has gone down, there is another network that can take over.

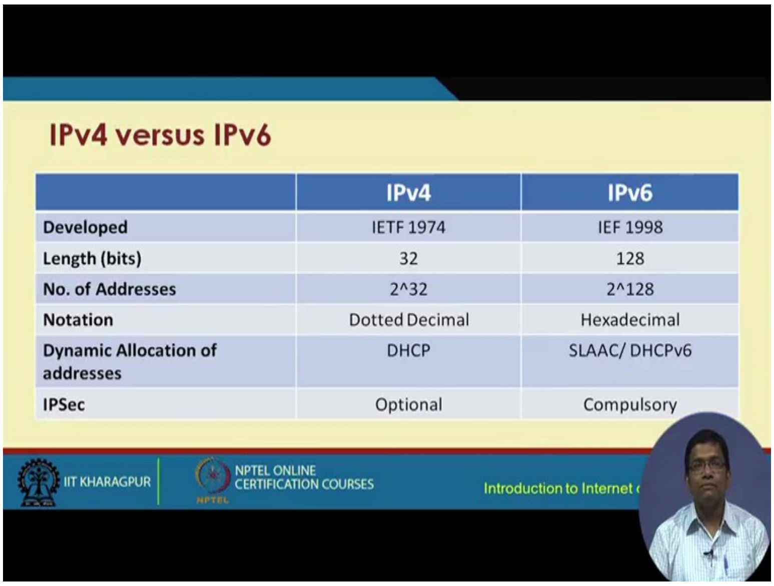
So, for these multi homing, there can be two different approaches; a Proxy based approach can be used or a Gateway based approach. I do not need to explain these two approaches in detail, but these names basically tell how the things are going to be managed for multi-homing using these different approaches.

(Refer Slide Time: 16:16)



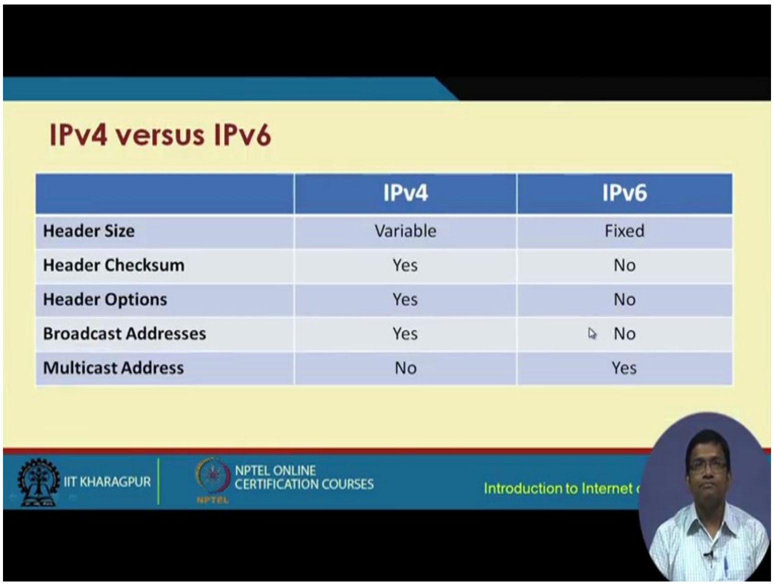
So, providing source address, destination address and routing information to the multi-homed Nodes is the real challenge in multi-homing networks. So, presently IETF is trying to standardize this particular issue.

(Refer Slide Time: 16:32)



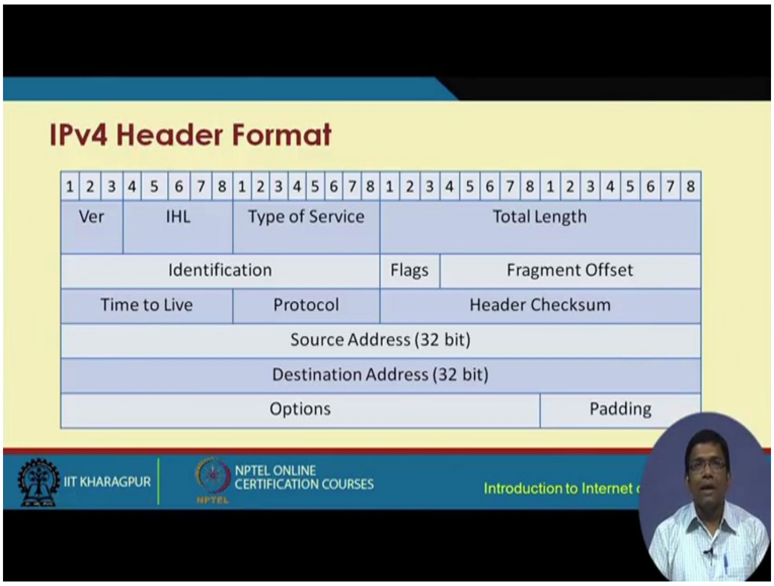
So, IPV4 is being used, some parts IPV6 being used. We can use both, but that is not going to be sufficient. We have to come up with a new addressing scheme which we do not know yet what is going to happen. People are still working on it, researches are coming up with different mechanism. There are still lot of research effort on building addressing schemes for IoT, but if IPV4 is used and IPV6 is used, these are the comparison points of comparison between the use of IPV4 and IPV6. The main point of difference is that because the bit length, the length over here in IPV4 is 32 and in IPV6 is 128, the number of addresses in IPV4 is S2 the power 32 only. On the other hand, the address space over here is 2 to the power 128. So, we are going to get a large address space and I think we already know that there is a difference in the notation in IPV4 which is dotted decimal notation and it differs from the IPV6 which has a hexadecimal notation for addressing.

(Refer Slide Time: 17:49)



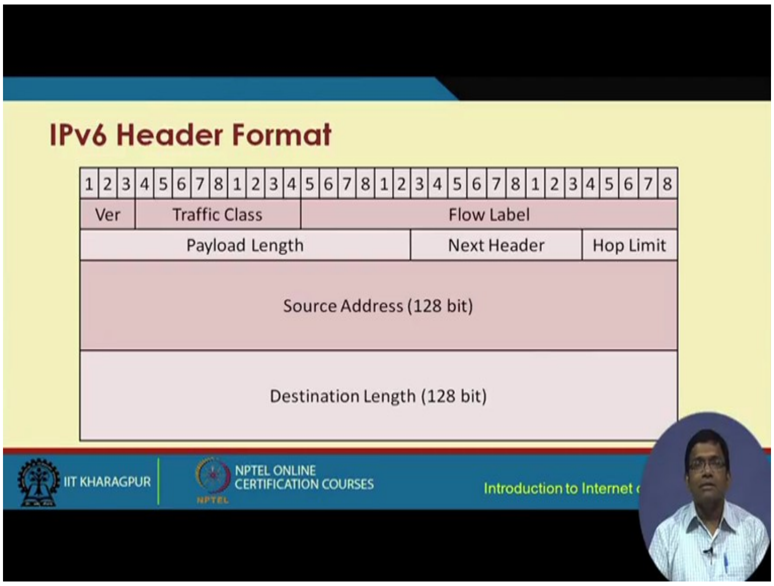
	IPv4	IPv6
Header Size	Variable	Fixed
Header Checksum	Yes	No
Header Options	Yes	No
Broadcast Addresses	Yes	No
Multicast Address	No	Yes

(Refer Slide Time: 17:55)

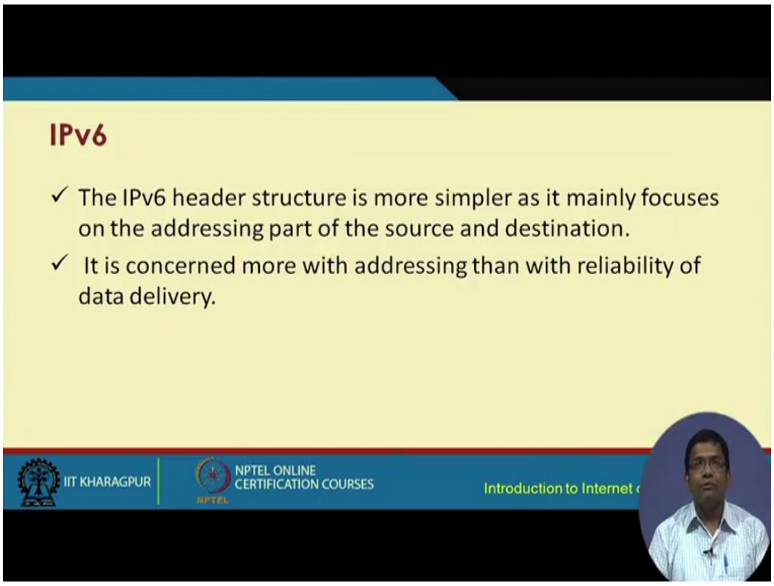


So, here are few other points of comparison which I am not going to go through and here is the IPV4 header format.

(Refer Slide Time: 18:01)



(Refer Slide Time: 18:06)



Here is the IPV6 header format. So, these IPV4 and IPV6, they have to go hand in hand until there is a new solution for addressing a new mechanism which is completely different from these proposed. So, they have to work hand in hand. So, you know mechanism such as tunnelling or address translation mechanisms have to be used in order for this thing to happen.

So, with this we come to an end of introduction on IoT Internet of Things. We have already understood the motivation for building IoT systems, the different applications of IoT systems, the different characteristics of IoT systems, the different challenges that are involved from networking prospective, what are the different components for building IoT. IoT is a joint network, but then you have to use a modular approach, a step by step approach, a phased approach to building IoT. So, what are the different components from a networking prospective that can be used is what we have already gone through and we have understood.

So, with this we come to an end of the lecture on the Introduction of Internet of Things.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 03
Sensing

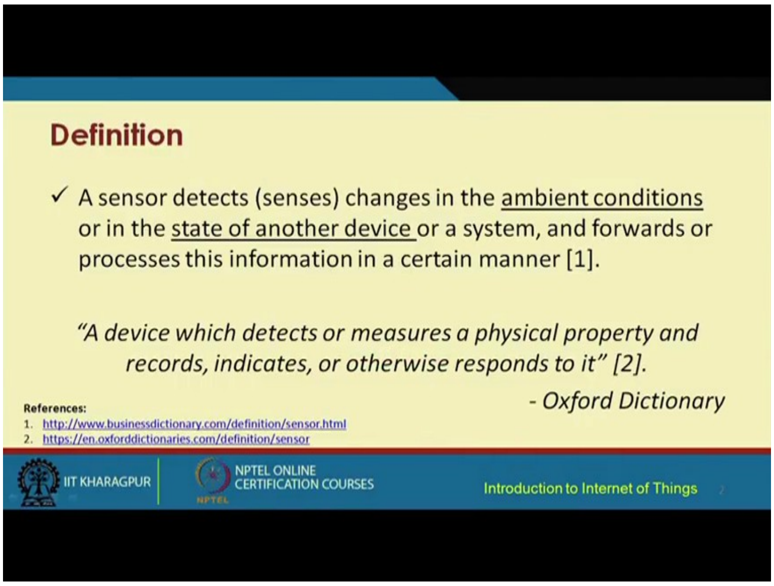
So, we have already understood the basics of internet of things. Now, let us try to understand that what are the essential building blocks of internet of things. So, one of the very essential components of internet of things is sensors and the other one is actuators whereas, the sensors basically sense the physical phenomena that are occurring around them and the actuators basically based on the sensed information. The actuators, they actuate. That means, they perform some actions on the physical environment. So, they take some actions based on what has been sensed.

So, essentially if we see that we have a gradual phase wise approach to building internet of things. So, we have sensors which are sensing the sensors, they sense different parameters depending on the sensor being used. For example, temperature, pressure, humidity conditions, lighting conditions and so on. Then, what will happen is these sensed information are going to be sent over a connected system. That means, over a network that information will be passed, it can also involve cloud and so on and finally, that information is going to be transmitted based on what has been sensed and based on the requirements, some physical action is going to be taken by an actuator.

So, may be a bulb might be turned on if certain conditions, in an agricultural field has happened, maybe if the field based on the sensors it is found out that in an agricultural field, the field has run out of stagnant water that is required for paddy crops. Then, what might be required is based on that sensed information automatically the valve of the water pump, the deep to well that is used or a shallow tube well that is used for irrigation, automatically that valve will be turned on, so that the field gets irrigated.

So, that can be done through the process of actuation. So, we have sensing. we have IoT or simply the network and then, we have this actuation. So, sensing network actuation we start with the sensing component. Now, in the next lecture we will try to understand how actuation is done.

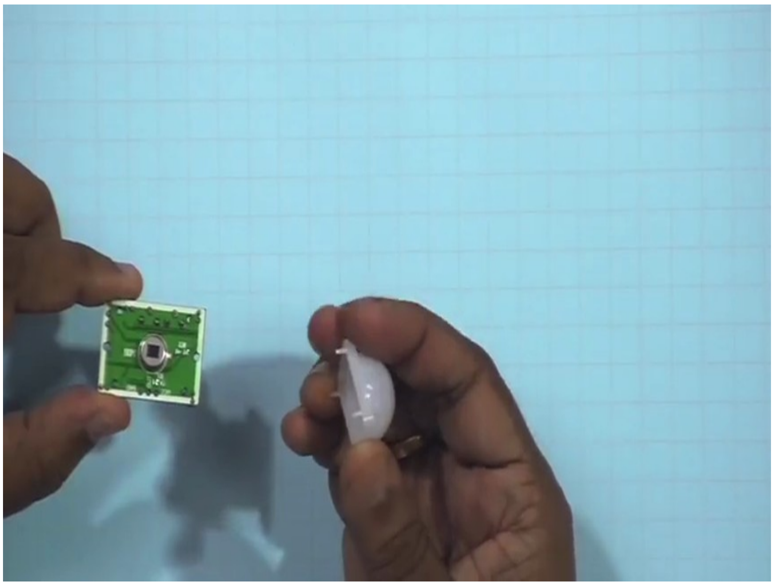
(Refer Slide Time: 03:17)



So, when we talk about sensing, we need to understand what is sensing. So, basically a sensor it detects or senses the changes in the ambient conditions or it can also sense the state of another device. So, maybe one sensor can check, can sense how and what is the state of another device. So, this is what he is done with the help of sensing. So, some physical property of the ambient conditions of the environment in which the sensor is in or of another machine or a system a separate one, these can be sensed with the help of sensors.

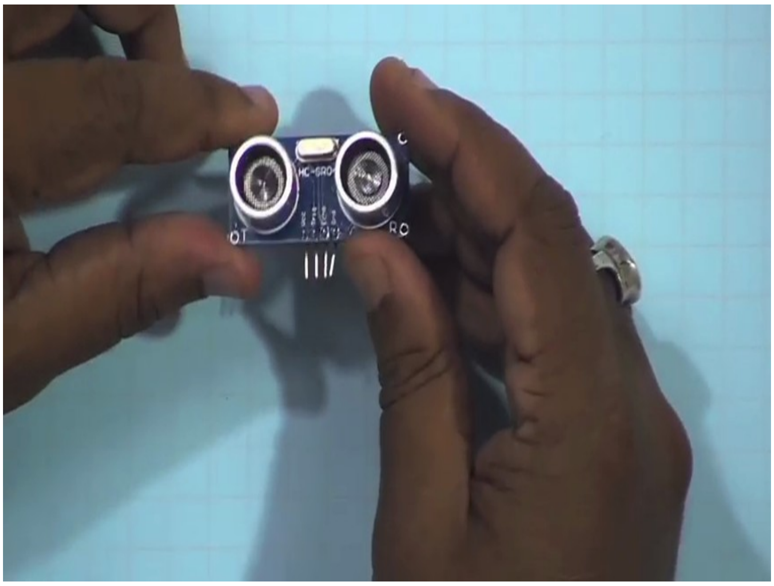
So, let me now show you some sensors, some real sensors that we have.

(Refer Slide Time: 04:06)



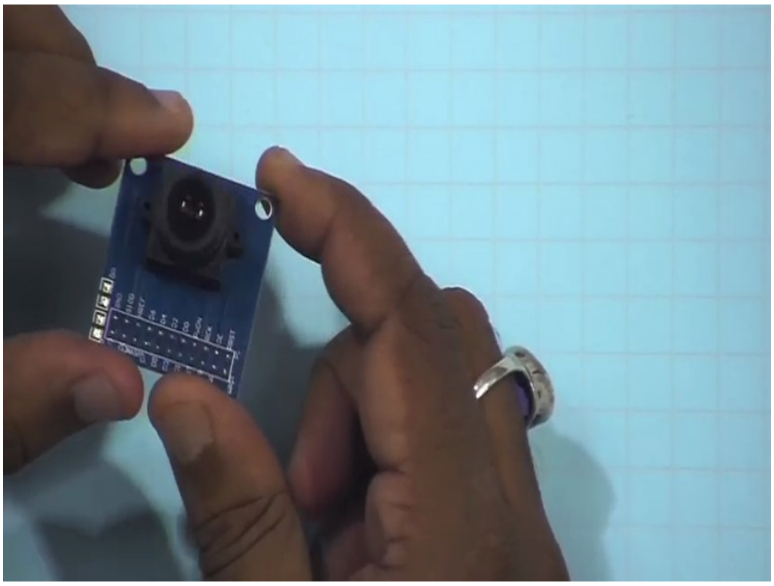
So, here are few real sensors and this is a sensor that is used for obstacle detection. This is a PIR sensor passive infrared sensors. So, this passive infrared sensor here can be used for detecting if there is any obstacle. So, this is an example of a PIR or obstacle based sensor.

(Refer Slide Time: 04:45)



Then, we have another sensor this is the ultrasonic sensor. This basically detects that how far that obstacle is. This is another sensor. So, here as you can see that there are like two eyes kind of things. So, what happens is these ultrasonic sensors may send ultrasound waves. So, these ultrasound waves are sent and then, that sound wave is going to get reflected back. We already know what velocity is and then, depending on how much time has elapsed from the point sound wave was sensed and the deflection is received back, based on that the distance is calculated. So, this sensor helps in basically getting an idea or sensing how far an obstacle is from a particular point where the sensor is.

(Refer Slide Time: 05:46)

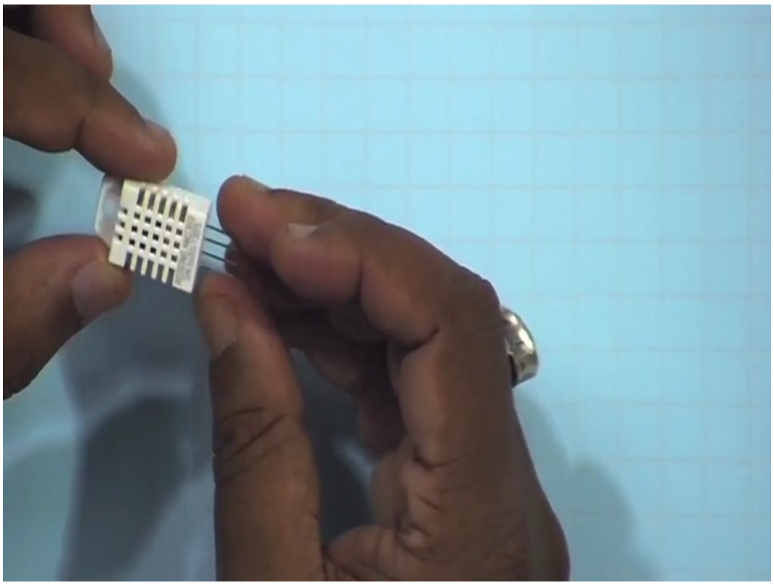


Then, we have another sensor which is the camera sensor. This is as you can see over here is small IoT camera. Since the camera sensor, then we have this one here which is a smoke detection sensor. So, this sensor can help in detecting the smoke.

(Refer Slide Time: 06:08)

Finally, I would like to show you another sensor which is the temperature and humidity sensor. This is actually, this measures both of these together this particular sensor.

(Refer Slide Time: 06:23)



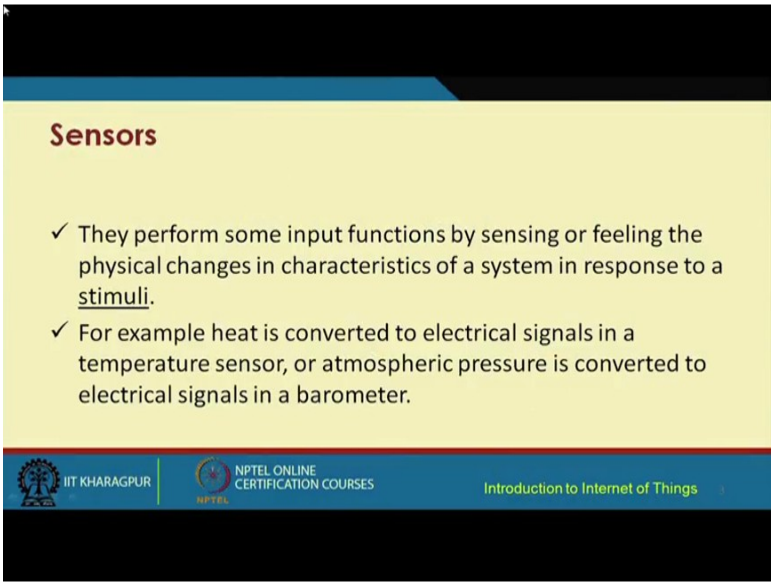
So, these are some real life sensors, real examples of sensors that I have just shown you like this. There are different sensors that can be purchased. These sensors, they have different functionalities and these functionalities are typically unique. That means that one sensor which is fabricated to do, to measure a certain physical property, it cannot measure another one or more specifically let me give you an example to illustrate this point because this is something that many people make a mistake.

So, a temperature sensor can measure temperature only. It cannot measure for instance smoke or it cannot detect smoke. So, these are very much application specific you know specific things, specific properties, basic specific physical properties can only be detected by these sensors.

Now, the sensors they come in different shapes and sizes. They can be very small, they can be very big. The same sensors can be mechanical sensors, these can be electrical sensors, they can be electronic sensors, they can be chemical sensors. There are so many different types of sensors and fabrication of a sensor is a completely different ballgame. So, whether it is a mechanical sensor or an electronic sensor, electrical sensor or you know a chemical sensor, whatever it is a completely different ballgame. Typically people who are into building of IoT, they focus more on the networking aspects. They focus more on the networking analytics aspects of IoT.

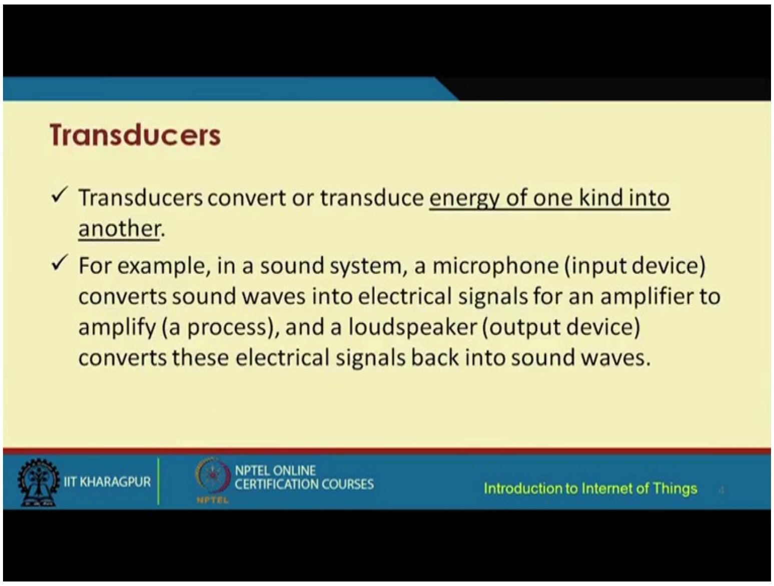
There are separate researchers who work on the design of these sensors. Some of these sensors that I have just shown you, the sensors you know that complete the design, the fabrication it is a completely different story altogether you know. So, you know this is and typically this is done by those who are focusing on sensor design and fabrication. So, typically they are concerned only about how these sensors can be developed, they can be fabricated and they are not bothered about building IoT as such. Of course, there can be some researchers who might also take interest sensors. You know not just the fabrication of the sensors, but also going beyond building of the IoT. Some people might be taking interest in that, but in general it is not.

(Refer Slide Time: 09:22)



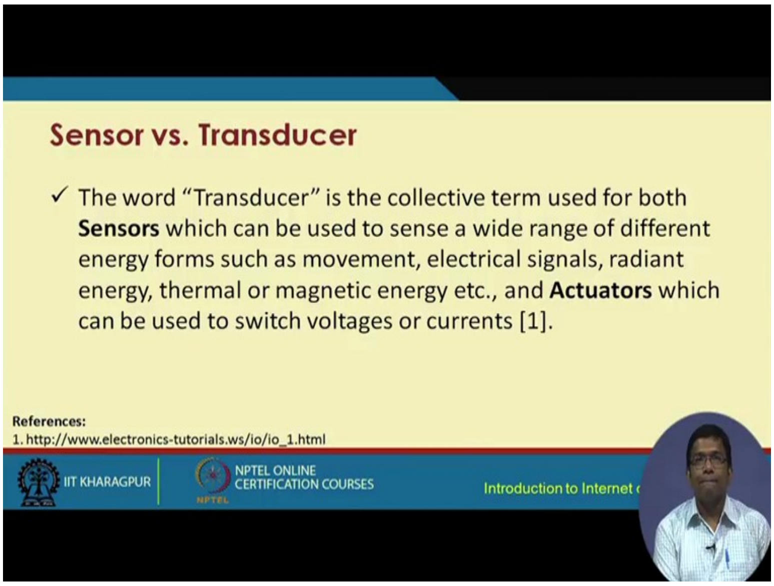
So, the sensors based on certain stimuli, the different stimuli might be there. They can measure the thing in the physical characteristics of the environment of the system and so on and these changes are basically converted to electrical signals. For example, for a heat sensor this heat is converted to electrical signals and this is for temperature sensors. I am sorry, this for temperature sensor, the heat is converted to electrical signals and for sensors such as atmospheric pressure sensors, the atmospheric pressure is basically converted to electrical signals. So, we have different sensors which measure different things, but then these sensed values are converted to respective electrical signals.

(Refer Slide Time: 10:30)



Now, there is an associated terminology which is for the transducers. The term transducers basically convert one form of energy into another form of energy being converted into another. For example, in a microphone what we have in a microphone. So, the sound waves are converted to electrical signals and then, to a output device like a loudspeaker and we are able to hear that sound. So, this is an example of a transducer.

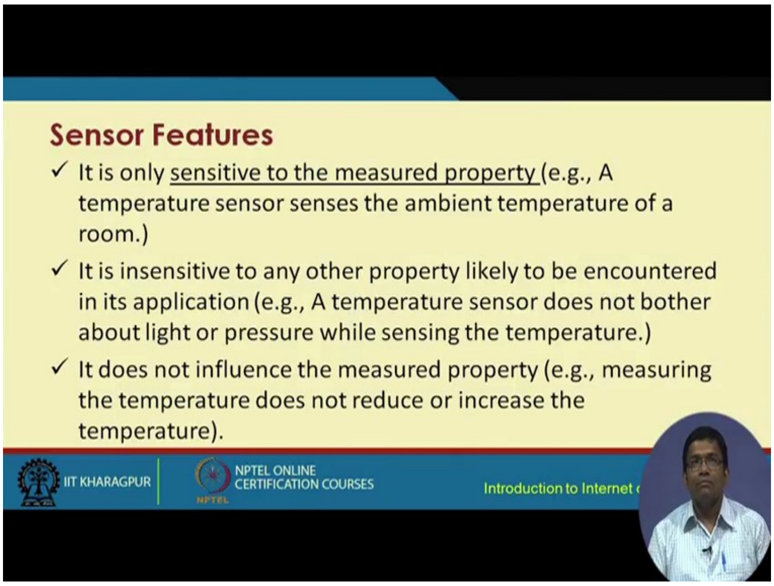
(Refer Slide Time: 11:09)



So, these terms sensors and transducers are very common. They have lot of overlap and we have to understand the distinction between these two. There is lot of misunderstanding people conceived sensors and transducers. We use these terms almost interchangeably, but there are differences.

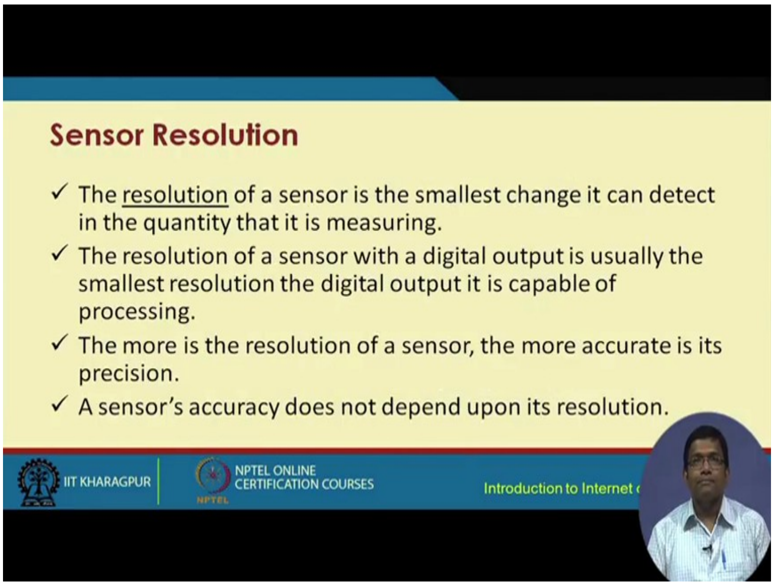
So, the word transducer is a collective term which includes sensors as well as the actuators that I was telling you. Before the sensors can sense what is going on around them and convert to electrical signals etcetera and the actuators can basically perform these actions by maybe switching voltages or currents.

(Refer Slide Time: 12:00)



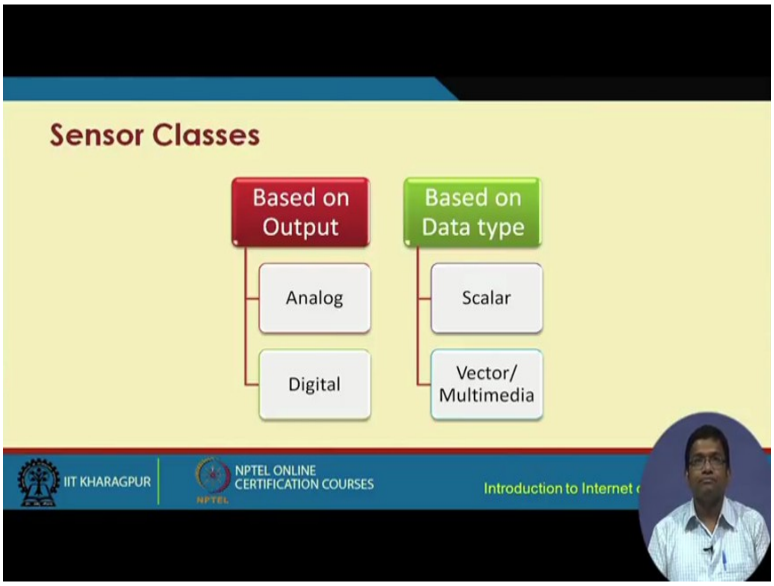
Now, the sensors have different features. They are sensitive to the property, the physical property that is being measured. So, they can do all. They are sensitive only to that measured property. So, basically a temperature sensor can sense only the ambient temperature of the room and it is insensitive to other changes, maybe changes in the atmospheric pressure or changes in the lighting condition of that room.

(Refer Slide Time: 12:31)



There is a terminology which is called the resolution. The resolution of a sensor is basically defined as the smallest change that it can detect in the quantity that is being measured. So, the smallest change that it can detect the resolution of a sensor with a digital output is usually the smallest resolution of the digital output. It is capable of processing.

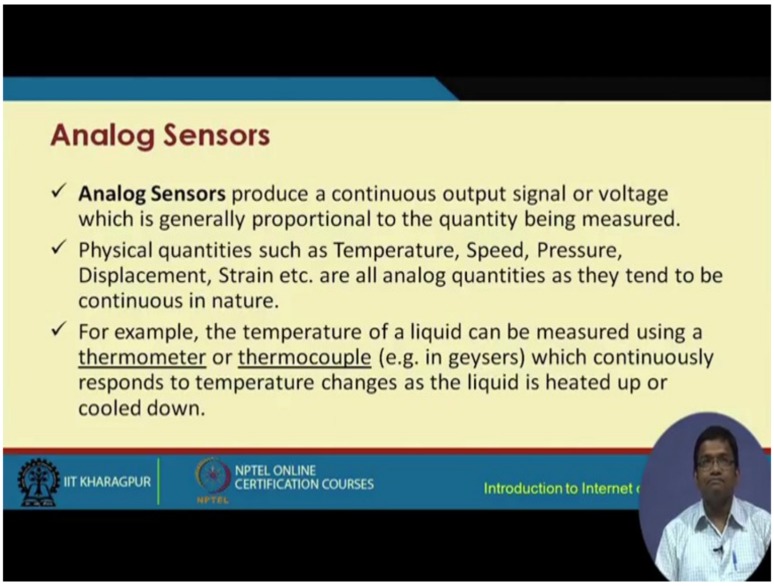
(Refer Slide Time: 12:54)



So, based on the output, the sensors can be classified as analog or digital and based on the data type, they can be classified as scalar or vector sensors. So, in the analog sensor, what we have these sensors give continuous analog output. So, for example, tint temperature sensor continuously changes in the temperature are going to be sensed, measured and the output is going to be an analog signal. Digital sensors basically gives digital outputs on and off for example, and like this come you know discrete digital values are given as outputs by these digital sensors.

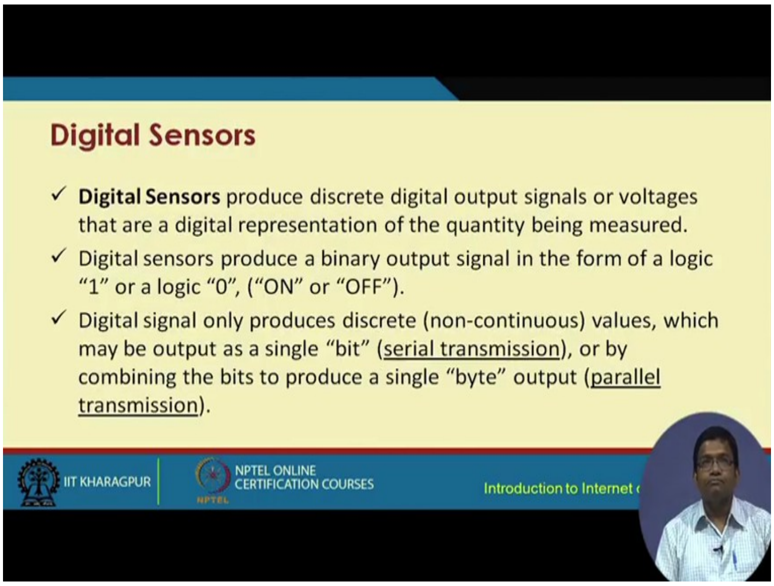
Then, scaler sensors basically measure scalar variables which can measure only the changes in the magnitude whereas, the vector senses not only the magnitude, but also the direction. So, scalar sensor example would be temperature sensor is an example of scalar sensor because you know irrespective of which orientation you put, the sensor temperature sensor or in which direction you are taking it, it is going to give you the magnitude value. Only the changes in the magnitude of the temperature, on the contrary we have the vector sensor. For example, the camera sensor or the accelerometer sensor whose values are dependent on the orientation on the direction and so on direction in which the sensor is being put and the weight is measuring. So, it is dependent on that. So, we have analog sensors, we have digital sensors, we have scalar sensors and we have vector sensors.

(Refer Slide Time: 14:44)



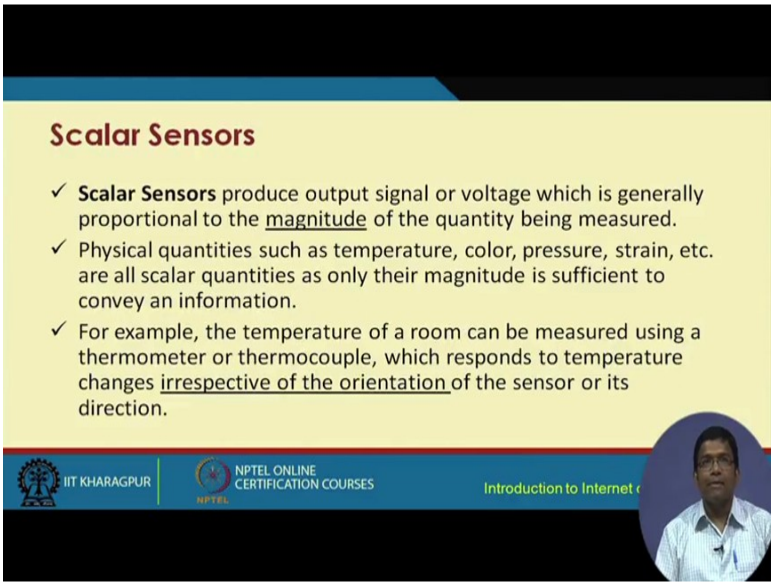
So, analog sensor I already mentioned about analog sensors, temperature sensor. You know temperature is typically measured with the help of thermometer or thermocouple thermometers are quite common, but thermocouple is something that is used in the geezers for example, you know. So, you have two different metallic strips for instance and these strips they know they can, in the thermocouple they can bend and so on. So, these based on that you know based on the amount of bending etcetera. You know they measure the changes in the temperature. So, if you calibrate the thermocouple you know, so accordingly it is going to give how much the temperature has changed and depending on that one can understand how much the liquid has heated up or has cooled down.

(Refer Slide Time: 15:36)



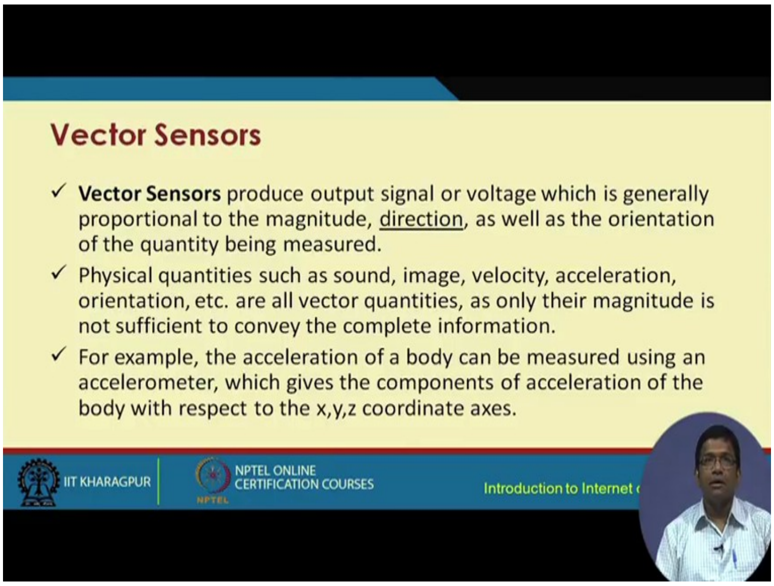
Digital sensors produce digital discreet voltage levels or signal levels. So, binary values like 0 and 1 or on and off or output the digital sensors.

(Refer Slide Time: 15:53)



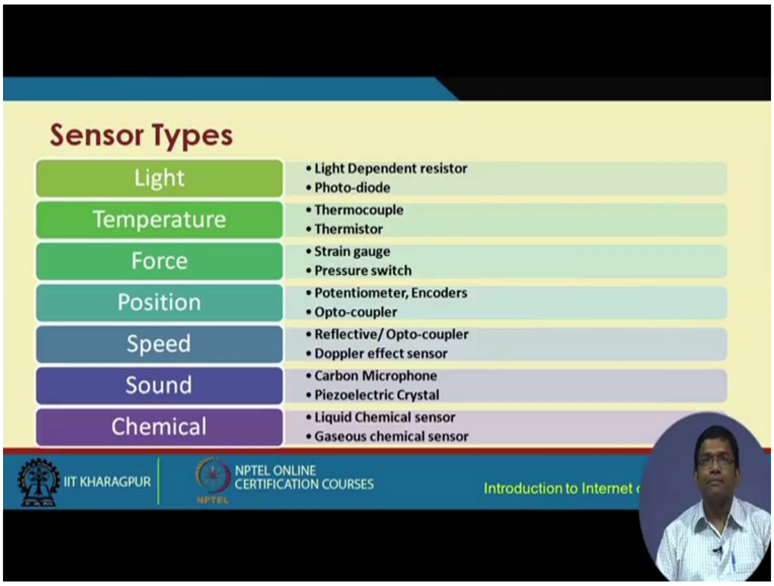
Scalar sensors measure only the magnitude physical quantities, such as temperature, color, pressure, strain etcetera. These are scalar quantities and measurement of the change of magnitude is sufficient to convey the information.

(Refer Slide Time: 16:13)



On the other hand, vector sensors produce output signal of the voltage which is generally proportional to the magnitude as well as the direction and orientation of the quantity that is being measured. So, physical quantities such as the sound, image, velocity, acceleration orientation, these are all vector quantities and their measurement is not just dependent on the magnitude, but also on the direction. So, for example, accelerometer sensor, they give outputs in three dimensions x, y and z coordinate axis.

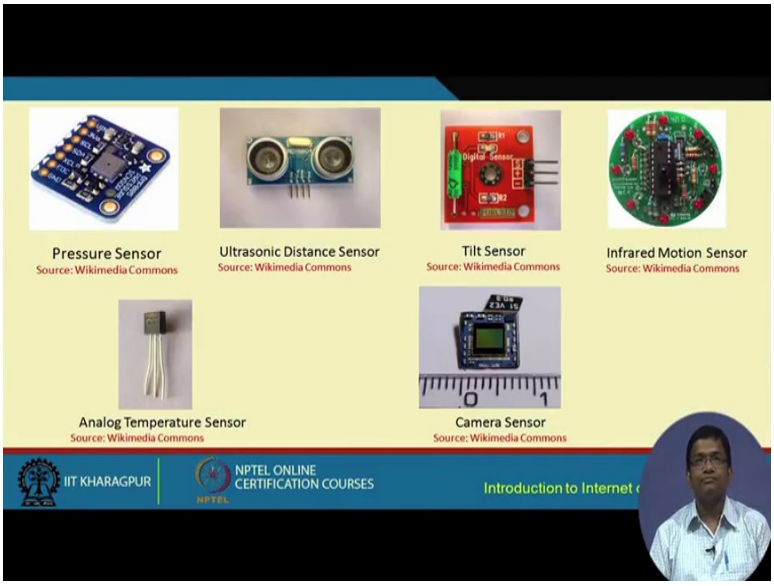
(Refer Slide Time: 16:50)



Here are some examples of different sensors, light sensor for measurement of light. We have the lDR which is the light dependent resistor photodiodes. This can act as sensors for measurement of light for sensing of light. For sensing of temperature, we have thermistor and thermocouple. Thermocouple briefly I told you, but thermistor is sort of like thermal transistor kind of thing, ok.

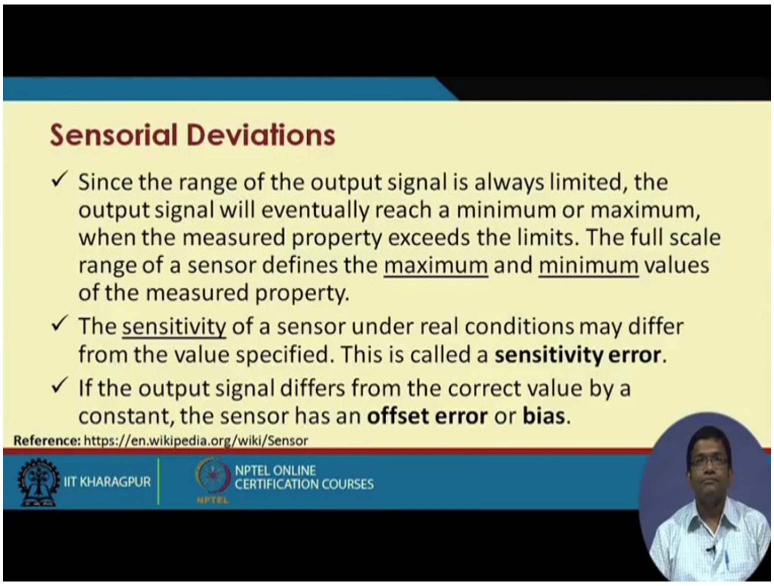
Then, we have for force, we have the stain, strain gauge and pressure. Pressure switch for position, we have potentiometers, encoders, opto couplers. Opto couplers basically you know. So, the optical signals are the optical rays are basically obstructed and based on that you know the position information can be obtained. So, opto couplers then we have the speed for speed sensing. We have reflective sensors, then doppler effect sensors. So, doppler effect based on the relative velocity for example relative velocity of sound you know. So, based on that you know this doppler effect sensors, they work. Then, we have the sound sensors, we have the carbon microphone like our existing traditional microphones, piezoelectric crystals and so on. For chemical sensing, we have the liquid chemical sensors and gas chemical sensors.

(Refer Slide Time: 18:18)



So, I had already in at the outset of this lecture, I had shown you some real physical sensors. Here are some other pi pictures of few other sensors, here is a pressure sensor, here is an ultrasonic distance sensor, tilt sensor infrared motion sensor, camera sensor, analog temperature sensor. So, analogs in temperature sensor, it has you know in addition to the output, it has 2. So, it has three pins. Basically one is for the plus 5 volts and the other one is the ground zero volts and this one is the middle pin is typically used for the output.

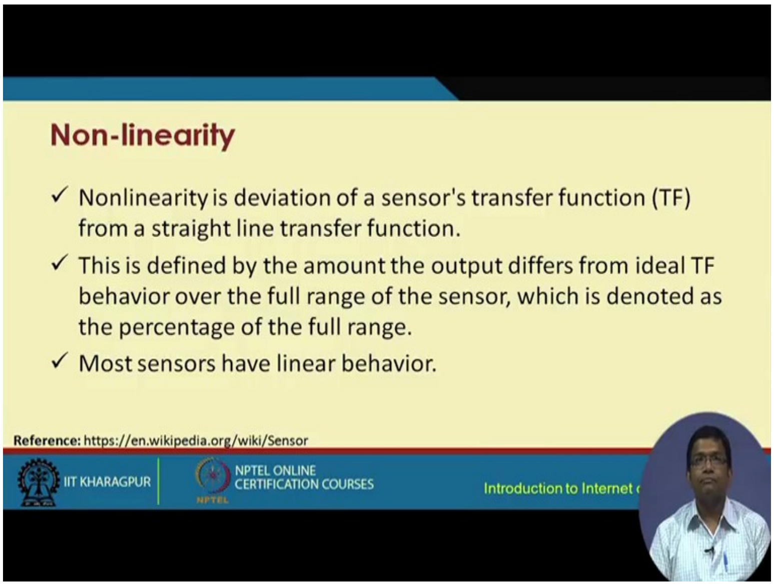
(Refer Slide Time: 19:04)



Now, the sensors often they do not give data that is accurate you know. So, there are some sensorial deviations. So, these sensors they have each sensor and they come with certain specifications. These specifications will give you the maximum and the minimum values that it can measure of the physical property that it is supposed to measure. The sensitivity of a sensor under real conditions may differ from the value that is specified and that is known as the sensitivity error and then, each sensor there can be given you know a value which is constantly the same, constantly different. So, what I mean by this is the correct value might be something and always it will be giving this particular sensor, might be giving a value which is an offset error or a bias and that might, so that many units of offset error reading will be giving at all times and that will be constant. So, for example, two units of offset might be given by a temperature sensor at all times. So, that is different from the sensitivity error that I told you.

So, sensitivity error is more about being sensitive to the changes you know under real conditions, basically how it is being sensitive. Then, what is specified in their actual specifications, it might give certain actual specifications, it might suppose give certain values, but in real conditions, it might be sensitive to certain things. So, this becomes the sensitive error and there will be some error that will be due to that and that sensitivity error that can change over time and that is different from the offset error which is constant over time.

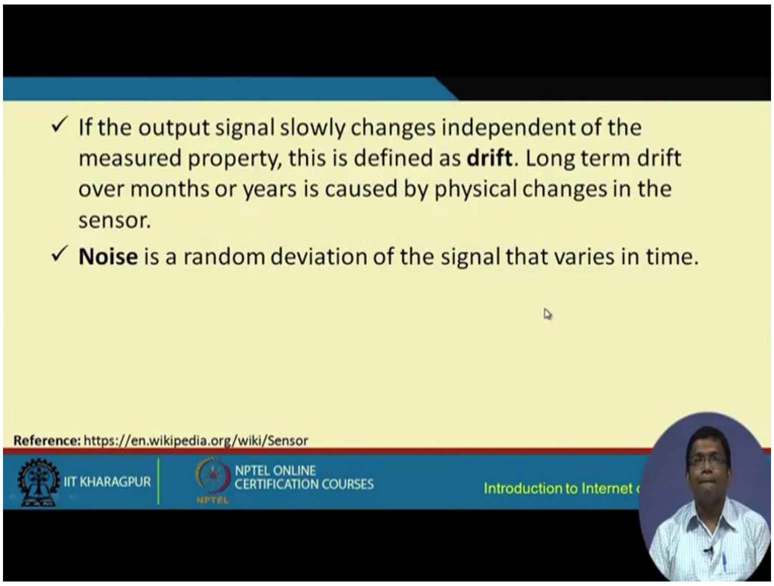
(Refer Slide Time: 21:17)



Now, these sensors typically have linear behavior. Most of the sensors, not all have a linear behavior, but there is often in practice a non-linearity behavior that is exhibited by the sensors and ideally they should behave linearly, but in practice stays off will behave non-linear. So, this non-linearity is the deviation of the sensors transfer function from linearity.

So, this is basically defined as the amount of the output that differs from the ideal transfer function behavior over the full range of the sensor.

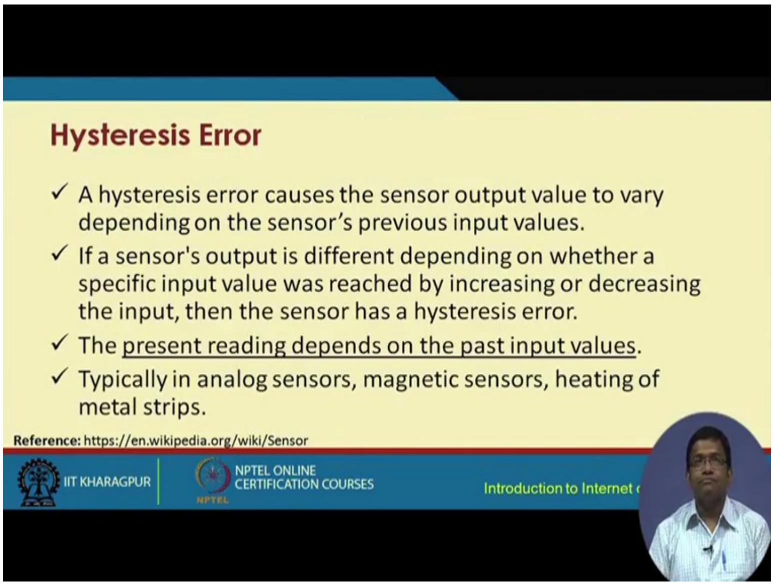
(Refer Slide Time: 22:09)



So, if the output signal slowly changes independent of the measured property, this is known as drift. So, it might happen that a particular sensor at one point we give a certain value and then, if you use the same sensors for measuring the same condition due to the drift, you might get a drifted sensed value. So, it will be different; it might be different. So, it induces some drift if you keep it overtime.

So, the other type of error is the noise which is basically due to different other external factors and it is a random deviation of the signal with time.

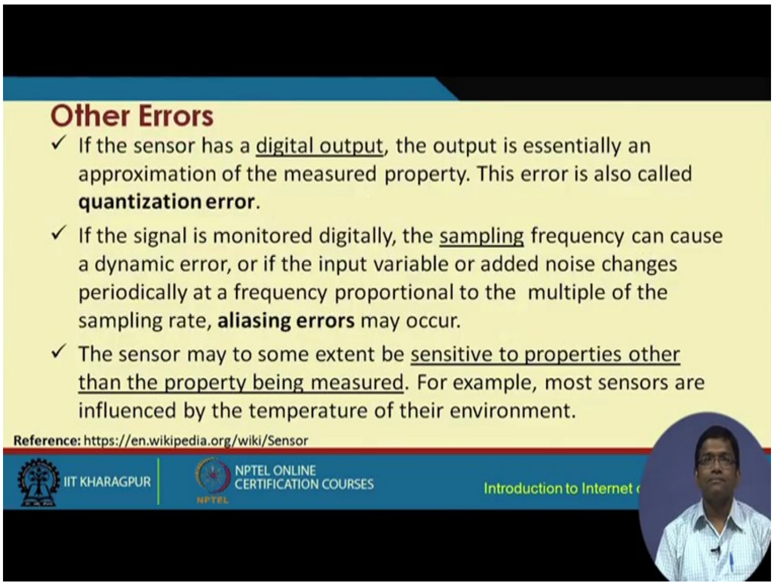
(Refer Slide Time: 22:52)



Hysteresis error is bit different and typically it is exhibited by analog sensors, magnetic sensors heating of in sensors that use the principle of heating of metal strips and so on.

So, in these sensors, these analog sensors or magnetic sensors and so on sometimes what happens that the present reading depends on the past input values. How? It is maybe because it uses some metal strips and maybe the property or the functionality of that sensor is such that when you heat it, it is going to the metal strip is going to bend. So, so you know if it has bent once to come back to its original position, it will take some time. So, this type of error basically talks about that you know if it is heated once you will get something. So, based on that if you heat it once again, you know your output is going to be dependent on the previous value. So, this is an error and this is known as the hysteresis error.

(Refer Slide Time: 24:06)



There are different other errors, such as quantization error which is basically if the sensor has a digital output, the output is essentially an approximation of the measured property and this is known as the quantization error. If you are sampling the signals, this leads to a type of error which is known as aliasing error and the sensors may at times be sensitive to the properties. Then, the property that is being measured for example, a temperature sensor might also sometimes be sensitive to few of the other things that are not directly being measured, maybe you know the humidity or pressure at times or maybe light, this will depend actually I mean this is not a perfect example that I have given you. So, it can be constitute, this particular error can be constituting this way that sometimes the physical property that is being measured that may get affected, that sensor may get affected by few of the other properties that are not directly being measured. So, this also leads to some kind of error.

So, with this we come to an end of the topic of sensors. So, here we have already seen that there are different types of sensors and I have shown you some real life sensors that can be used for building of internet of things. I have also shown you pictures of many other sensors and these sensors are used in something known as the sensor nodes. The sensor nodes are eventually going to get connected, they are not going to be networked together, internetwork together and together that is going to form an internet of things and this internet of things is going to be used for improving the overall service quality in the society of the business of the environment as a whole.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

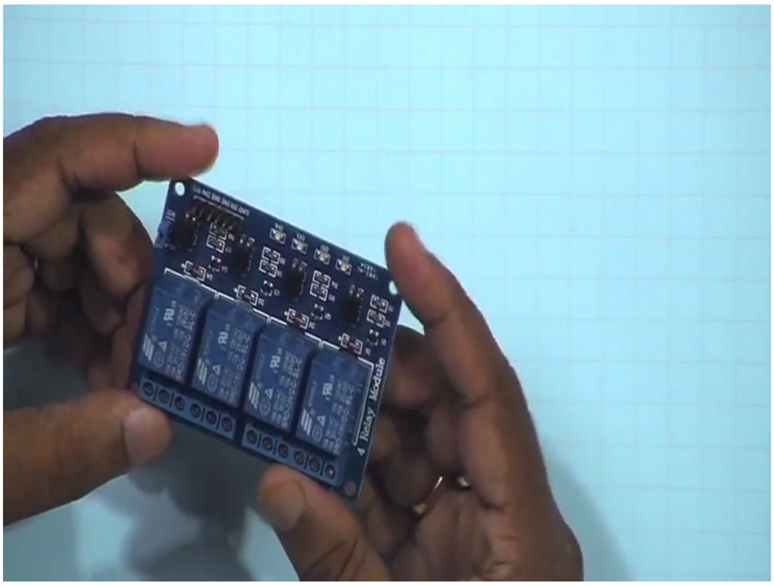
Lecture – 04
Actuation

So, this particular lecture is on actuation. So, based on the readings of the sensor, we have already seen different types of sensors in the previous lecture and based on the readings of these different types of sensors, some action might be required to be taken and that is done by actuators. These actuators basically perform certain actions on the environment on another system on a device and so on.

So, there are different examples of actuators. I am going to show you a different type of actuators very shortly, but these actuators, they can have principle of working principles which are based on electronics, then electrical, then you know mechanical systems and so on. So, they basically you know use some kind of control behavior, some control signals are sent. So, this is how these actuators, they perform.

We are going to go through the different mechanisms behind the functioning of these actuators in this particular lecture.

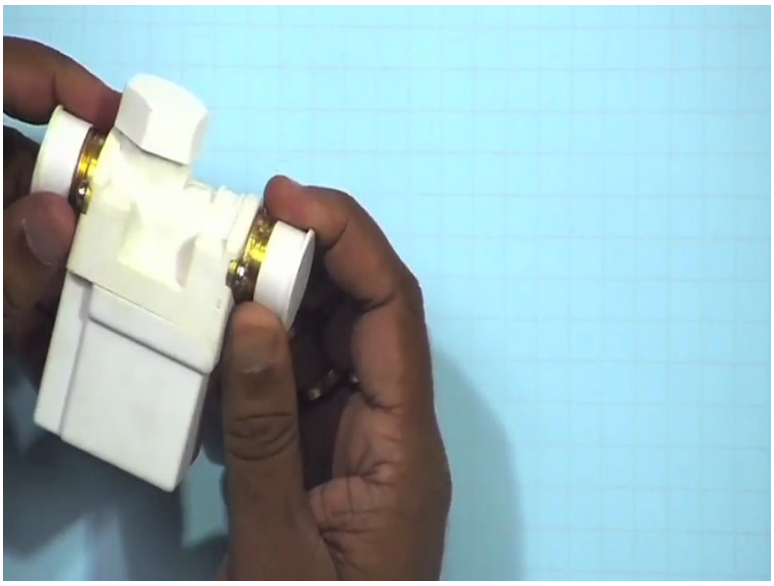
(Refer Slide Time: 01:37)



Before we proceed, I wanted to show you at the outset some of these actuators that can be used. So, here is an example of a sample actuator which is known as the relay switch. So, this relay switch, it is an electromechanical switch which can be used to switch between AC and DC for instance or different other things can be performed. So, the sensor networks, the sensor nodes, they typically operate in DC and based on the sensed value maybe you know you want to switch off the electricity in your room or at your home based or maybe something, maybe fire has been detected by the sensor network, then you want to do something or you want to turn off the power in your home.

So, that is AC that operates on AC, right. So, this particular switch, this electromechanical switch will basically turn off AC that the power supply at your home. This can help in doing it. So, this is an example and this is known as relay.

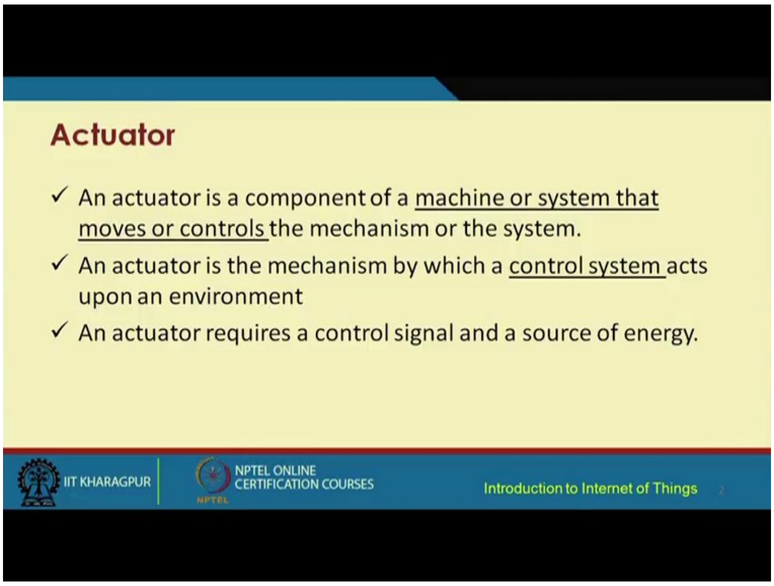
(Refer Slide Time: 02:50)



There is another one which is the solenoid valve and this basically can help in controlling the flow of liquid. So, you have an input; you have an output. So, we have an input, we have an output and the solenoid valve if we open it, so what we can see over here is what is inside. So, you know water can flow in and depending on the conditions, this valve is going to either allow the water to flow out or it is going to stop. It is not going to allow.

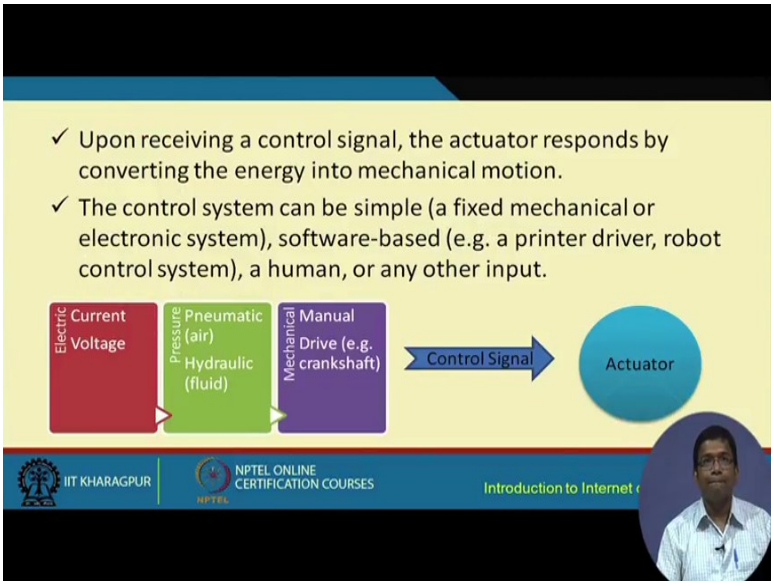
So, this is another actuator. Like this there are different actuators that are available for use in IoT. So, having seen some real life actuators, let us try to understand the basic principles of actuators, but before that let us go through some of the basics.

(Refer Slide Time: 03:52)



So, an actuator is a component of a machine or a system that moves or controls the mechanism of the system. So, typically these actuators are based on some control system and these control systems, they act on the environment. So, an actuator basically requires some kind of a control signal and a source of energy for their functioning.

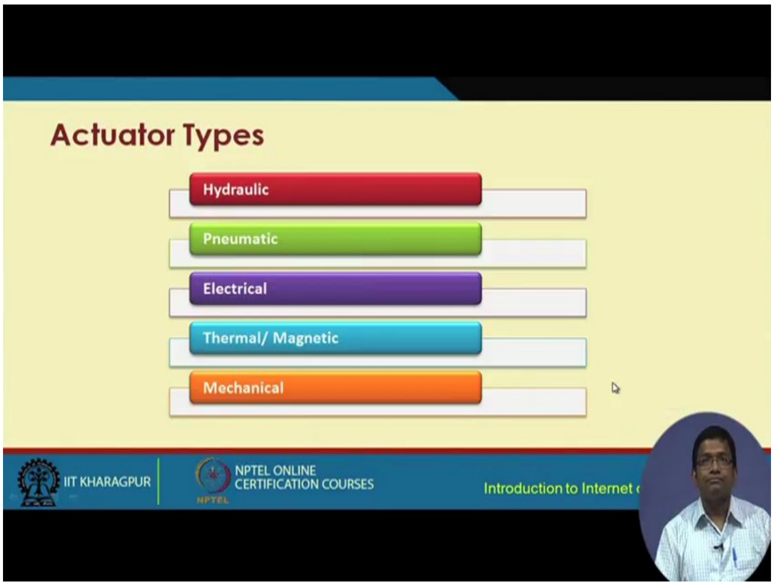
(Refer Slide Time: 04:28)



So, typically I said that control signals are required for the actuators. So, when these actuators receive a control signal, they respond by converting that energy into mechanical motion. Some mechanically something is going to be done. This is an example of course. So, they convert that electrical signal, some control signal into mechanical motion and that control system can be simple which can be based on some mechanical or electronic system or it can be software based like a printer, driver, robot, control system, a human or any other input.

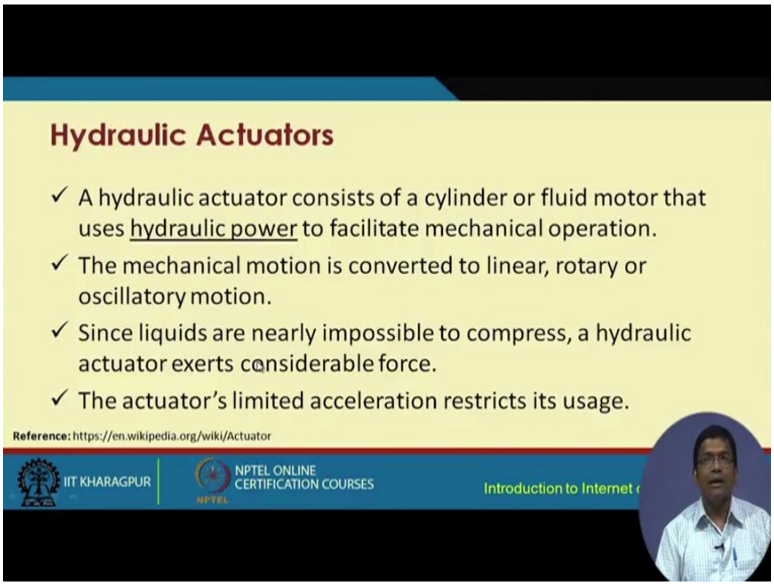
So, what we have are three types. Three types of actuators, one of actuators, one is these electric based actuators. We have this pressure based actuators and we have these mechanical based actuators. Each of these, they send control signals and based on that the actuation is going to be performed.

(Refer Slide Time: 05:33)



So, we have hydraulic actuators, pneumatic actuators, electrical actuators, thermal actuators, magnetic actuators and mechanical actuators.

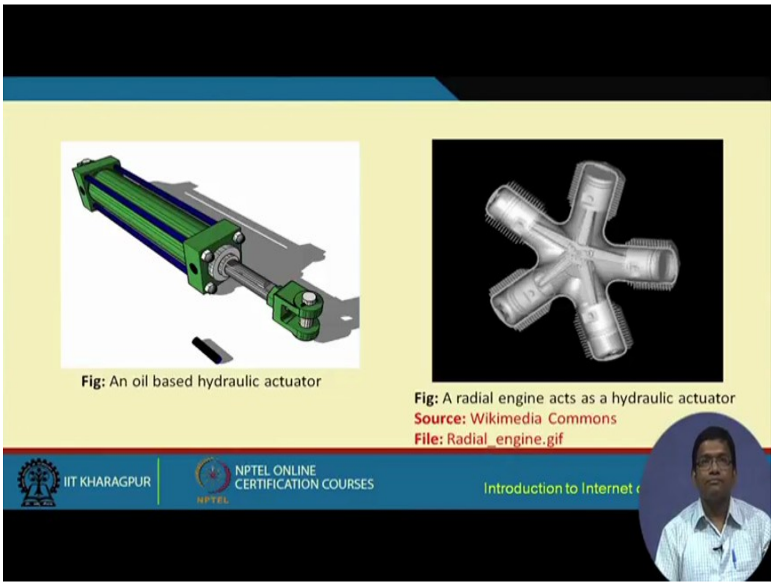
(Refer Slide Time: 05:44)



So, this name suggests, these hydraulic actuators consist of a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation. The mechanical motion is converted to linear rotary or oscillatory motion.

So, basically you know when some fluid passes through, then you know that motion is converted to some linear motion or some oscillatory motion or rotary motion and since liquids are nearly impossible to compress, most of the hydraulic actuators basically exert considerable force. So, that is the reason why liquid based actuators are typically used you know. So, these are quite popular because of this particular reason.

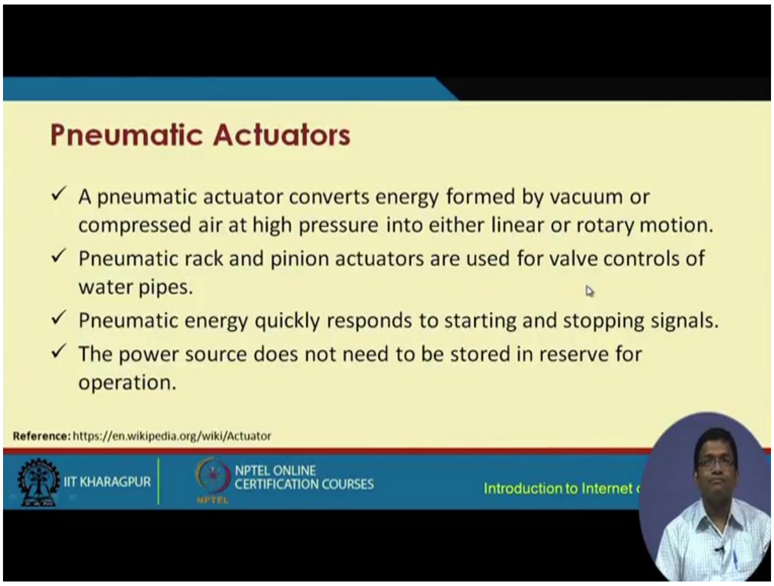
(Refer Slide Time: 06:36)



On the left hand side, we see an example of an hydraulic actuator which is based on the use of oil. So, in this particular cylinder, oil will be there and then, when you put, when you apply pressure on it, it is going to give an output based on which there can be some linear motion or some oscillatory motion or rotatory motion or whatever that can be performed.

So, here on the right hand side, we see over here a figure which shows an hydraulic actuator based an hydraulic actuator, based on radial engine. So, as we can see over here, this is quite. This animation is quite. You know it is quite explanatory. So, as we can see over here you know liquid goes inside and when you synchronize the liquid going inside from these different directions, then what happens is you can emulate a rotatory motion like this. So, this basically can help in the functioning of an engine. So, it can give a rotatory motion in this manner.

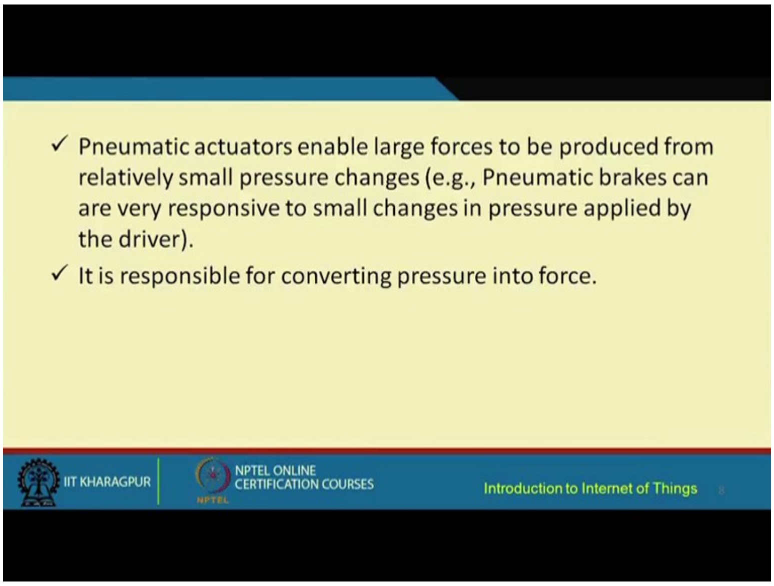
(Refer Slide Time: 07:51)



So, those were the hydraulic actuators. Pneumatic actuator, pneumatic means air based. A pneumatic actuator basically converts the energy formed by vacuum or compressed air at high pressure into either linear or rotatory motion.

So, you know the rack and pinion actuators are typically the pneumatic actuators and these are used for valve controls of water pipe, water pipes. Pneumatic actuators basically exert a lot of force and for example, the pneumatic brakes can be very responsive to small changes in pressure that are applied by the driver.

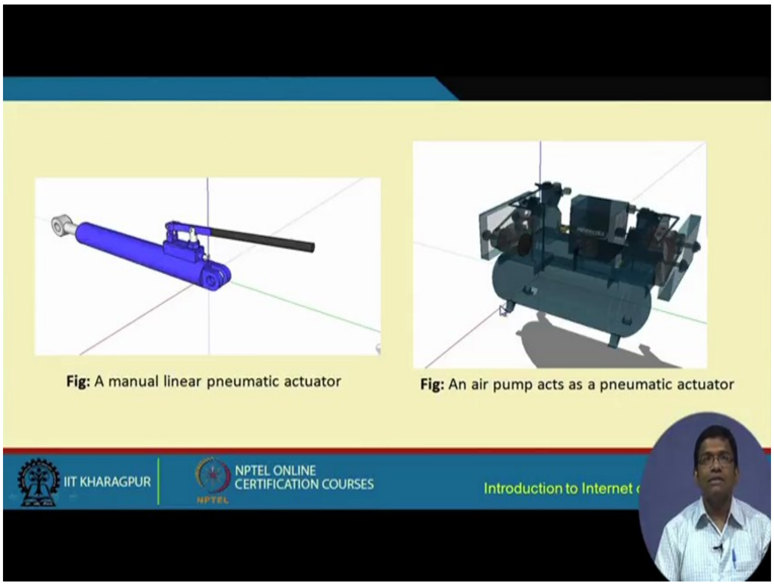
(Refer Slide Time: 08:22)



So, pneumatic brakes are quite common in different like trucks etcetera. They use pneumatic brakes. So, hydraulic brakes are more common in cars, in trucks. The pneumatic brakes are quite common.

So, these pneumatic brakes, the advantage is that they are very responsive to small changes. You know if the action, if the brake is pressed little bit, you know they become, they act quite fast. This is an advantage of these pneumatic actuators. So, basically what happens is the pressure that is put on the brake that is converted into force pretty fast. So, this is one of the advantages of these pneumatic sensors.

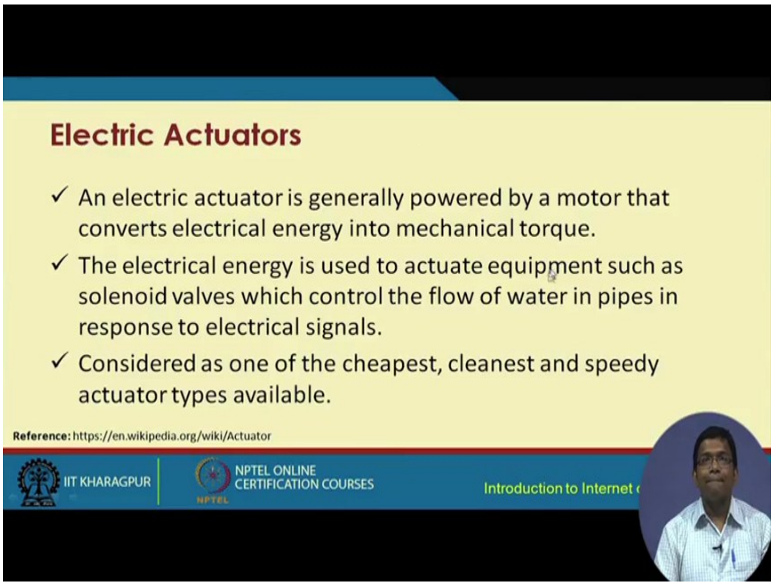
(Refer Slide Time: 09:16)



So, here is a figure of a pneumatic sensor when you apply pressure over here. So, this shaft, this crankshaft or this shaft will move and this is an example of a pneumatic actuator.

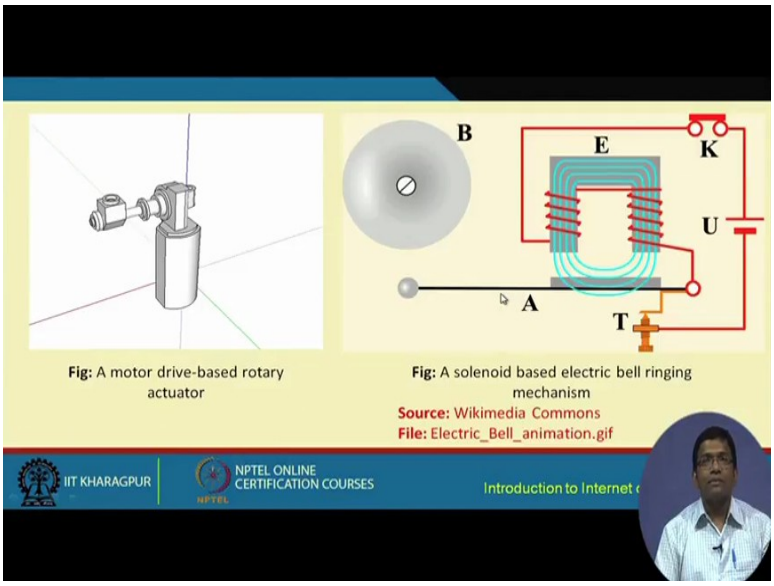
So, basically this is a figure which shows an air pump acting as a pneumatic actuator and then, we have seen hydraulic actuators, we have seen pneumatic actuators.

(Refer Slide Time: 09:40)



Then, we have the electric actuators. An electric actuator is generally powered by a motor that converts electrical energy into mechanical torque. So, this electrical energy is used to actuate the equipment, such as the solenoid valve which control the flow of water in pipes in response to electrical signals and this is what I was showing you at the outside. I showed you one of the actuators. The solenoid valve I had shown you and this basically works on the principle of electrical actuator.

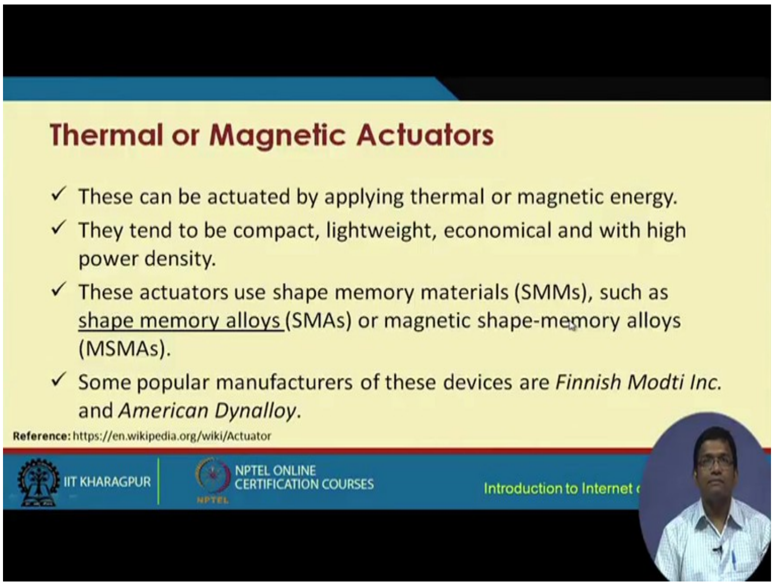
(Refer Slide Time: 10:19)



So, on the left hand side is a figure showing a motor drive based rotary actuator. So, basically you know what happens is this basically you know the electrical signal over here will help in moving this. So, it is going to give a rotary motion of this particular part. So, this is an example of a motor drive based rotary actuator. Here in this particular animation what you see is an electric, the functioning of an electric bell. An electric bell is an example of a solenoid based actuator.

So, as you can see over here once the bell is pressed, then the connectivity is established and then, the electromagnetic field is generated due to which the bell sounds and this is the way in which solenoid based electric bells functions. So, these are two examples of electrical electrical actuators.

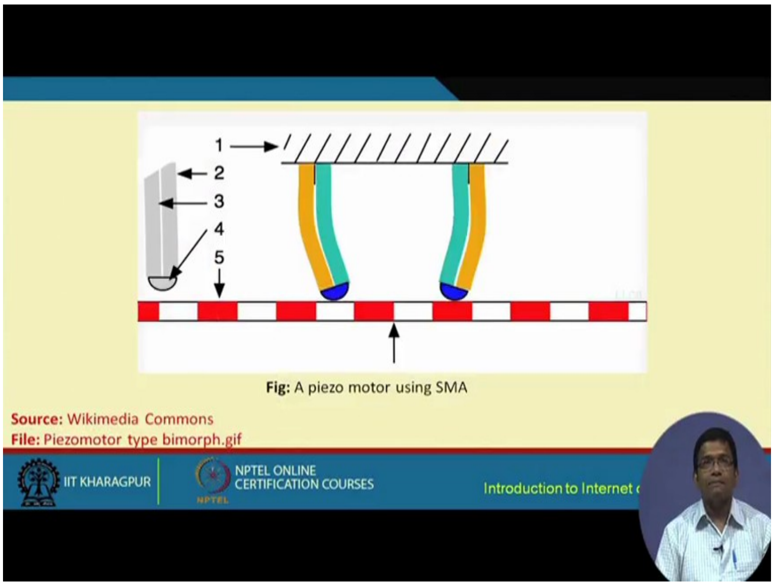
(Refer Slide Time: 11:39)



Then, we can have thermal or magnetic actuators which can, so thermal or magnetic actuators, these can be actuated by applying thermal or magnetic energy and typically, they are very popular because of being that they are very compact, lightweight, economical and with high power density.

So, these active actuators use shape memory materials or shape memory alloys SMAs and this is very popular at present.

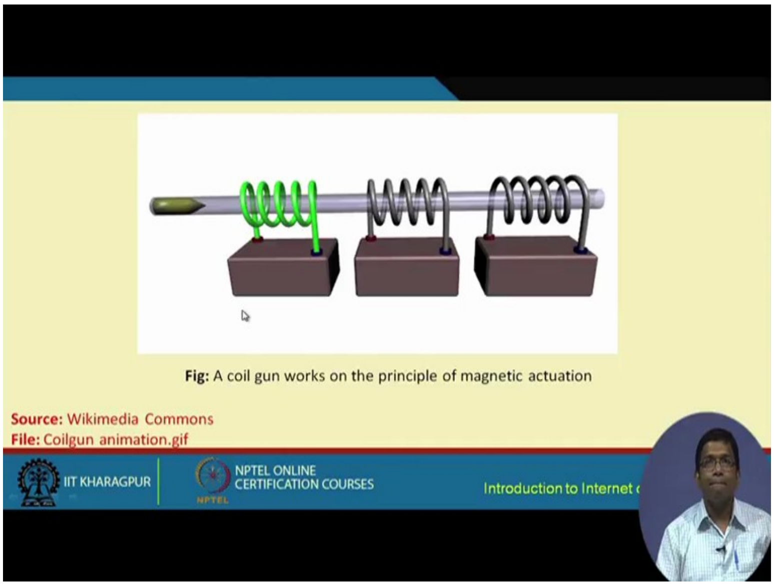
(Refer Slide Time: 12:12)



So, this is how it works. So, this is an example of an SMA based piezo motor. So, as you can see over here, these are the different steps in which it works. So, these are two metal strips and when you know when the energy is passed through it, they bend and when they bend, they basically move this red and white strip mechanically. So, this basically acts as an actuator.

So, this is like a joint metal bar and this is like this, sorry. So, when you heat this metal bar, this is an alloy bar consisting of two metal strips. So, you know the property is that when you heat it, then it is going to bend and when it bend, it is going to move this particular strip in this manner. So, the different steps are shown over here and this is quite evident, it is quite explanatory from these steps.

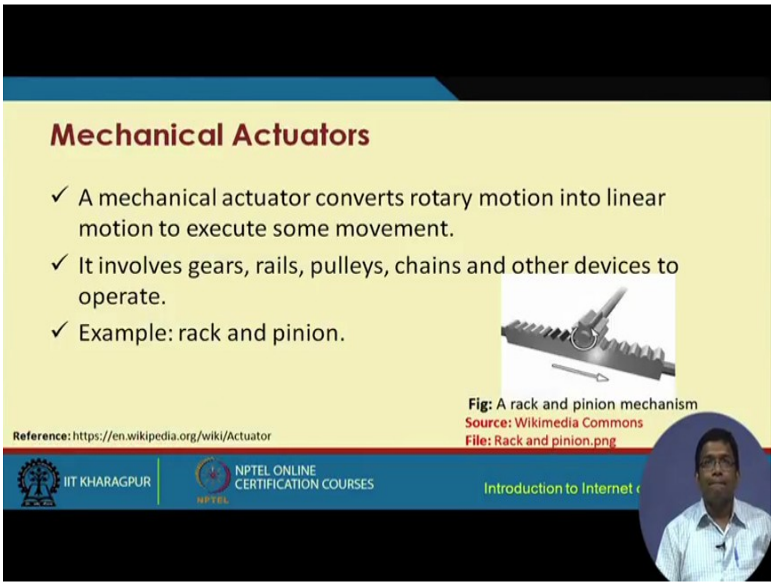
(Refer Slide Time: 13:30)



So, this is an example of a coil gun which basically works on the principle of magnetic actuation. So, this is also quite explanatory. So, this coil gun you know. So, basically you know electromagnetic field is generated and then, you know again it is pushed and so on.

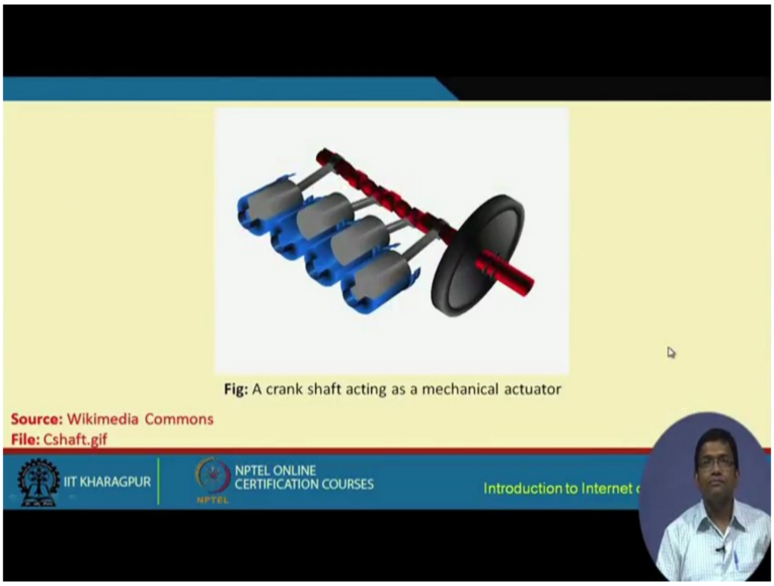
So, basically you know functioning of the hyper loops, at present people are talking about hyper loops, right. So, presenting if the functioning of the hyper loops are also you know based on this particular principle.

(Refer Slide Time: 14:05)



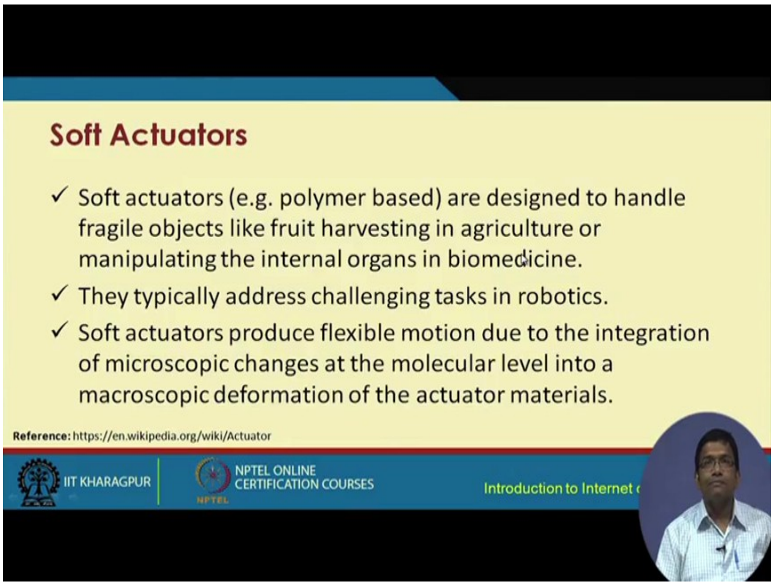
Then, we have these mechanical actuators which basically converts rotatory motion into linear motion to execute some movements. So, this basically involves these gears, the pinions, gears, pinions rails, pulleys, chains and other devices to operate. So, rack and pinion is an example of a mechanical actuator. The figure shows it and it is quite exponentially from this.

(Refer Slide Time: 14:34)



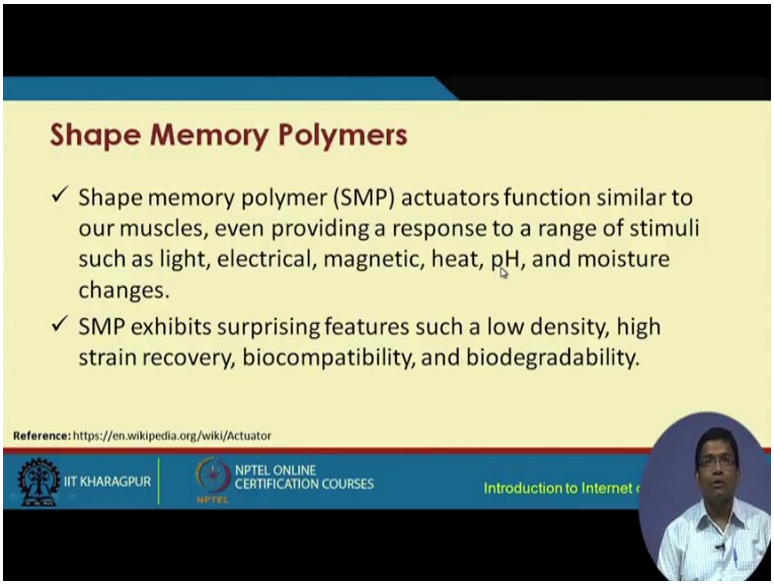
So, as it moves, basically this also moves. So, a crankshaft is another example of a mechanical actuator. So, this is how the crankshaft works.

(Refer Slide Time: 14:54)



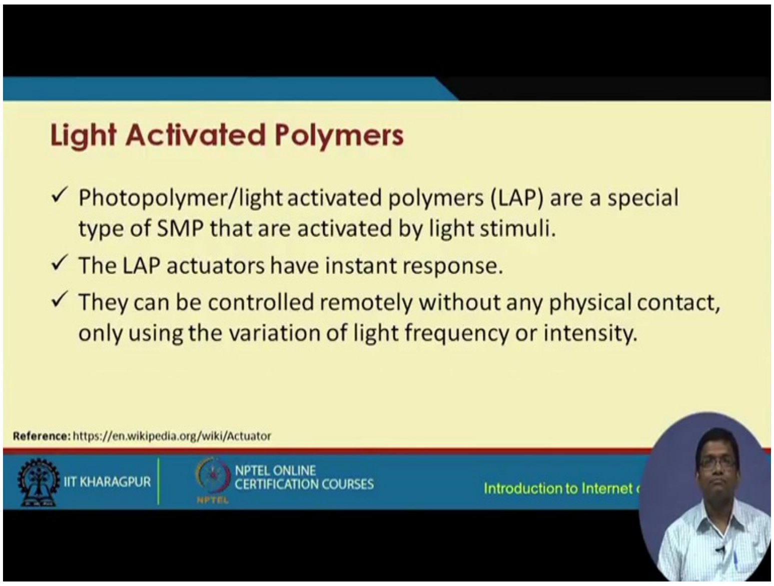
So, as this thing moves in this manner, so this gives this one a mechanical motion, a rotatory motion. There are different soft actuators which are actually polymer based and the design to handle fragile objects like fruit harvesting in agriculture or in biomedicine, handling internal organs of human beings and typically these are used in robotics. So, soft actuators are also quite popular.

(Refer Slide Time: 15:16)



These basically use something known as SMP, the Shape Memory Polymers which are actually polymers and the behavior of the polymers will change depending on the stimuli. The stimuli for these polymers are the light, electrical signals, magnetic signals, heat, PH etcetera. They have different properties. These polymers, they behave differently due to these different variations in these physical properties.

(Refer Slide Time: 15:43)



Then, we have the light activated from polymers. These polymers basically get activated through light stimuli and these are also quite popular. So, what we have seen are different actuators, their actuation principles and different diagrams and figures of them and at the outset, we have already seen some real actuators that can be used for building IoT based systems.

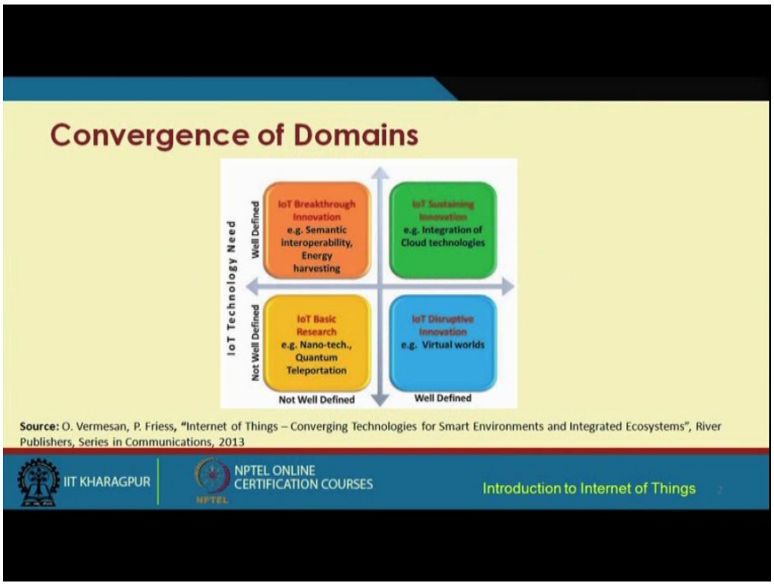
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 05
Basics of IoT Networking-Part-I

In this lecture and a subsequent few, we are going to go through some of the basics on the networking aspects of Internet of Things.

(Refer Slide Time: 00:35)



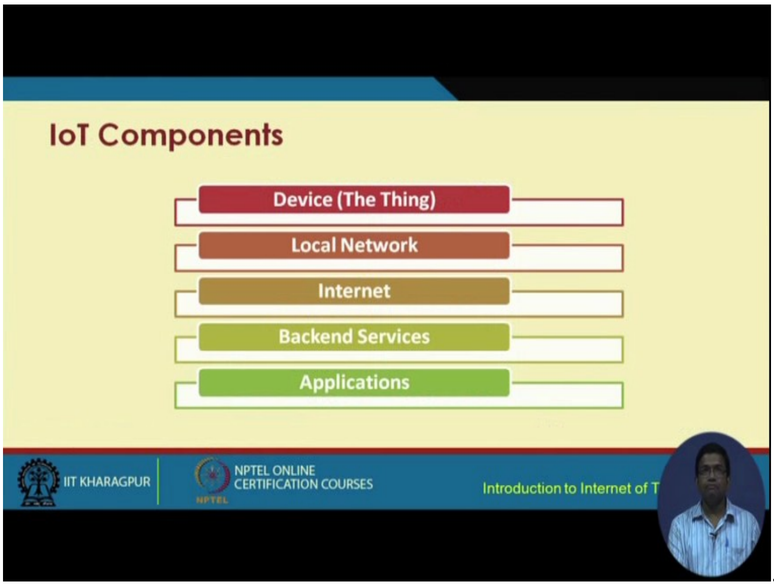
So, the first thing that we need to understand is that IoT has evolved a lot. So, starting from basic research, basic fundamental research and innovation, there has been different other types of innovation which are done through, which are disruptive, and some of the other innovations which are sustaining in nature. So, in terms of basic research, there has been a lot of research on the nanotechnology, the use of nanotechnology, the use of quantum teleportation. Quantum teleportation basically means that how the different information at the atomic level is sent from one point to another.

So, it is transported from one point to another at the atomic level and nanotechnology, it involves things like nano IoT, nano nodes, nano networking, nodes, nano sensor nodes and nano networks. That means, at the nanoscale forming a network which can be for different purposes, nano networks are used for different purposes in the human, inside the human body at the molecular level nano networks can be used. So, like this at the nanoscale and for quantum communication, there has been lot of advertisements that has been done for involving basic innovations, basic research innovations.

So, this is one likewise for semantic interoperability. There has been lot of research on semantic in for interoperability. For example, let us see that a temperature sensor, it might be given the data as temp, another temperature sensor as temperature, another temperature sensor the third one. So, there has to be interoperability between all these different collisions, but they are all different to the same temperature, right. So, this is basically taken care of by things like semantic interoperability. There has been lot of research on this one, this particular aspect then energy harvesting. Again there has been lot of research, you know energy harvesting through different renewable sources such as wind energy, solar, etcetera. How these can harvest, you know how these deferent renewable sources from these how energy can be harvested to power the different nodes and IoT, these are very small powered you know small sized nodes with very limited power.

So, energy harvesting is very crucial. It plays a crucial role in the sustenance of these networks. So, there has been lot of work on this one also and this has been like you know these aspects for example, there has been lot of brick through innovation on these. Then, disruptive innovation for example virtual reality, augmented reality you know. So, these are all like you know involvement of these incorporation into the IoT network, there has been lot of research on this particular front and things like cloud big data, these are like sustaining technologies for IoT. Again there has been lot of work on these technologies as well.

(Refer Slide Time: 03:59)



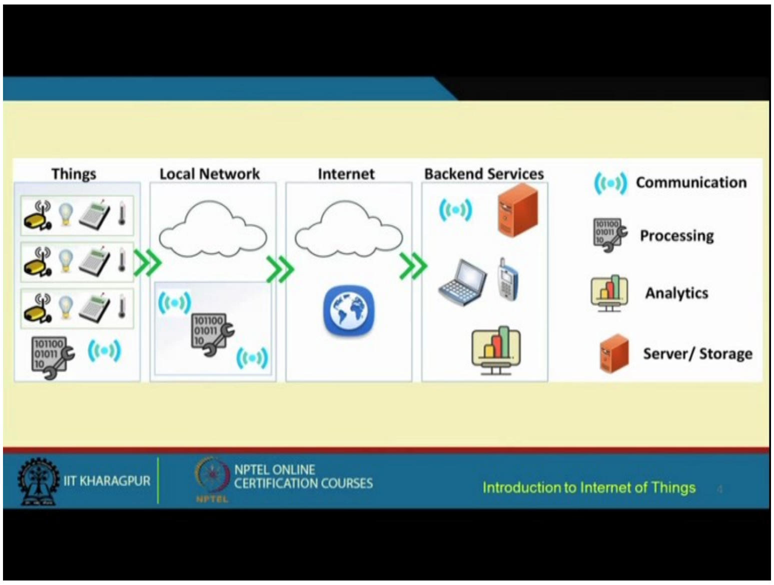
Now, when we talk about IoT, if we think about IoT, what we have? We have these different things which as I said in one of the previous lectures is these things are fitted. These are basically physical objects once again. So, these physical objects are fitted with different sensors and these sensors basically sense different physical phenomena that are occurring around them.

So, these sensor fitted things, sensors actuators and different other emirate devices, these are one component of the IoT, but these become different nodes in the network, these are the individual nodes in the network. So, then what we have is, these nodes they have to communicate with one another and the information that is sensed by one of these sensors fitted to these nodes, this information from the sensor and the other sensors, these are taken and are sent to the other sensor nodes, the destination nodes. So, how is that turn? First this information has to flow through the local network and then, if the destination, intended destination is outside this local network, then it is sent through the internet.

Typically if we are talking about an IoT which is basically internet based IoT, then basically it is going to flow through the internet or some other wide area network and finally, it is going to arrive at the intended destination node and may be there can be some at that point, actually there can be some analytic engine which is running on some backend server, those could be there and from that point from the decision, from these analytics, they can run on these servers decisions about actuation could be made.

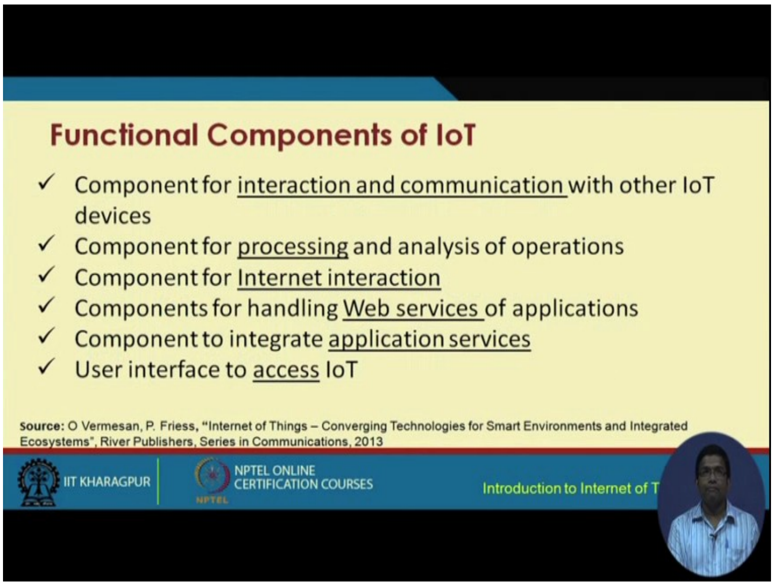
So, what we see is from sensors to actuators through the local area network, the internet involving you know backend services analytics which includes again some you know high end processing at different servers and different complex algorithms, execution of different algorithms which are based on may be machine learning neural networks and so on and so forth. These are all required. So, basically you know what happens is we basically can conceive an IoT as a very complex system involving sensors, actuators, networks, local area, wide area internet and different servers, different algorithms, machine learning and so on, all executing together to make the system function as as one single entity. So, going back we have in this local network as you are saying then we have the internet, we have the backend services and finally, the applications that I have been served.

(Refer Slide Time: 07:20)



So, these are the different basic components of IoT. So, this is the scenario that I was referring to earlier. So, what we have we are these different things. These things could be like you know different physical objects which are fitted with different sensors. These things could be telephones, lightning systems, could be cameras, could be different other scanner, sensors like the temperature sensor and so on and these things are able to communicate with one another with the help of wireless technologies like Zigbee, Bluetooth, WiFi and so on. So, as you can see that this wireless basically helps these different devices to talk to one another and this information from these devices, they will go through a local network and from a local network, they will go through the internet to you know these data are basically sent to the backend services involving different servers processors and so on and so forth. For running different analytics and then based on that different devices can be actuated you know may be a pump. This is an example that I gave earlier in a previous lecture basically for agricultural purposes. The use of IoT pump might be started might be actuated based on the data that is received from the sensor nodes and based on analytics are run at the different servers that are involved in the backend service processing.

(Refer Slide Time: 09:03)

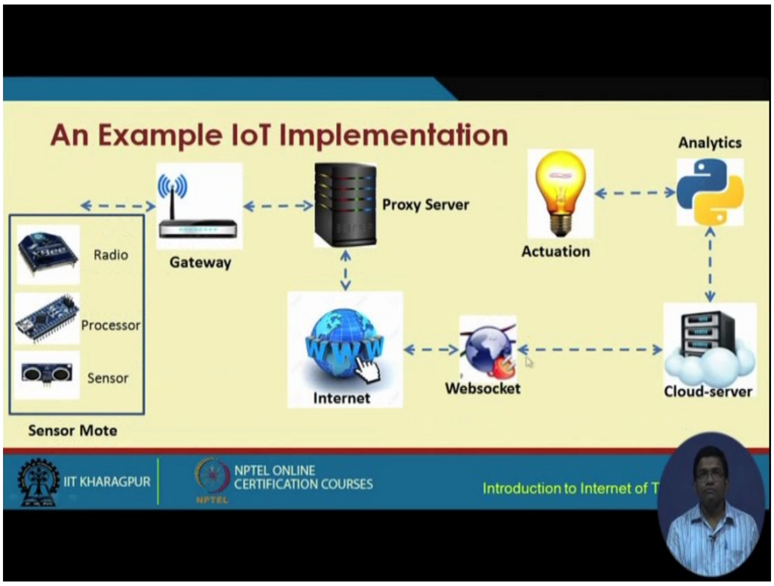


So, in terms of the functional components of IoT, one of the very important things is basically interaction. Interaction not only with the physical environment by this different sensors but also interaction and communication with the different devices, that means, a different nodes in the IoT in the IoT network, then comes the processing. So, processing and analysis of the different functioning and the operations that taken place, so processing of that data, the processing of operations, so this is another component, the third functional component is basically the interaction typically with the internet and because you know at present most of the times, the most of the IoT implementations are still using the internet. So, it is all you know internet powered IoT implementations.

So, internet interaction is one of the very important components of building IoT. Then, we have the web services, web services machine to machine communication and so on. So, basically what is going to happen earlier most, when you talk about a web technology, typically we are talking about human to machine communication, you know web service we are talking about you know some machine sending or some equipment basically sensing and sending that data to another machine for further processing or machine to machine communication is involved and offering different services. So, one machine offer some services to another machine and so on. So, this is basically you know this sort of thing in a IoT scenario is taken care of typically and then, we have the integration of different applications services and the user interface to access the IoT. That is another component.

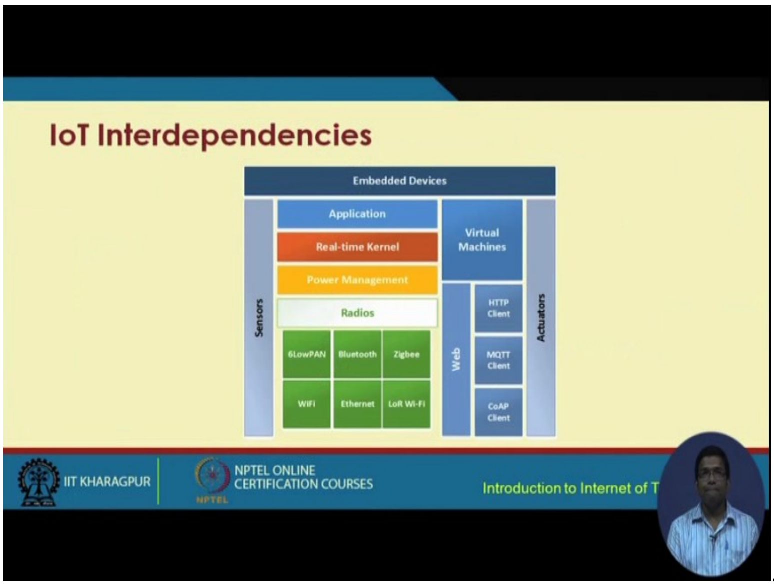
So, there has to be a user interface, a human interface to access the IoT network or the IoT you know mega network.

(Refer Slide Time: 11:17)



So, looking at this particular figure, I would like to try to clarify how the IoT implementation is typically done and it can be done to achieve different application needs. So, this is a figure which shows that we have different sensors, processors and radio. It refitted to each of these devices or the sensor nodes or the sensor motes or the IoT motes as you may want to call them. So, these motes, they talk to one another, but these different sensor nodes, they are basically within the jurisdiction or the domain of the gateway. So, the gateway is basically tasked to assign different locally unique addresses to these different nodes, to these different IoT nodes and the gateway basically takes care of the local addressing within that particular local area network. So, from the that point, all the data can flow through a proxy server if internet access is required. So, it will go through the internet, then a web socket and from the web socket, it goes through a cloud server. That means, this is where lot of analytics and backend processing takes place and based on that the actuation based on the analytics and the infer ant says that and run from the sensed data actuation of different devices can take place.

(Refer Slide Time: 12:56)



For example, lighting a particular lamp could be the actuation of that particular lamp. We have different interdependencies that are evolved in the implementation of IoT. So, if we look at IoT from another prospective or we have sensors, we have actuators and a bunch of other things that they are in between as shown in this particular figure. So, this is basically the entire spend of these different embedded devices.

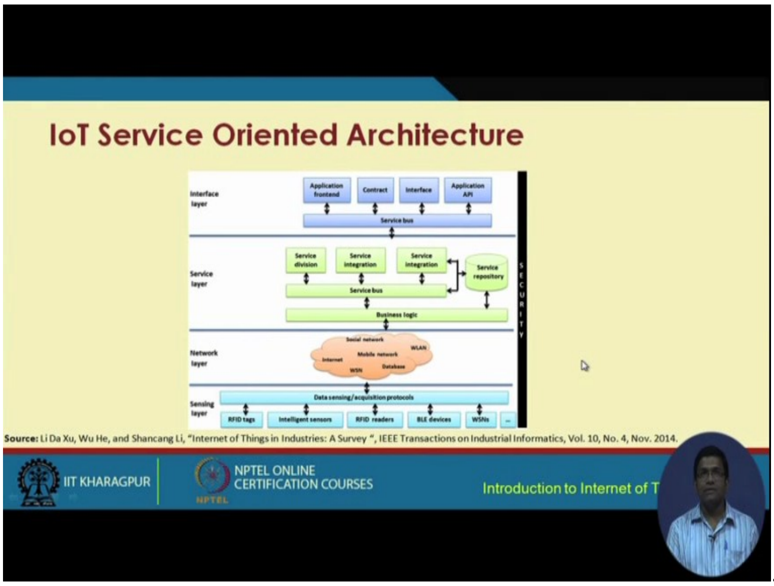
So, the sensors basically sense the data and that data is basically serving the application requirements and then, we have an operating system and a power management unit which basically you know does things like duty cycling of the sensors, how much the sensors you know how much time we are going to be active or how much time they are going to be in the sleep state, how to power them because these are very small sized you know, very resource staved sensors. So, basically the power unit in these sensor nodes, these are very small in size. So, basically consequently what happens is these embedded devices, they themselves are very resource staved.

So, we have a very power management unit which basically takes care of power management as a whole. How much power is required, for how long it is going to power, then what are the ways to harvest energy if at all it can be harvested and how much power consumption is going to take place at different points of time, can it be optimized different points of operation on and so on and so forth and as you can see over here, there after we have these different radios involving bluetooth, Zigbee, 6Low Pan, Wifi, Ethernet and low range basically wifi.

So, these are the different you know radios that can help in communicating the data that is sensed onward to other nodes. These basically different radio technologies can help for the communication purpose. So, alongside we also have things like virtual machines which takes care of the virtualization of the nodes, we have the web, we have you know different things like http client MQTT client, CoAP client. So, these are the once MQTT CoAP, we are going to talk next in the subsequent lectures. So, that will make our understanding clear, but these are like no different application level protocols that are used for functioning of these different IoT devices and finally comes the actuator verticals.

So, we have the sensors, we have different applications operating system, power management, radios, virtual machines web and then, we have these actuators all together which forms the embedded systems, the embedded devices.

(Refer Slide Time: 16:09)



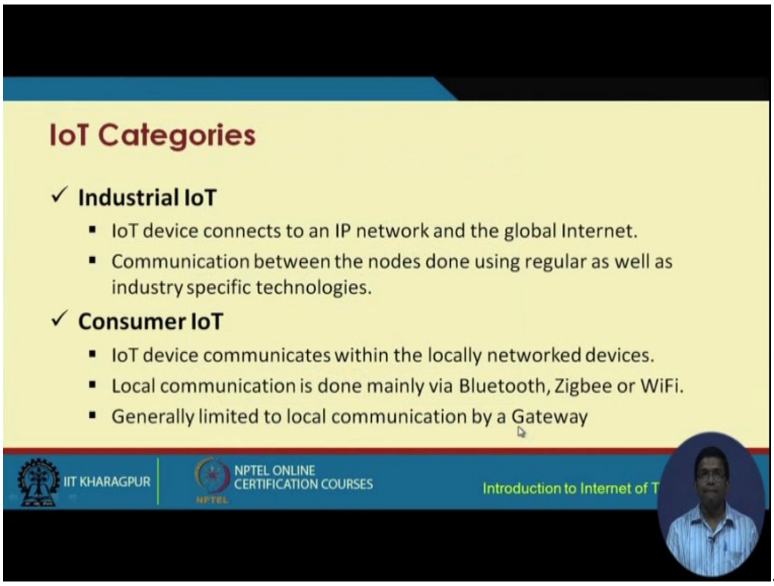
.

Now, let us look at the service orientation, the service oriented architecture of IoT. So, in the IoT if here what we have at these different layers, the sensing layer, the network layer, the service layer and the interface layer.

So, we have four different layers and as the name suggests, sensing layer basically takes care of sensing through different RFIF tags sensors and so on and so forth and then, data are sensed are acquired and so on are sent to the next layer higher up which is the network layer. The network layer basically serves sensor networks, social networks you know different other networks and data bases internet and so on. That is the network layer. Then, what we have? We have the service layer which deals mostly with the service delivery such as service, division service, integration service, repository service, logic by business logic and so on. So, all these different things that I involved with the offering of the services to support the business functions.

Then, we have the interface layer, we have the application frontend, we have a contract interface and application APIS. So, this becomes the interface layer and when we have the security issues which basically span all these different layer verticals, sorry layer horizontals.

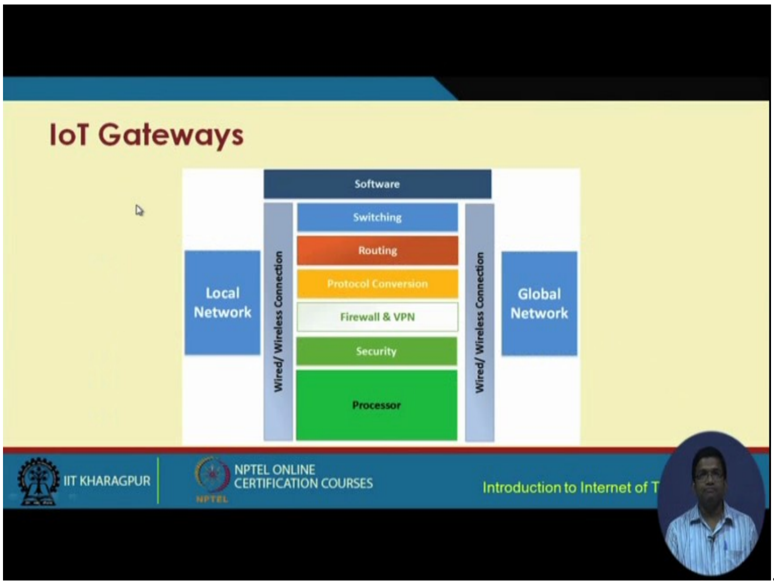
(Refer Slide Time: 17:50)



So, in terms of the categorization of IoT, it can be categorized into two. One is the consumer IoT which is what typically most of the people tempt to use and these are here, basically these different devices, they communicate with another through these local networks and it can be you know find a further communication can also take place over the internet as well depending on the requirements either local or through the internet. Then, we have the local communication which is typically done via bluetooth, zigbee or wifi. So, basically this local communication is constraint within the bounds or within the domain of the IoT gateway. So, this is consumer IoT. Then, we have the industrial IoT which is basically quite similar to the consumer IoT, but the application interest is in the industrial sector.

So, we are talking about manufacturing industries with different machines, with these machines are fitted with different IoT devices and they together become the IoT device. They have different sensors and so on feature are there which can node as a whole can communicate with other machines and so on. So, this becomes the industrial IoT and basically, there are different communication that takes place between the different nodes as well as different industry specific technologies. Now, we talk about IoT gateways.

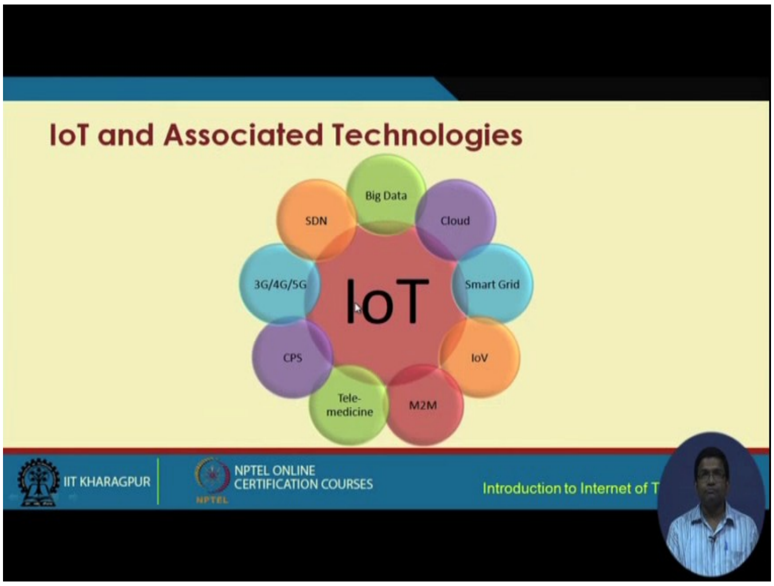
(Refer Slide Time: 19:25)



So, this is what I told you that in a local network, you have this locally unique addresses and that is they are within that local area network, IoT network.

So, these local addresses basically they take care of the addressing of the different nodes now. So, what are these gateways doing? So, the gateways basically take care of the addressing, but then in this is what the gateway structure looks like. So, this is what is here. So, we have the local network on one side of the gateway, we have the global network on the other side of the gateway and this is where the gateway, this is how the gateway looks like. So, the gateway has and functions different tasks such as switching, routing, protocol conversion, firewall and VPN services, security as a whole and processing. So, this is what a gateway does and the gateway with the local network and the global network communicate via the wired or wireless channels and so on.

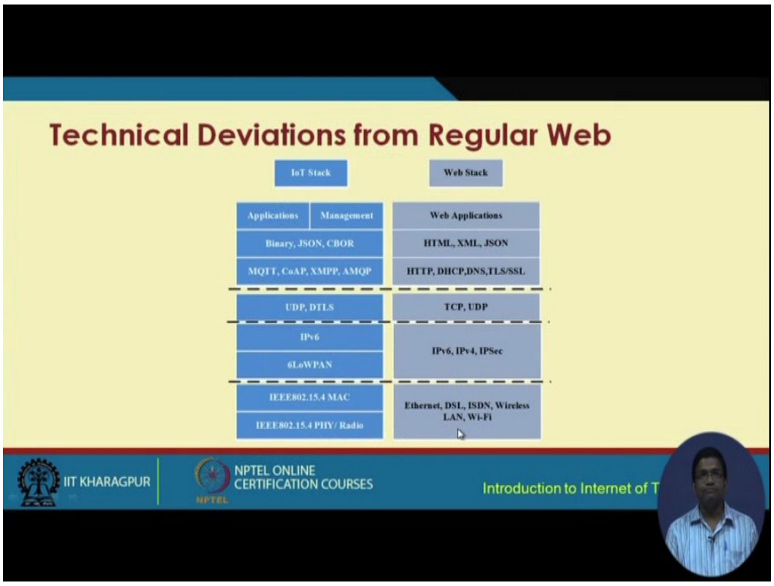
(Refer Slide Time: 20:46)



So, this is how the IoT gateways function different associated technologies of IoT involving big data, cloud, smart grid, internet of vehicles. That means, you know different vehicles on the road are fitted with different IoT devices which can communicate with one another and different intelligence about the route traffic conditions, about the offering different road side services can make possible with the help of internet of vehicles. Then, we have the machine to machine communication where one machine talks to another without any human intervention.

We have telemedicine offering you know offering health care services to the demote hospitals, demote health care centers and so on. CPS server physical systems, we have 3G, 4G, 5G, we have sdn and so on. So, these are the different associated technologies which together make IoT which together are used to deliver IoT solutions.

(Refer Slide Time: 21:47)



Now, you know if we try to make a side by side comparison between the IoT stack and web stack, we will see that more or less the application layers remain the same for both IoT as well as the web. So, conceptually these application layers, these different layers, communication layers and application layers that communication layers remaining the same between IoT and web, but what is different is that we have a new set of protocols that are used over here. So, the new set of protocols and additionally in IoT, unlike in the case of web things such as different types of management, management of the network, management of the power, management of different other resources, these are all additionally taken care of in the IoT node in the IoT stack which is not available in the case of the web and this is very much required because you know in the case of IoT, we are talking about heavily resource constraint nodes and this heavily resource constraint nodes basically required management, network management in terms of energy, in terms of processing, in terms of data and so on so forth.

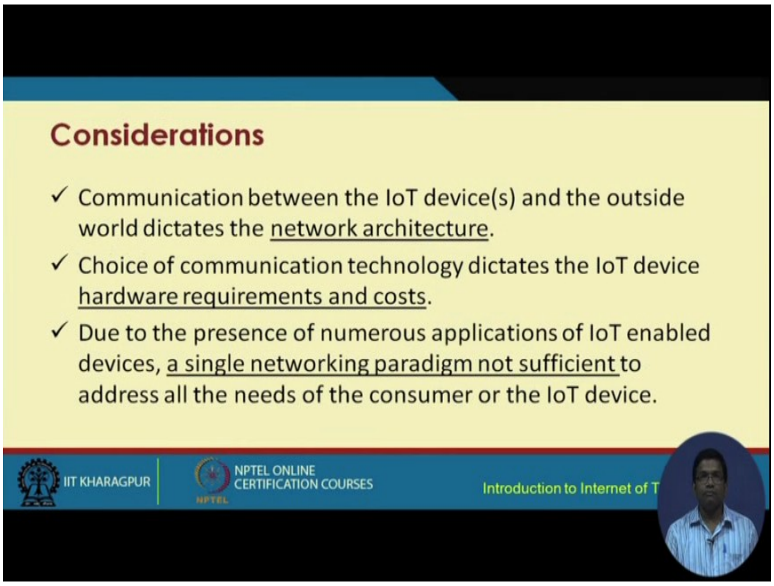
(Refer Slide Time: 23:13)

So, there are different key technologies that basically help IoT survive. We have the future internet knowledge aggregatio obtained through data assignation, data collection processing and analysis. Then, we have different standards, we have sensor networks, we have communication, we have cloud computing, we have discovery services, nanoelectronics embedded systems, software system integration and last, but not the least what is this over here on top is the security on privacy issues. So, security on privacy issues are per amount in IoT because there are heavy concerns because you know we are dealing with resource constraint nodes with communication constraints, bandwidth constraints, processing constraints, energy constraints and so on. So, these nodes become very much valuable to different type of attacks, different types of security breaches and also because IoT systems are very much detailed intensive, there is lot of information that frozen through the network as a consequence of which the privacy of the individuals of the organizations might be at stake. So, security and privacy and trust also which is not mentioned over here, these are very much important to power IoT technologies. There are different types of challenges, securities, scalability, energy efficiency, bandwidth management, interfacing interoperability.

(Refer Slide Time: 24:39)

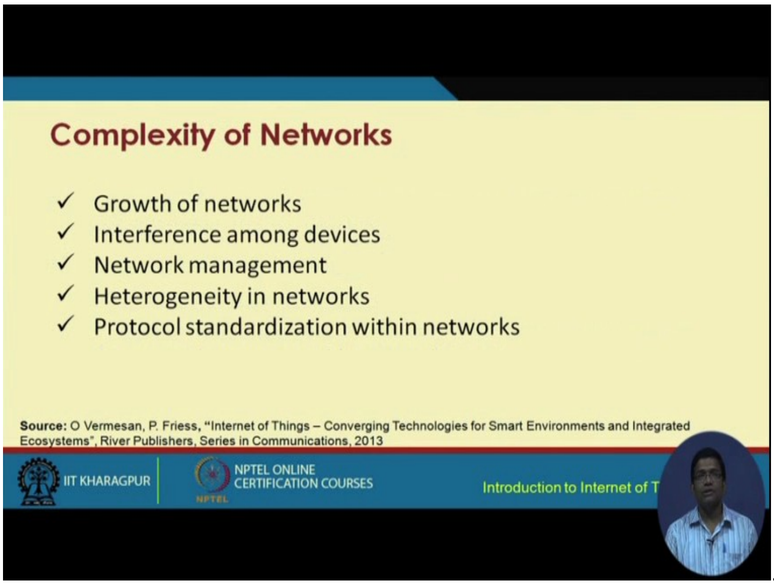
So, when we are talking about interfacing, it is typically we are referring to device interfacing. So, different you know one device talking to another device may be these devices do not belong to the same vendor, they are not running the same stack, they are not following the same standard and so on. So, then comes consequently then comes the interoperability issue. How to make these devices talk to one another? How different protocols, the different devices, the different algorithms, they are going to hand shake with one another? So, like this, this is another challenge which is typical of IoT implementations and then, we have data storage and analytics and complexity management with tools such as SDN. So, SDN basically helps in addressing the complexity of systems by decupling the control plane from the detect plane of the networks, different considerations and they are for building IoT. One is that will have a straight network architecture which can be used by different IoT implementations.

(Refer Slide Time: 25:40)



So, there has to be governing network architecture. Number two, hardware requirements and cost are important you know what type of communication hardware are going to be used and different devices in the costs that are involved and due to the presence of numerous applications of IoT enabled devices, a single networking platform may not be sufficient to address the needs of the consumer or the IoT device.

(Refer Slide Time: 26:23)

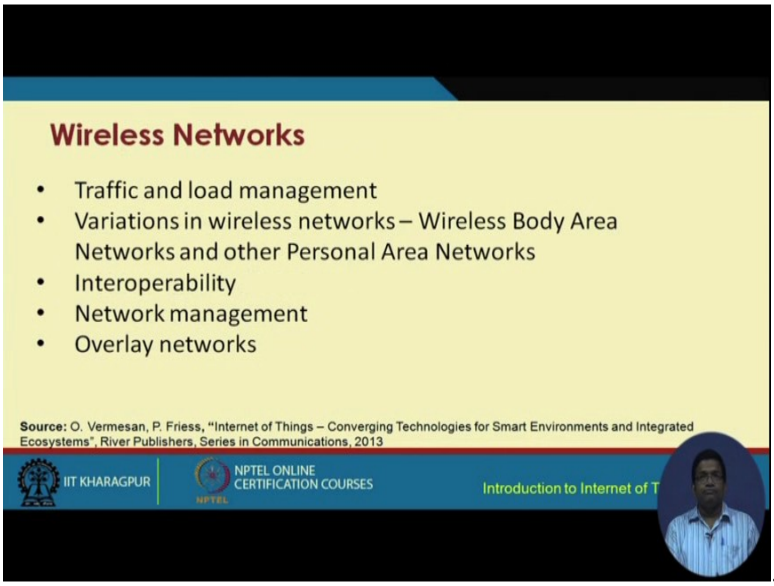

.

So, this is another. The third consideration that has to be taken into account while building the IoT systems, then we have the complexity of the networks. Uou know if the number of nodes in the network increases, then whether in the solution because if the system is going to be you know sustainable whether it can be scaled up or not, then we have interference among the different devices. This is very much vital in any network. Interference is a crucial issue and particularly IoT networks involve lot of large number of typically densely deployed nodes and these nodes as you know typically wireless power by wifi or bluetooth or zigbee and so on.

So, interference between these different communication between these different nodes that at the corresponding radios and so on is possible. So, how do you handle it? Network management as a whole as I was telling in earlier involving you know energy management, involving computation management, involving communication management, involving service management and infrastructure management and so on. So, network management as a whole then heterogeneity in the networks. Heterogeneity in terms of the devices standards the protocols, the algorithms and so on.

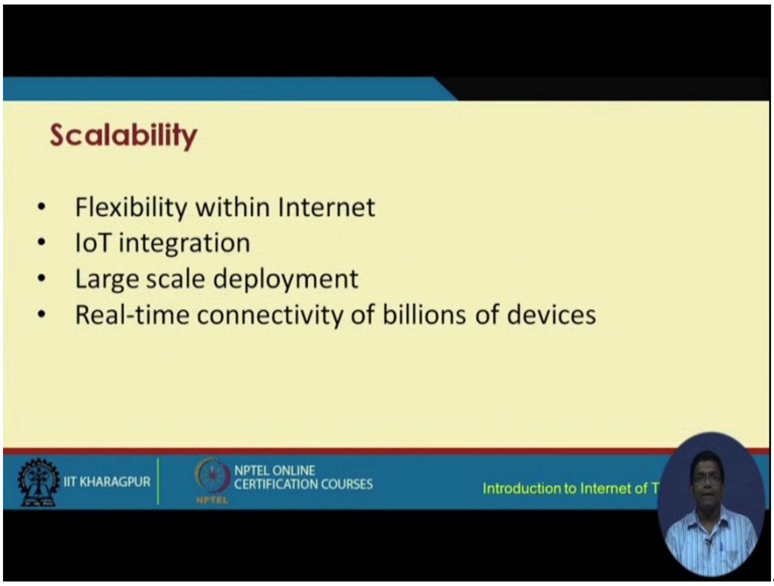
So, how do you handle because IoT devices unlike traditional internet, IoT networks come in different, you know come from different vendors, different devices coming from different vendors, different devices using different algorithms, these different protocols being used and so on. So, all these basically invite dealing with the issue of heterogeneity and lot of heterogeneity is involved. So, how heterogeneity is taken care of and protocol organization and standardization within the network, how the different protocols can be standardized, so that a device running one protocol can talk to another device and so on.

(Refer Slide Time: 28:30)



The different wireless networks are used issues such as traffic management, load management, then variations in the different wireless network forms for example, wireless personal area network, W turn versus wireless body area network, interoperability which I have already mentioned just a while back, then network management and overlay network. So, basically you know the overlay network takes care of some kind of a virtualization of the physical devices on you know and one type of this physical virtual devices and the networks and overlay is created, this is basically the overlay network.

(Refer Slide Time: 29:07)



Scalability is involving flexibility within the internet. Then, integration of different IoT devices, there are many manufactured using different standards may be in using different you know vender specific protocols. So, IoT integration is a very complex issue which basically dictates the scalability of the system, large scale deployment issues and real time connectivity of billion centurions of devices.

With this we come to an end of this lecture on the basics of IoT networking, but this is just a first part. We are going to cover many other issues involving the networking aspects of IoT in the subsequent lectures and from there, we can understand from this subsequent lectures, we can understand how forming an IoT is very complex, what are the different protocols, individual protocols that are how they are, may not be a single isolated or a single thread head. Let us say one protocol for IoT as a whole, but there all these individual protocols settled there. So, how that can be taken care of and for how can architecture be sent up between these different IoT devices manufactured by different vendors. So, like this actually there are different complexities that I have involved. So, we have really talked about that in the subsequent lectures.

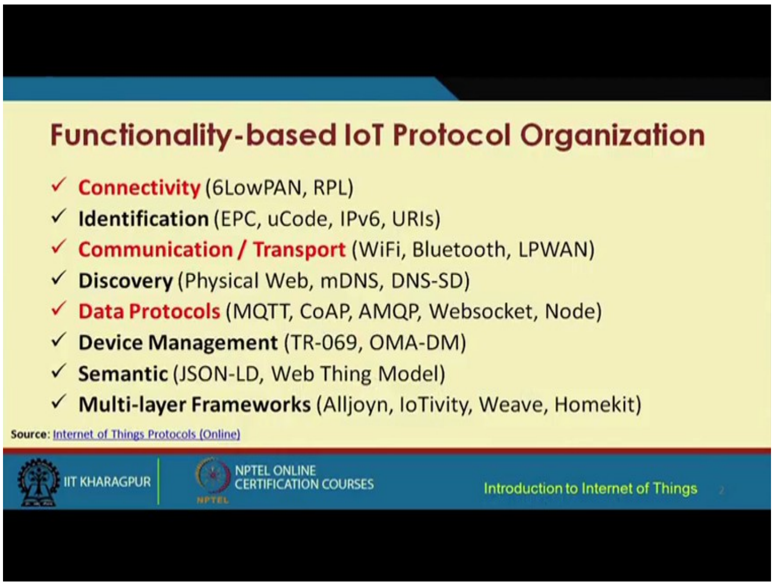
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 06
Basics of IoT Networking-Part-II

So, we are now going to continue our discussions on the basic issues, basic aspects of the networking in internet of things. So, we have already seen the different fundamental issues that are out there. Now, we are going to look at the different protocols that are there that can be used for something different purposes in IoT.

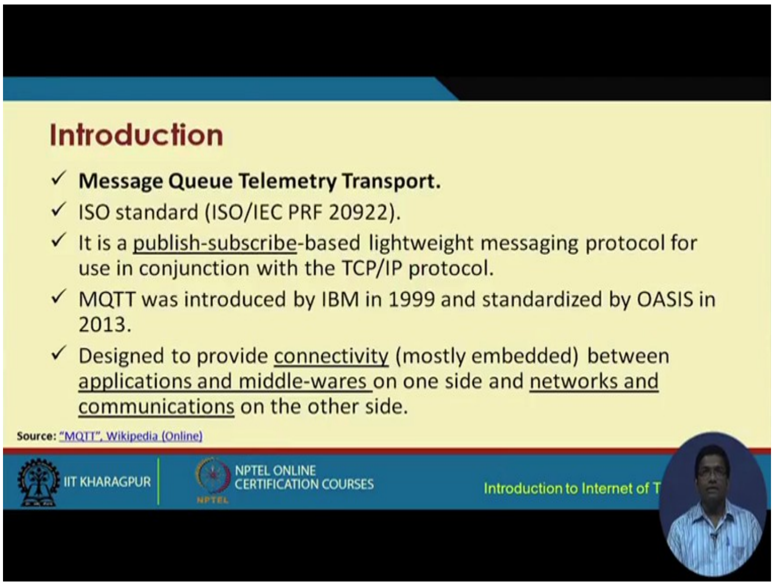
(Refer Slide Time: 00:44)



Now, based on the different functionalities, there are actually large numbers of protocols that are proposed for use in IoT. So, based on the functionality, these protocols are classified in this in this manner. So, this is just a classification that has been shown, but this is not unique classification in anyway and it should be constituted in that manner. So, this is just a classification attempt under different categories that is shown and here as we can see the different protocols for something.

These classifiers you know a different issues are also mentioned in brackets like this. So, it is basically not possible and also not required to go through all these different protocols. So, we have selected only a few protocols from this you know red coloured category and this is what we are going to discuss in this particular course.

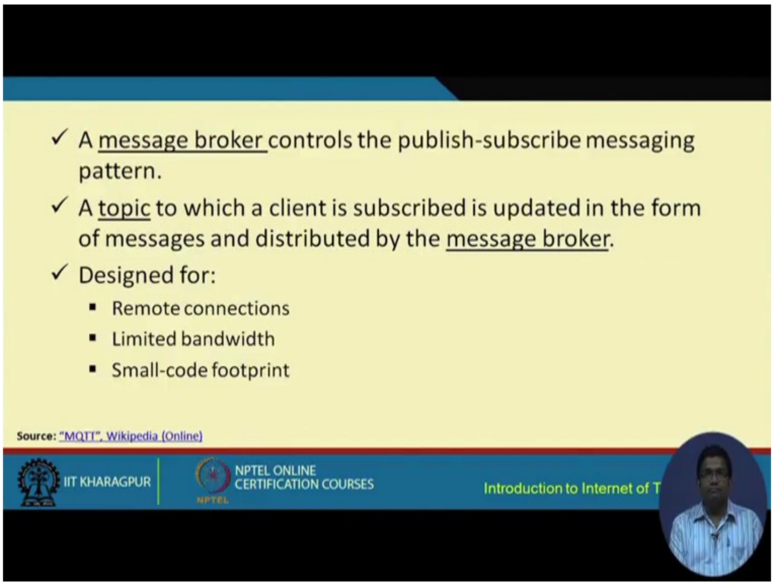
(Refer Slide Time: 01:55)



So, we will start with the MQTT protocol first and this MQTT, the full form of this is Message Queue Telemetry Transport. So, it is an ISO standard which is based on publish subscribe model. So, basically you know what happens is there is some kind of publishing of the data and then, the fetching of the data by the subscribers. So, this is how this publish subscribe model works and MQTT basically what it has done is, this publish subscribe model, it has been made lightweight through the use of this protocol, so that this lightweight protocol can be used in conjunction with the TCP IP protocol suit. This is what MQTT supports.

MQTT going back to the history was introduced in 1999 by IBM and is standardized in 2013 by Oasis. This is a standardization organization oasis. So, it has standardized in the year 2013. So, this particular protocol does couple of things. One is offering connectivity between different embedded devices between the applications and then, middle ware of one device and network and communication on the other side of the device. So, we have connectivity between applications and middle ware for one side and the networks and communication on the other. This is what MQTT does.

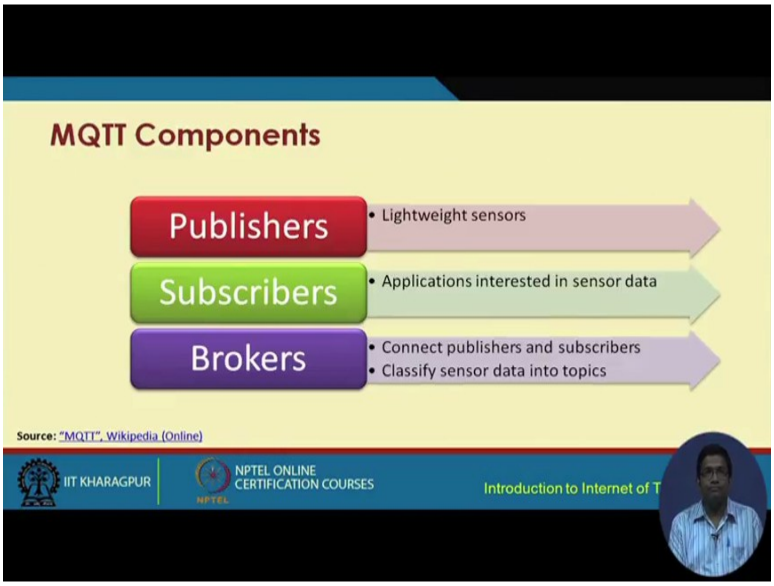
(Refer Slide Time: 03:32)



So, in MQTT there are three concepts that are involved. The first we are going to go through is the concept of a message broker and first, we are going to go through some of these concepts and there after I am going to show you pictorially how MQTT functions. So, we have a message broker; the concept of a message broker that basically serves like a broker which takes control of publishing of the messages and subscription of the messages. So, publish subscribe is basically controlled by the message broker, number 1. Number 2 is there is a concept of topic and this is what the client is subscribed and based on the updates. The data are sent to the clients by the message broker, this data are distributed by the message broker to the clients who have subscribed to the services.

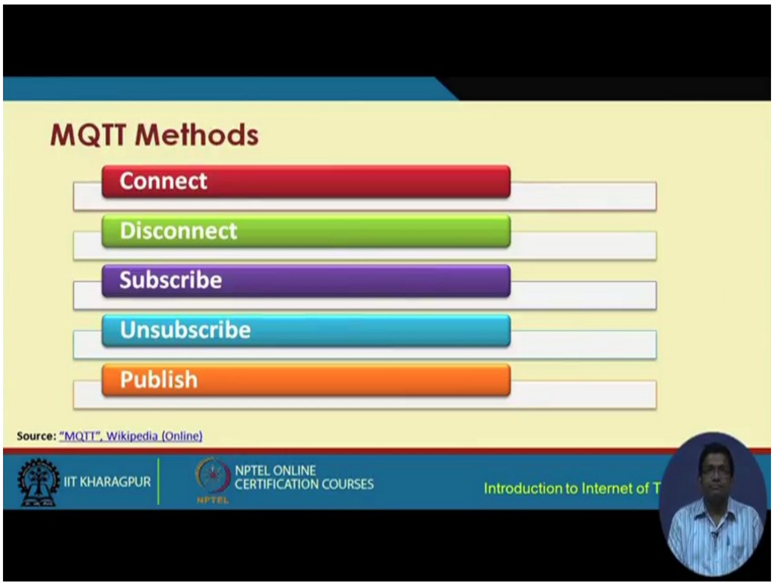
So, this is design for remote connections limited bandwidth environments and MQTT, basically the advantage is that it provides every small code foot print. So, basically you know by writing only a small piece of code, one would be able to achieve all these different functions that I have just mentioned.

(Refer Slide Time: 04:48)



The different components of MQTT are as follows. We have three principle components. The publishers which involve the different sensors, the subscribers and that means, those entities, those applications, those units that are interested in the data that is published by the sensors. Number 3 is the broker in between which helps the publishers and the subscribers connect to one another and also help in classifying the sensor data into different topics.

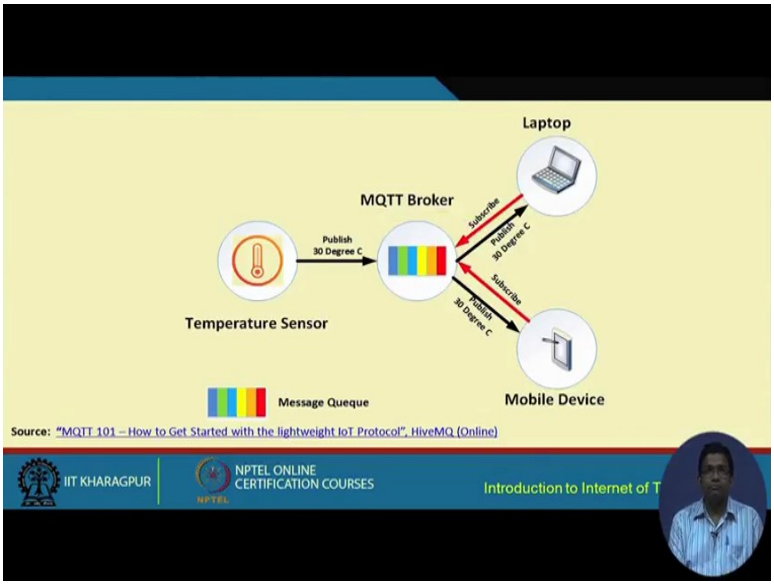
(Refer Slide Time: 05:29)



In MQTT there are a few different methods. One is connect, the second is disconnect, subscribe, unsubscribe and publish. So, basically the connect method helps to connect with the server, helps to connects this device with the server. Then, disconnect is the opposite. Whenever it is no longer required to be to remain connected, the disconnect method helps in disconnecting from the server from TCP IP service offerings and so on. And then comes the subscribe which is basically subscribing to the services and unsubscribe is the opposite that whenever it is no longer required to continue with getting the different data offerings, the data services and so on.

The unsubscribe method can be executed and then, we have the publish method which is basically publishing data for maybe you know publishing the data from these different sensors or these different devices to the broker for it to be fetched by the different application clients.

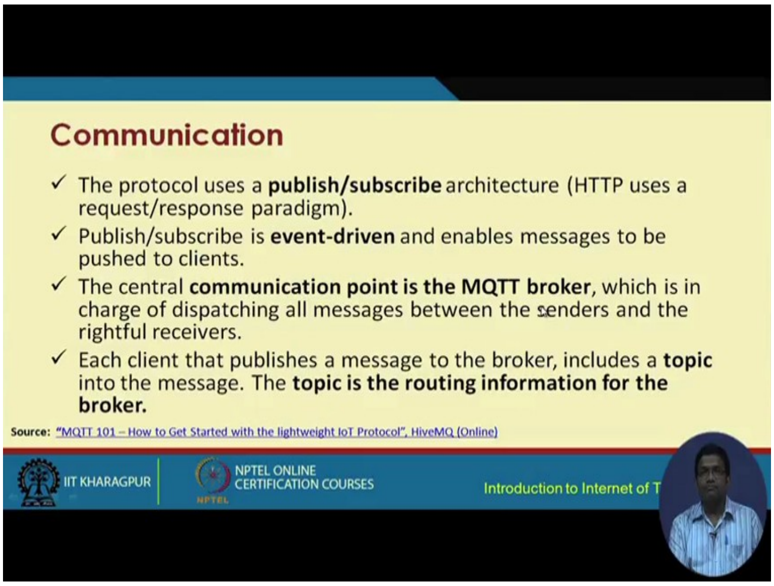
(Refer Slide Time: 06:49)



So, this is what I was referring to just a short while back. So, what we have is these pictorial depictions of how these publish subscribe model works in the case of MQTT. So, we have a temperature sensor, we have laptops, we have mobile devices. This temperature sensor in this example publishes the temperature which is basically brokered at this MQTT broker. So, what this fellow does is, it broker you know because it is a broker between the different clients and different other application serving devices which required the data which can subscribe to the data that is published by these different sensors.

So, what it is going to do is, first it is going to get the subscription requests from these different clients, the mobile device, the laptop and so on and so forth. So, first is the subscribed and there after it is published. So, what is published? The temperature is published. Where is the temperature residing? It is fetched from the sensor and it is being brokered at the MQTT broker. So, from those devices, those clients which have basically subscribed to the services, they are going to get this sensing updates, the sensor data updates.

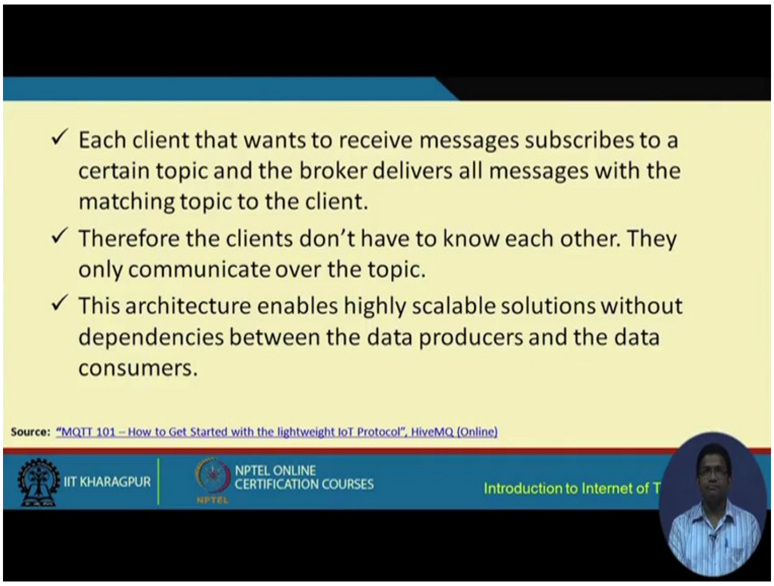
(Refer Slide Time: 08:27)



So, when we look at the communication, the architecture that is followed is publish subscribe publish subscribe architecture and not the request response architecture that is typically followed by traditional http which is used for the internet, this publish subscribe model is event driven. That means, whenever there is an event, whenever there is a fire, when the temperature increases, whenever a camera may be an IoT camera basically observes some kind of change in the environment or whatever maybe there is an intruder or whatever it is, so the central communication point.

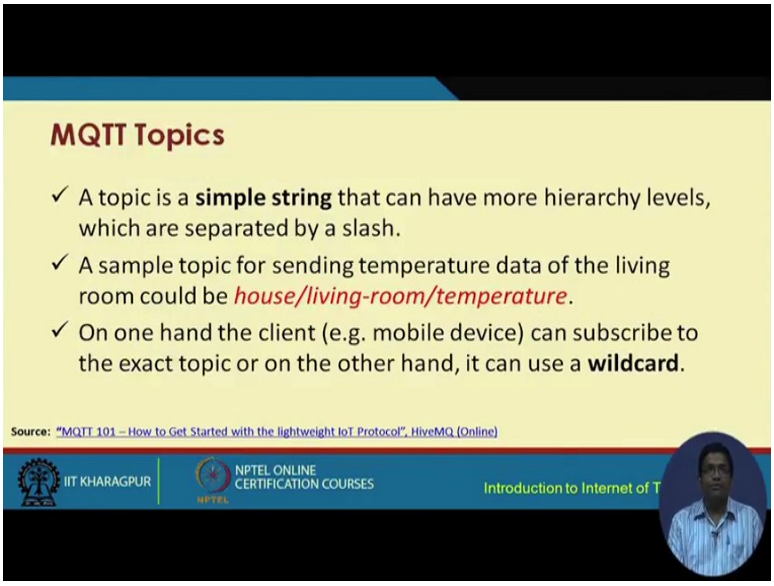
So, it is sorry, I am sorry. So, what we have is it is event driven. So, whenever there is some kind of an event and those data are basically pushed to the clients, so these messages basically are pushed to the clients and then, we have this broker which is in-charge of dispatching all the messages between the senders and receivers and each client that publishes a message to the broker includes a topic into the message and this is the topic which is very much important in the case of MQTT and this is the topic which is of interest to these application clients.

(Refer Slide Time: 10:02)



So, each client that wants to receive the messages subscribes to a certain topic and the broker delivers all the messages with in the matching topic to the client. So, essentially what is happening is the clients, they do not have to know each other and what is required is they only need to communicate with each other over the topic. So, they do not know about each other and this architecture basically appears to be a scalable architecture with a scalable solution. There is not much dependency between the producers and the consumers of the data and that is where MQTT is very popular.

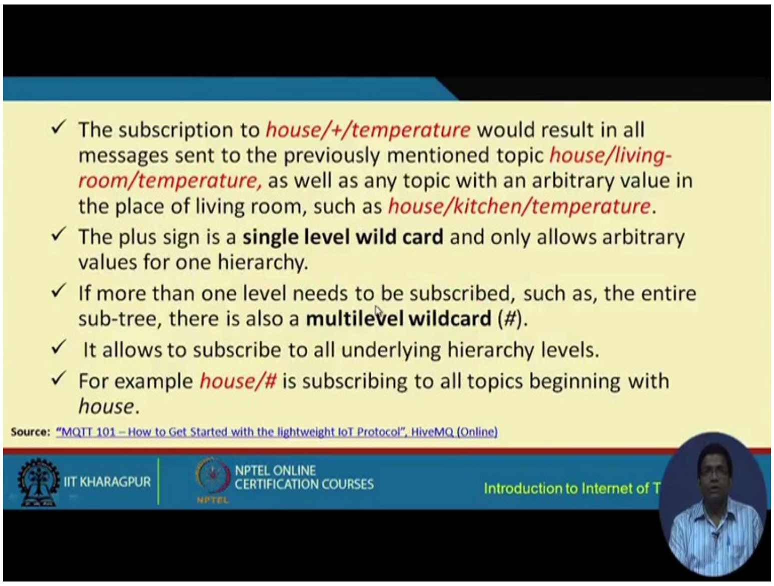
(Refer Slide Time: 10:43)



In MQTT we have the concept of the topic as I just mentioned a minute back and this topic is nothing, but a simple string that can have more hierarchical levels which are separated by a slash. In this manner a sample topic for sending the temperature data of the living room could be marked in this manner, could be named in this manner. So, we have house, a smart house kind of scenario. We have house and within the house we have living room and the temperature that is collected from this particular living room is of interest. So, this topic that is of interest and this is a sample, this is an example of how the topic for sending temperature data of a living room looks like.

So, on one hand the client like a mobile device, a laptop or whatever can subscribe to the exact topic or on the other hand, it can also use a wildcard. So, this is an example of an exact topic. Wildcard could also be used.

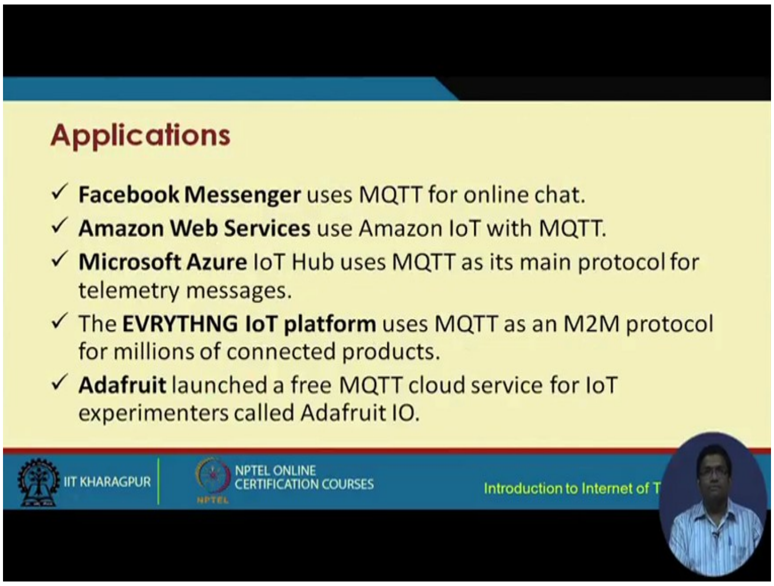
(Refer Slide Time: 12:01)



Wildcards can be used in different ways based on the different levels the subscription to house/+/temperature results in all messages sent to the previously mentioned topic, house/living room/temperature as well as any topic with an arbitrary value in the place of a living room such as house/kitchen/temperature.

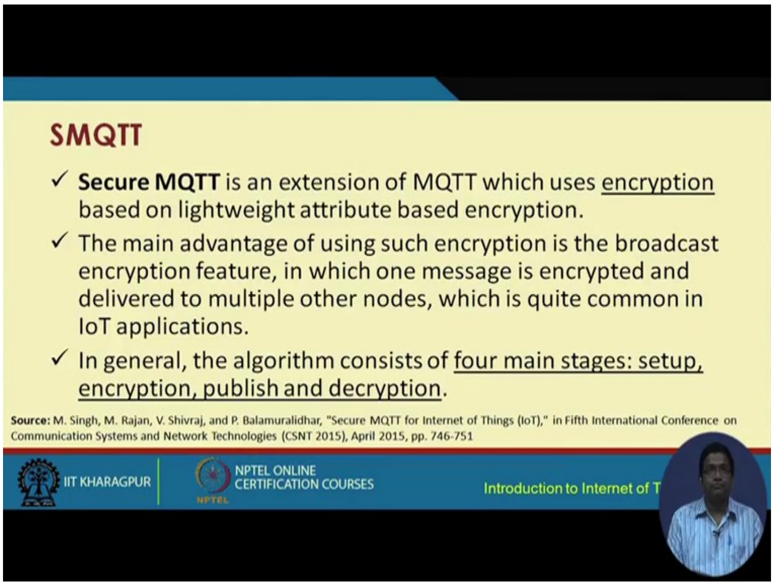
So, basically you know this plus sign is a wildcard character which only allows arbitrary values for one hierarchy. If more than one hierarchical level is required, the multilevel wildcard is used. So, this is single level wildcard. The plus one is a single level wildcard and this hash sign is as multilevel wide wildcard. It allows to subscribe to all underlying hierarchical levels. For example, house/# is for subscribing to all topics beginning with house.

(Refer Slide Time: 13:06)



Different applications that use MQTT, Facebook messenger for online chat, Amazon website service use Amazon IoT with MQTT, Microsoft Azure IoT hub uses MQTT as its main protocol. For telemetry messages, the EVRYTHNG IoT platform uses MQTT as an M2M protocol for connecting several products and devices. Adafruit uses MT MQTT cloud service for IoT experimenter's caller Adafruit IO.

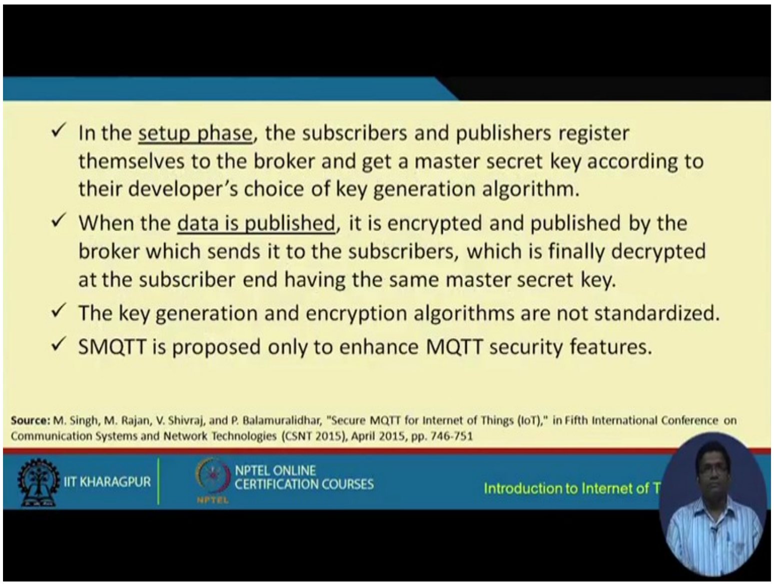
(Refer Slide Time: 13:45)



Finally after understanding the overall philosophy behind MQTT, let us now quickly review the secured version of MQTT which is called the secure MTTM MQTT, the secure MQTT or SMQTT in short. So, this is known in both these ways and this actually to me is quite similar in notion to http and https, the secure http. So, we have http secure http, we have MQTT secure MQTT.

So, secure MQTT is an extension of MQTT. So, basically it is an extension of the MQTT that we just discussed by using different security features such as encryption and so on. The advantage of such encryption is the broadcast encryption feature in which one message is encrypted and delivered to multiple other nodes which is quite common in IoT applications. In general, the algorithm consists of four main stages i.e. the setup stage, the encryption stage, the publish stage and the decryption stage. So, setup encryption publish and decryption.

(Refer Slide Time: 15:03)



In setup phase, the subscribers and publishers register themselves to the broker and get a master secret key according to the developer's choice of key generation algorithm. So, depending on what key generation algorithm is used, the subscribers and the publishers register themselves to the broker and get a master secret key according to that particular algorithm.

So, when the data is published, it is encrypted and published by the broker which sends it to the subscribers which is finally decrypted at the subscriber end having the same master secret key. The key generation and encryption algorithms are not standardized SMQ. SMQTT is proposed only to enhance the security aspects of MQTT.

So, in this part of the lecture on basic topics on IoT networks, what we have done is primarily we have gone through two protocols. We have seen that there is an assortment of different protocols that they have to support the networking of IoT, but in this particular part of the lecture, we have focussed mostly on two protocols. One is the SMTT and the other one is, sorry MQTT and the other one is SMQTT which is basically the secure version of MQTT.

So, we are going to go through few other protocols in the next lecture and from that we can use them finally to establish to build different platforms for IoT in a small scale or even in the larger scale.

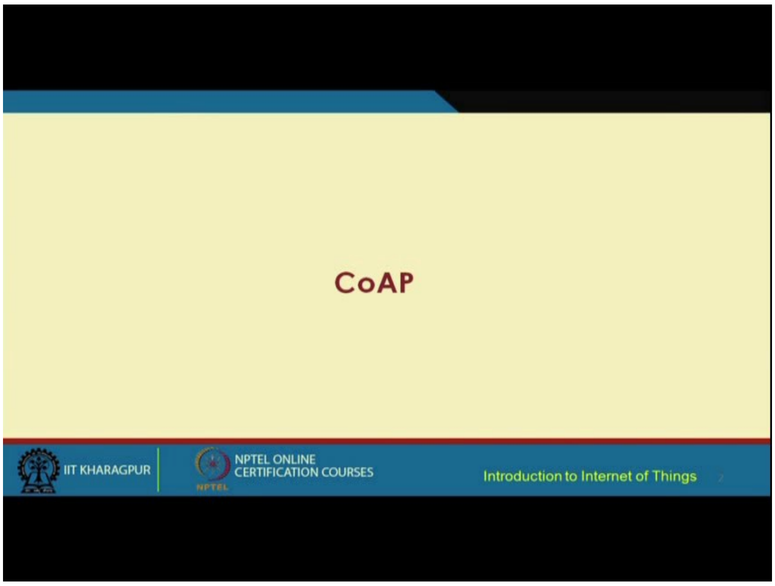
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 07
Basics of IoT Networking- Part- III

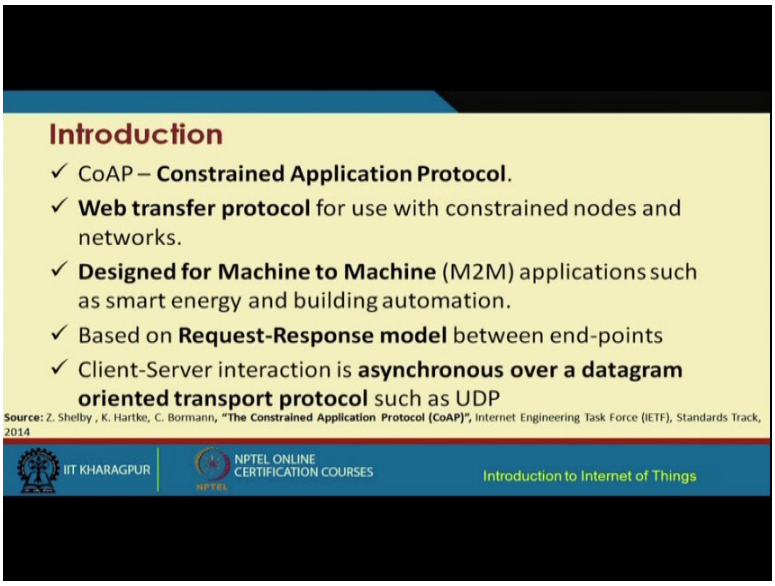
So, we continue with our discussions about the different protocols that are used for communication and networking of internet of things.

(Refer Slide Time: 00:34)



So, the next protocol that we are going to cover is the CoAP protocol and the full form of which is Constrained Application Protocol.

(Refer Slide Time: 00:37)

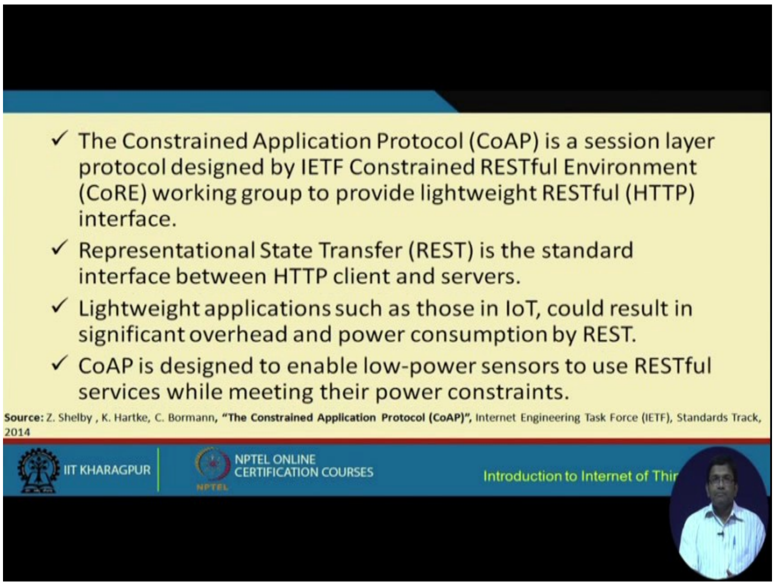


This protocol is particularly used for web transfer and by web transfer I mean very similar to the HTTP, but web transfer in the context of constrained networks resource, constrained networks with nodes which are constrained with respect to different resources, such as limited energy or power supply, limited computational resources, limited communication resource, limited bandwidth environment and so on.

So, CoAP is sort of like an HTTP equivalent that can be used in the context of IoT and the other thing that we have to understand is CoAP is strictly speaking a session layer protocol. However, we can also contribute as an application layer protocol as well. So, in IoT particularly when we taking to consideration the different applications involving machine to machine communication for example, smart energy, smart environment you know building automation and this kind of applications CoAP comes out to be very much useful.

CoAP is based on a request response model. So, basically you know it will very clear shortly about how CoAP works. So, at this point you know you have to understand that there are two endpoints, the source and the destination and a request is sent and a response is received back from the in the other end point and that means, the destination. So, this is how CoAP works. So, there is sort of like a client server, kind of interaction that goes on. So, there is the datagram that is sent from one endpoint to another and that basically, it is an asynchronous kind of communication and it also works on top of in the transport protocol UDP.

(Refer Slide Time: 02:55)

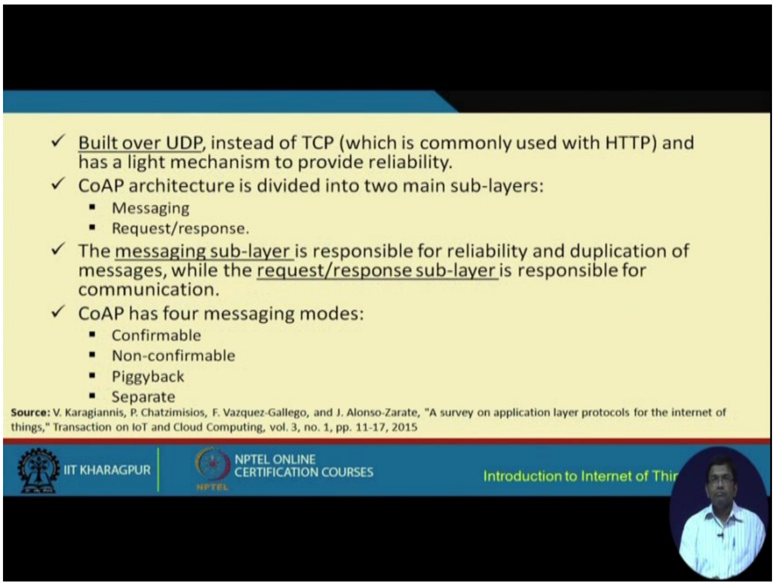


So, basically CoAP, we have to keep in mind that CoAP works on top of UDP. So, this particular protocol is based on IETF RESTful Environment Working Group. So, there is architecture, restful architecture and these people who have to post the restful architecture, they have proposed the CoAP protocol. So, it is basically used sort of like a lightweight equivalent of the HTTP and it is a standard REST. So, let us go back to the rest protocol first.

So, REST is a standard interface between the HTTP clients and servers, but this REST protocol is useful where there is no resource limitation because you know this is quite resource hungry kind of protocol which communes lot of resource. REST basically is not good for constrained environments like IoT.

So, CoAP is sort of like a protocol which is a lightweight equivalent of the rest architecture and rest protocol and it helps to communicate with under low power constraints.

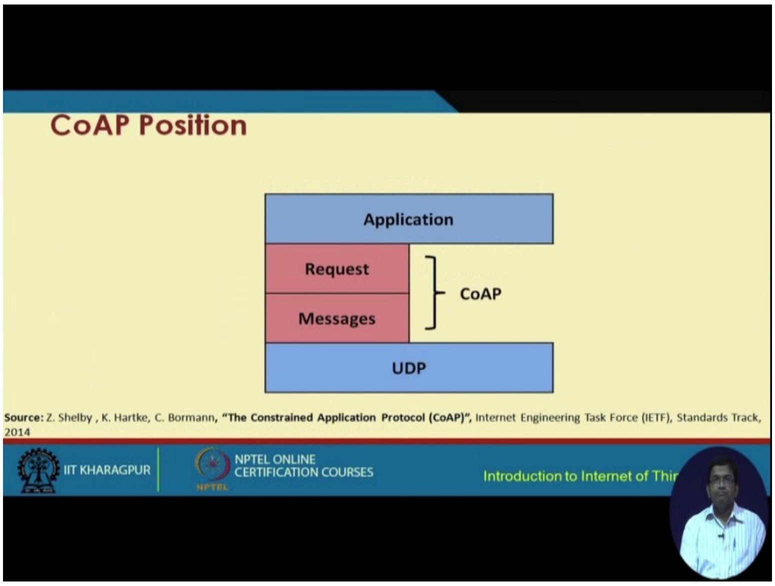
(Refer Slide Time: 04:19)



So, this is how CoAP works. So, as I was telling you that it is a session layer protocol or even we can think of it as an application layer protocol. So, it basically works on top of the transport layer. So, session layer or application layer are on top of the transport layer and the transport layer protocol that is used in the context of CoAP is that UDP. So, CoAP basically has two main sub-layers, one is the messaging sub-layer and the other one is the request response sub-layer and I will show you pictorially how it looks like shortly.

So, in summary actually at a high level, we can think of the messaging sub-layer to be responsible for functionality, such as reliability and duplication of avoidance of duplication of messages while the request response sub-layer is responsible for the communication, exact communication that is going to take place, the request being sent and the response being received. So, these are two main sub-layers that are there in the CoAP protocol or the CoAP architecture more specifically. So, there are different messaging modes for CoAP, one is the confirmable mode, the second is the non-confirmable mode, the third is the piggyback mode and the fourth is the separate.

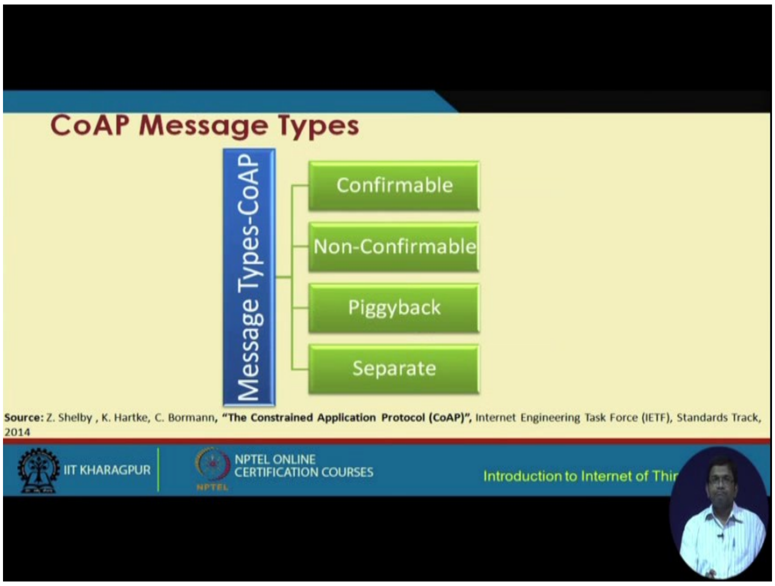
(Refer Slide Time: 05:41)



So, as I was telling you in the protocol stack in terms of the layered architecture, CoAP is a protocol of the session layer. Some can also think of it you know in some cases we try to avoid the session layer. So, in that case, we can think of CoAP to be merged with the application layer, but if session layer is considered, it is a protocol of the session layer. So, session layer means that it lies between the transport layer and the application layer.

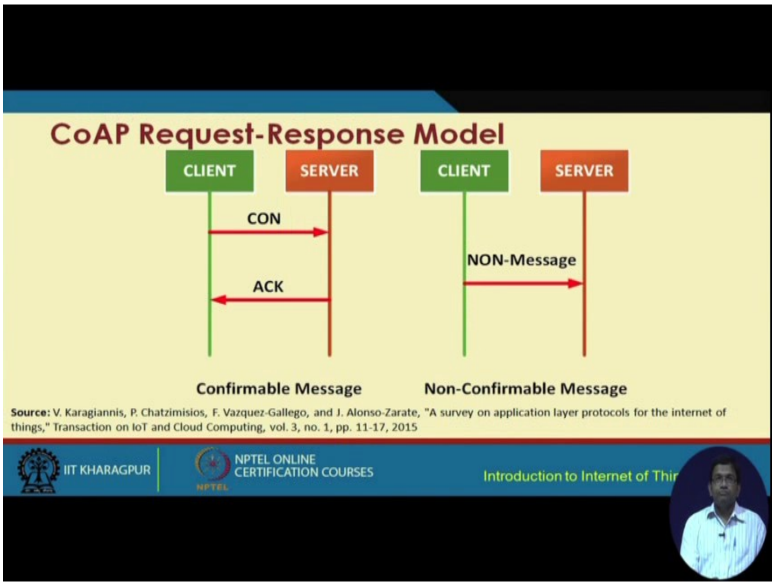
So, at the transport layer, we have the UDP protocol and different applications being run in the application layer and CoAP basically sits in between. So, we have two sub-layers, one is the request response and the other one is the messages. Messages is mostly concerned about the reliability in sharing, reliability of the network, reliability in communication whereas, request response is more to do with the exact communication in terms of sending a request and getting a response back.

(Refer Slide Time: 06:49)



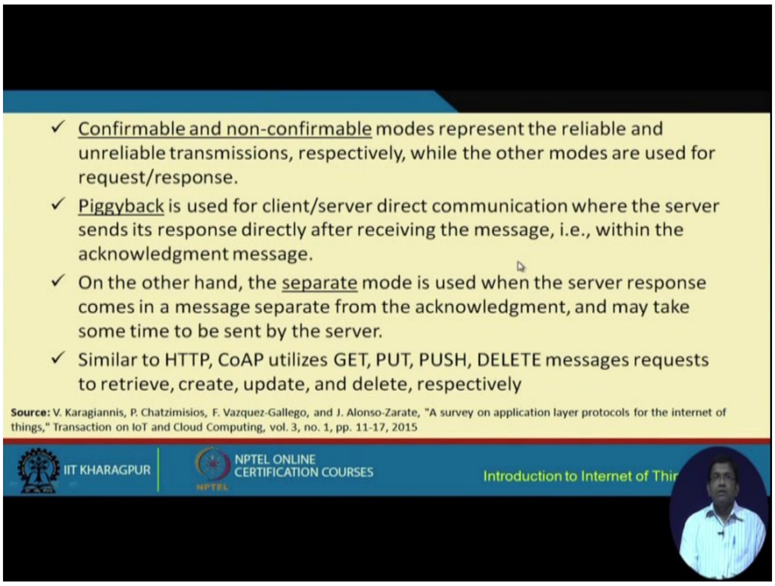
So, this is what I was mentioning earlier. So, we have different types of messages that are used in CoAP. The first one is the confirmable message, the second is the non-confirmable message, the third is the piggyback message and the fourth is the separate message.

(Refer Slide Time: 07:11)



So, basically when we look at CoAP confirmable message, this is how it works. So, we have CoAP is basically a connection between the client and the server in a resource constraint environment. So, what happens is a message is sent and an acknowledgement is received in the case of a confirmable message.

(Refer Slide Time: 07:48)

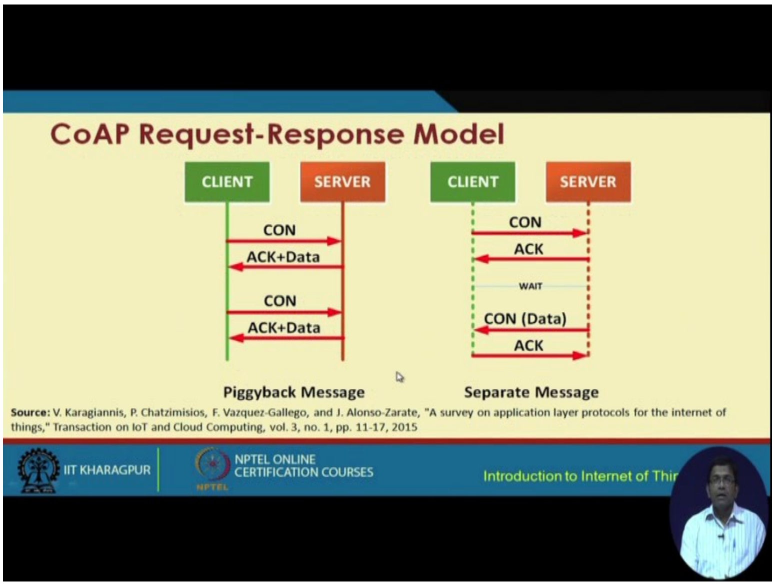


So, this message basically you know it gets an acknowledgement back. So, it is a confirmable message and then, for non-confirmable message, there is no acknowledgement from the server and then, we have the piggyback message which is used for a client server direct communication where the server sends its response directly after receiving the message. So, that basically you know what happens is along with the acknowledgement message, the data is also sent, the response is also sent in the case of piggyback messages.

And in the case of the separate mode, it is used when the server response comes in a message separate from the acknowledgement and that basically may take some time to be sent to the server, this particular message might you know because it is coming separate from the acknowledgement. May be acknowledgement might be received and the message might be received after a rewind back.

So, no sorry find thereafter I am sorry and so, similar to HTTP code basically utilizes different functionalities, such as get functionality, get message, put message, push message, delete message etcetera. So, basically get is for retrieval of some data, put is for creation. So, you want to put some data or some message into the repository, so in that case push or put the server. So, in that case that put message is used and then, we have the update for that push is used and the delete message is for deletion purpose.

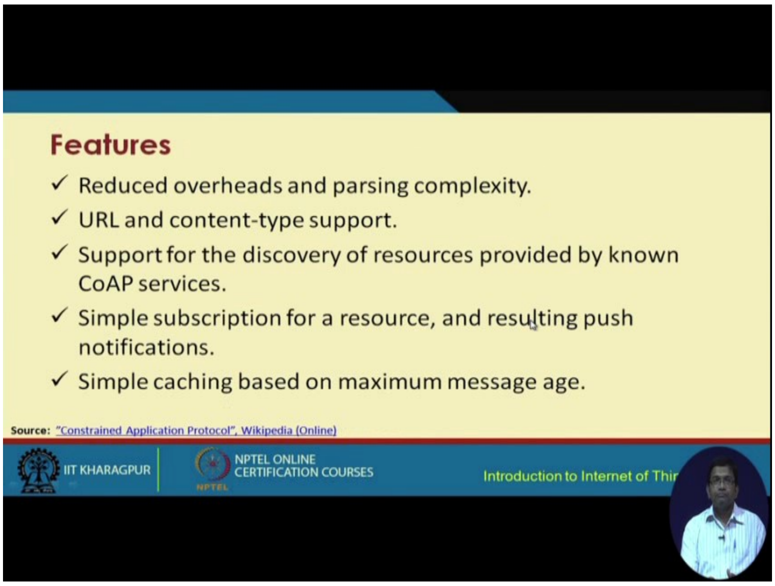
(Refer Slide Time: 09:30)



So, we have already looked at how the confirmable and the non-confirmable message request response looks like. So, let us now look at pictorially how the piggyback message request response model looks like. So, here basically as we can see first a message is sent in piggyback in contrast to the previous two models. That means, the confirmable and the non-confirmable models, rather the confirmable model. So, what we have vary as we can see the data is basically piggybacked along with the acknowledgement message. So, this is how the piggyback message request response model functions.

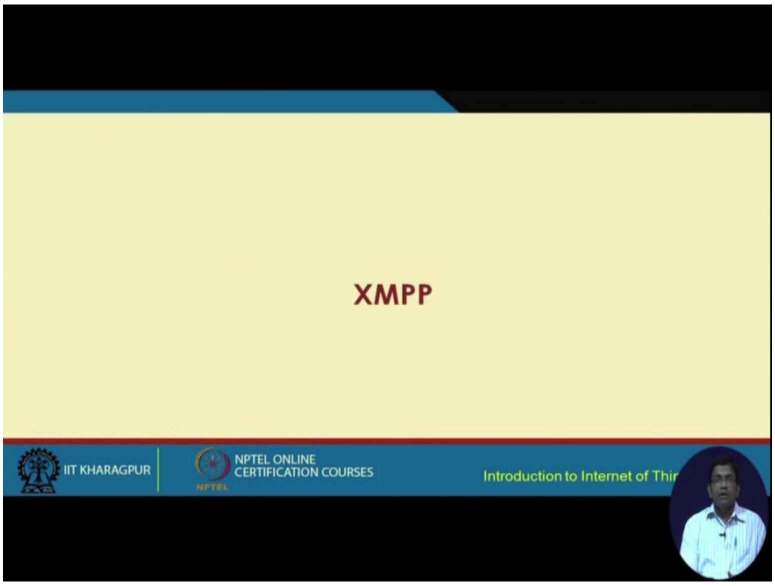
Separate message, we have a message being sent and acknowledgement being received and there is a wait period after which the data is going to be sent separately from the server to the client and corresponding to that the client is going to send an acknowledgement back to the server.

(Refer Slide Time: 10:52)



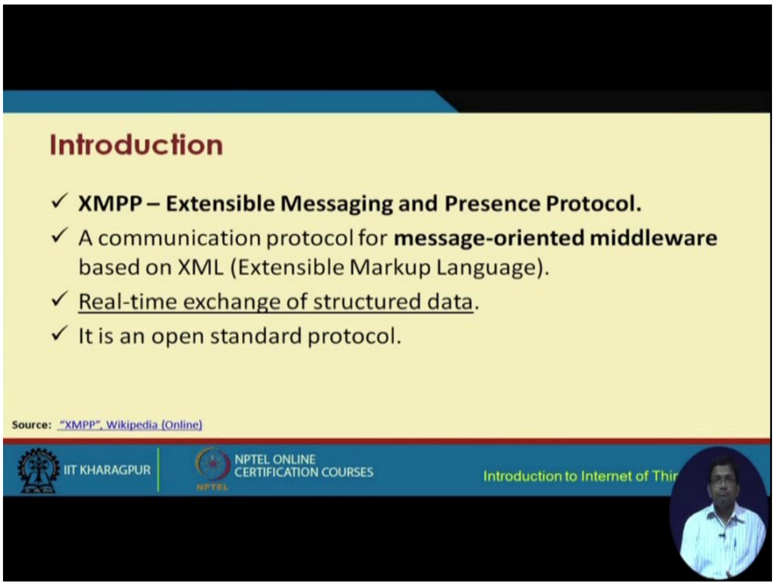
So, this is how separate messages look like so these basically CoAP as a whole and these different message types, they together help to induce the overhead and the parsing complexity of the network. So, there are different types of discovery of resources that are supported by CoAP and we are going to go through them little bit further.

(Refer Slide Time: 11:23)



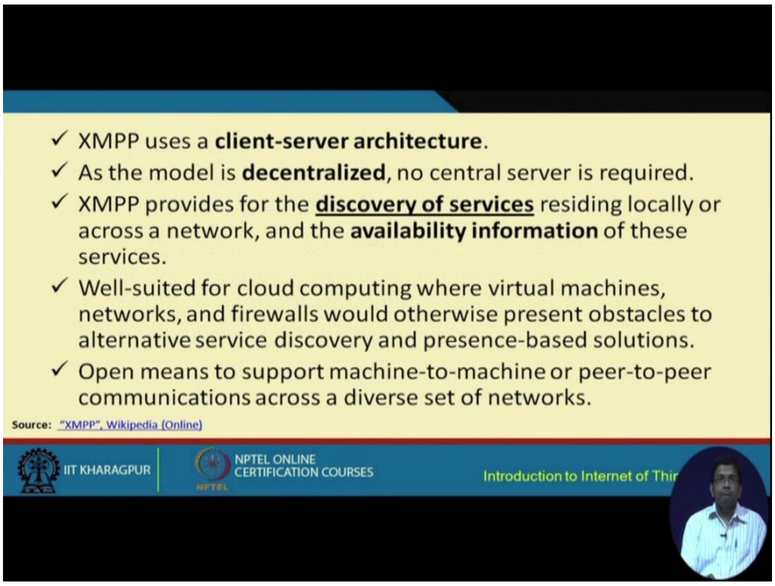
So, but so we now start with the XMPP protocol which is the next protocol to be discussed.

(Refer Slide Time: 11:34)



The full form of XMPP is Extensible Messaging and Presence Protocol. So, it is a message oriented middleware that is based on XML, whereas XML is particularly used for unstructured data. XMPP is useful for real time exchange of structured data and it is an open standard protocol.

(Refer Slide Time: 12:03)

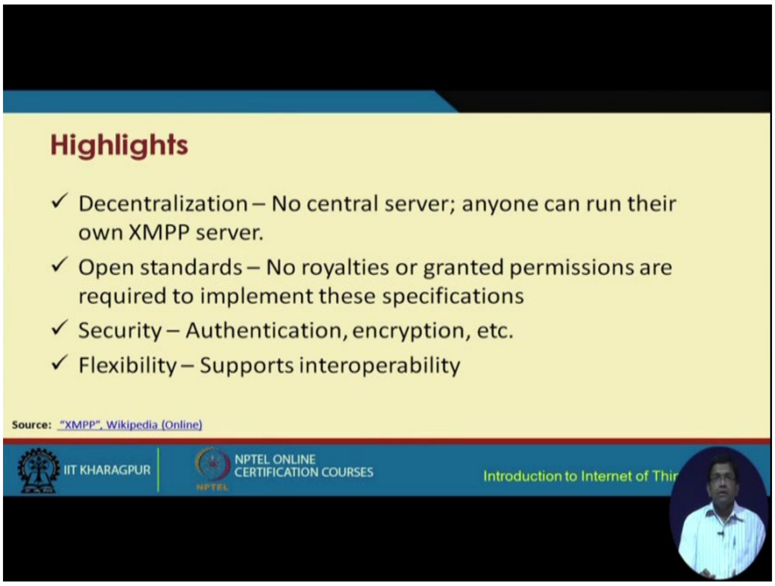


So, XMPP uses a client server architecture, it uses a decentralized model meaning that there is no server that is involved in the message transfer and it provides facilities for discovery of messages which are residing locally or globally across the network and the availability information of these services.

So, as we can now basically think about it, so it is well suited for cloud computing environments, where virtual machines networks and firewalls are involved and would otherwise present obstacles to the alternative service discovery and message based solutions. So, you know think of it this way that with the help of XMPP, we can do things very similar to like pin protocol. So, in the case of pin, basically when we have the involvement of firewalls etcetera, so pin cannot be used as such, right.

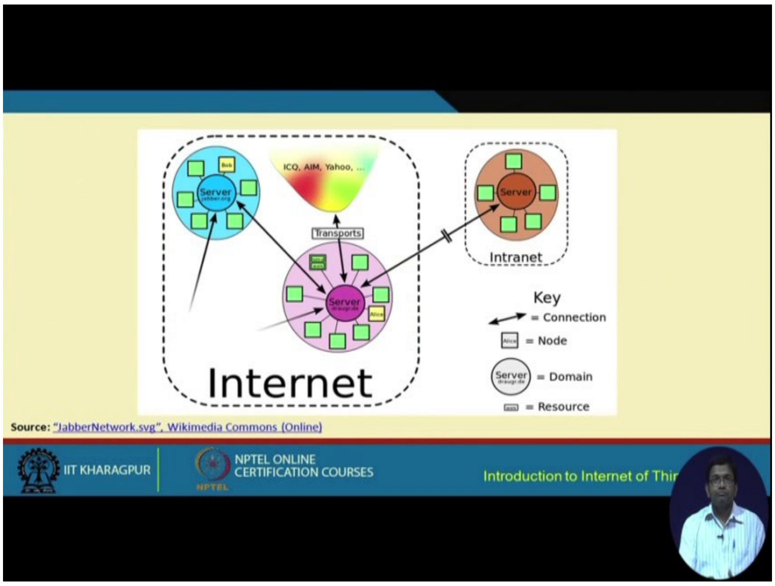
So, in this particular case, in the case of XMPP, it basically removes all these constraints, these barriers for having the discovery of the services and if it is the discovery of services locally, then it is no problem, but if it is across the network and there is a firewall in between, then XMPP can still work.

(Refer Slide Time: 13:34)



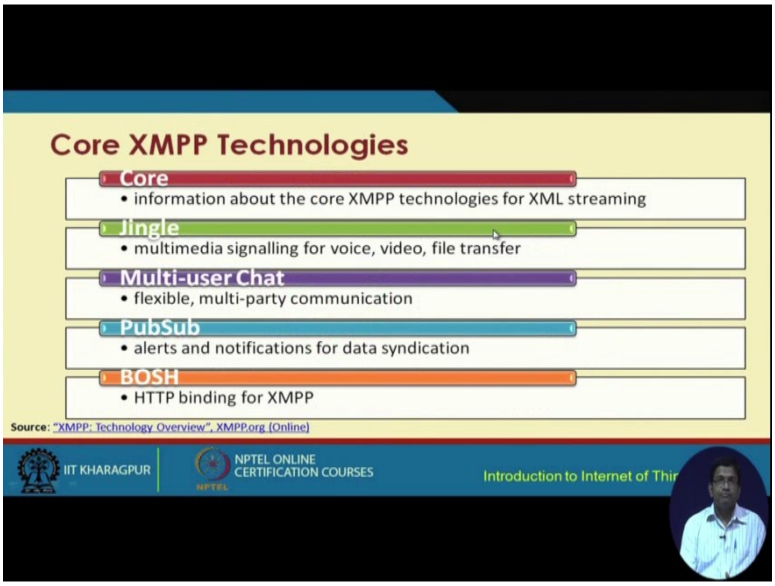
So, some of these highlights of the XMPP protocol, it is based on the concept of decentralization where there is no central server and then, you know everybody can run the XMPP server theoretically and it is based on open standard. So, there is no involvement of royalties or granting permissions to implement the XMPP specifications, different security features that the standard ones, such as authentication, encryption, etcetera, can be implemented using XMPP on top of XMPP rather and XMPP also offers flexibility in terms of supporting interoperability between different systems, different devices, different protocols, and so on.

(Refer Slide Time: 14:26)



So, consequently I was giving you the analogy with the traditional pin protocol that is used for internet and here we are trying to have something similar, but you know it is bit different in this particular manner. So, it is now if you look at this particular figure what we see is with the help of XMPP, not only it is possible to communicate with other servers like in the case of the traditional internet, but also with other messaging platform such as ICQ, AIM, Yahoo and so on. So, this is also possible. So, not only that this is possible, but additionally it is also possible to communicate with other intranets, other intranets.

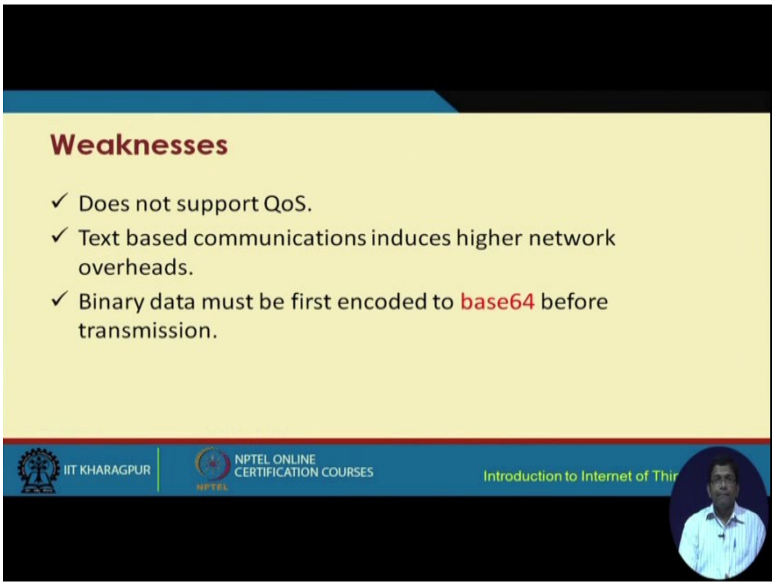
(Refer Slide Time: 12:25)



So, XMPP basically helps in doing this. There are few core XMPP technologies, one is the core technology which provides information about the core XMPP technologies for XML streaming, then we have jingle which is used for multimedia signaling with the help of voice you know wherever there is multimedia resources, such as voice, video, file transfer etcetera, it can help in signaling jingle multi-user chat.

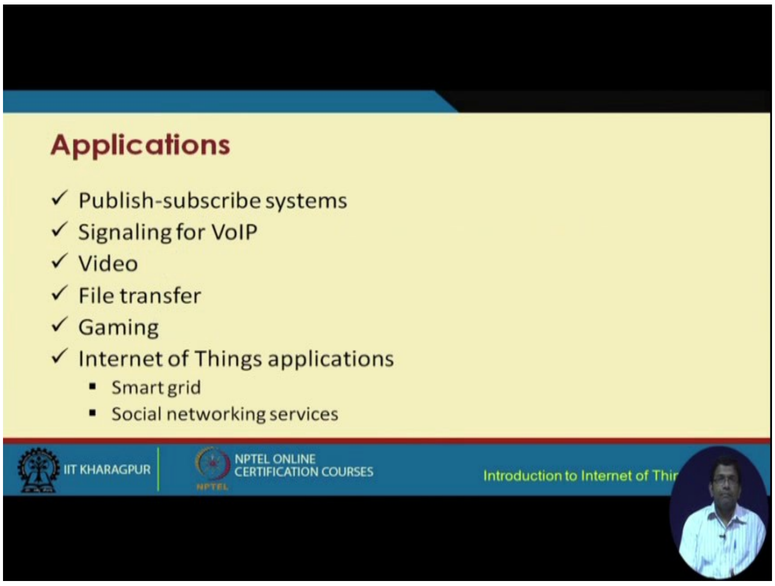
It is a flexible technology which can be used for multi-party communication. Pub sub is Publish Subscriber. Publish subscribe model and publish basically alerts, this pub sub model basically alerts and notifies for data syndication and the BOSH technology. It is used for HTTP, binding for XMPP wherever there is required meant for HTTP binding when using XMPP, this can be used.

(Refer Slide Time: 16:23)



There are different weaknesses as well of XMPP protocol. It does not support QOS, text based communication including you know Higher Network Overheads are involved in the use of XMPP. So, it is not good for text based communication.

(Refer Slide Time: 16:56)



Binary data must be first encoded to base 64 before it can be transmitted. The different applications that use XMPP publish subscribe systems, pub sub systems, then signaling for voice video file transfer, gaming applications, IoT applications such as smart, grid, social networking and so on.

So, with this we have come to the end of two order protocols. We have discussed that two order protocols. So, XMPP is a protocol that is very useful. So, we have discussed about the CoAP protocol first with the session layer protocol which is useful for use in a similar kind of platform, where rest is required for communication between the client and the server. So, CoAP protocol and then, we have discussed about the XMPP protocol.

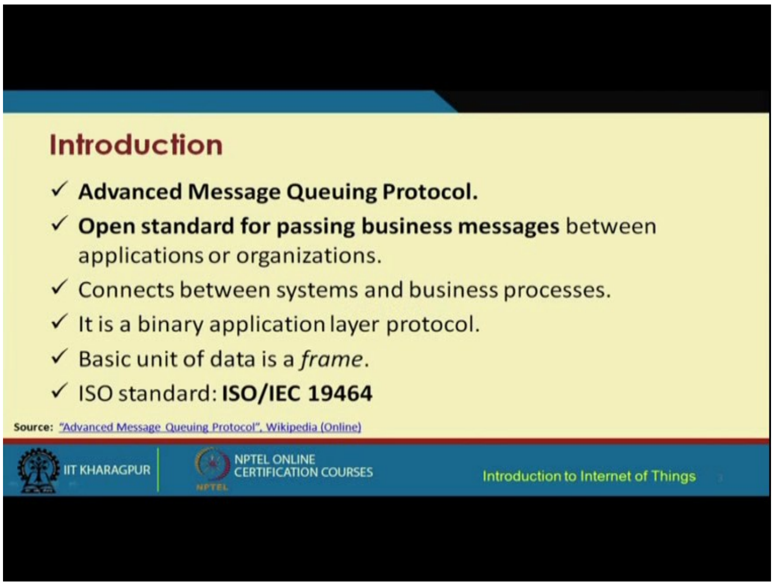
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 08
Basics of IoT Networking- Part- IV

So, we continue with few other protocols and now, we are going to look at one very interesting protocol which is bit different from the previous protocol that we have been discussing in the context of basics of networking, IoT networking.

(Refer Slide Time: 00:42)

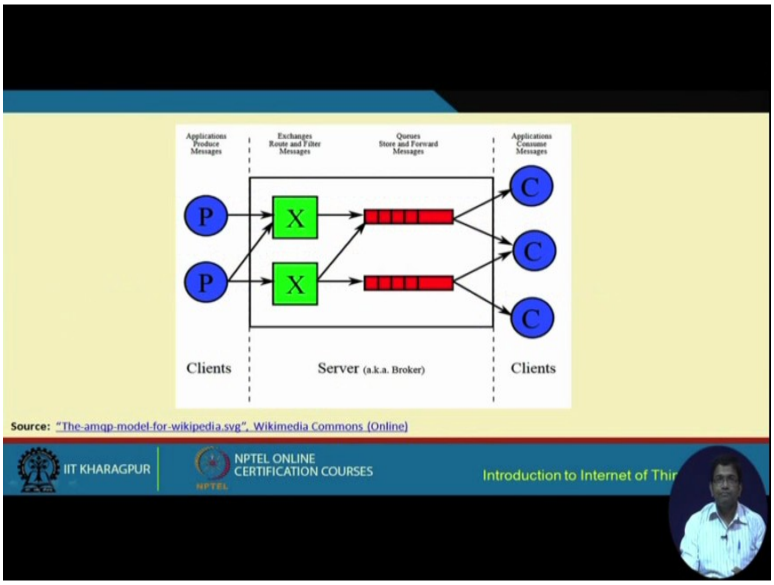


So, this protocol is the AMQP protocol and the full form of which is Advanced Message Queuing Protocol and this Advanced Message Queuing Protocol basically follows some kind of an open standard which is based on the ISO. So, it follows, basically ISO IEC 1964 Standard.

So, this standard basically helps define how mists are going to be passed from businesses, business applications or organizations. So, in other words, a particular business is comprised of different systems and different processes, business processes. So, a business can be conceived as a collection of different systems and business processes. So, this particular standard helps in communicating between these systems connecting rather connecting between these different systems and the business processes of that particular business.

So, it is a binary application layer protocol. It is an application layer protocol and the unit that is used for data transfer in this case is known as the frame. So, it is bit different from the concept of frame in the link layer. So, you know here also it is known as frame, but it is not exactly the same frame that we talked about in the context of link layer protocols.

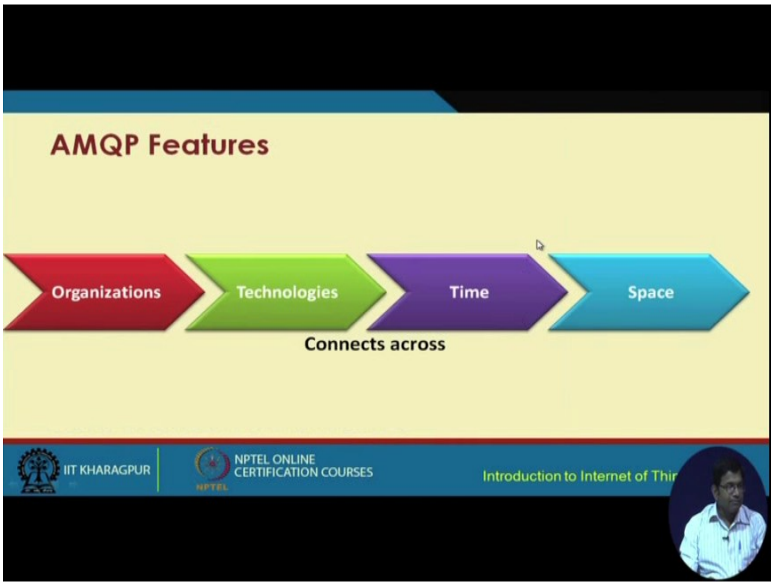
(Refer Slide Time: 02:07)



So, let us now try to understand how this particular protocol works. So, we have clients which are producers of different messages. We have a server and on the other hand, we again have a layer of clients which are consumer of the messages. So, we have the producers of the messages, we have the server which comprises of routers and filters and queues for forwarding the message, for queuing and for buffering and forwarding the messages and then, we have the consumers of the message. So, this server basically acts as a broker, the server acts as a broker.

So, essentially what happens is these clients for example, different sensors they produce different data. They produce different messages. So, these messages are sent to the different routers and filters in this manner which again can be buffered in a queue and with the intention of forwarding them again in the future and these data, the forwarded data beyond the server are sent to other types of clients which are the consumers of these messages. So, we have the producers, we have the server in between and we have the consumers.

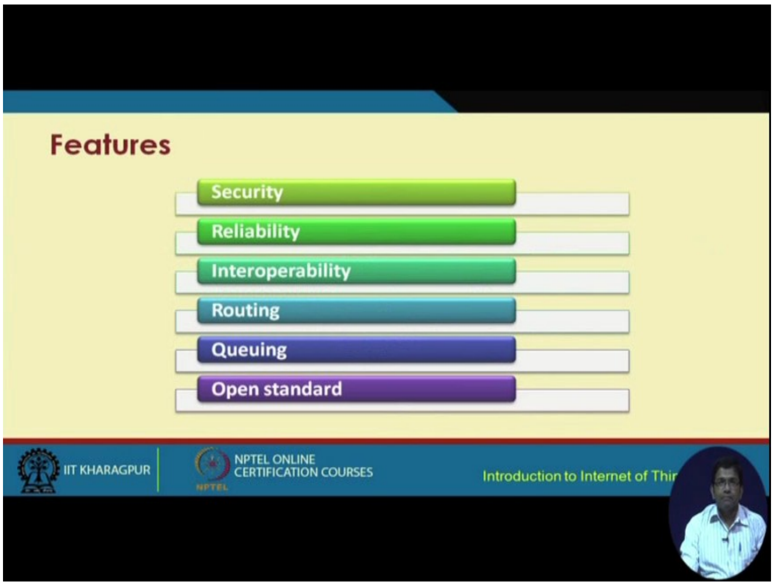
(Refer Slide Time: 03:48)



So, AMQP can be thought of as a collection of different features. These features basically cut across things such as organization. So, basically AMQP can help in connecting different organizations, connecting different technologies, connecting different organizations with respect to time and that means, at different points of time and the technologies and the organizations that are located in different locations connecting them as well.

So, these are the main features of AMQP. So, connecting organizations technologies time and space which could be distinct from one and so, distinct organizations, distinct technologies you know with respect to time variations in the space AMQP basically helps in connection.

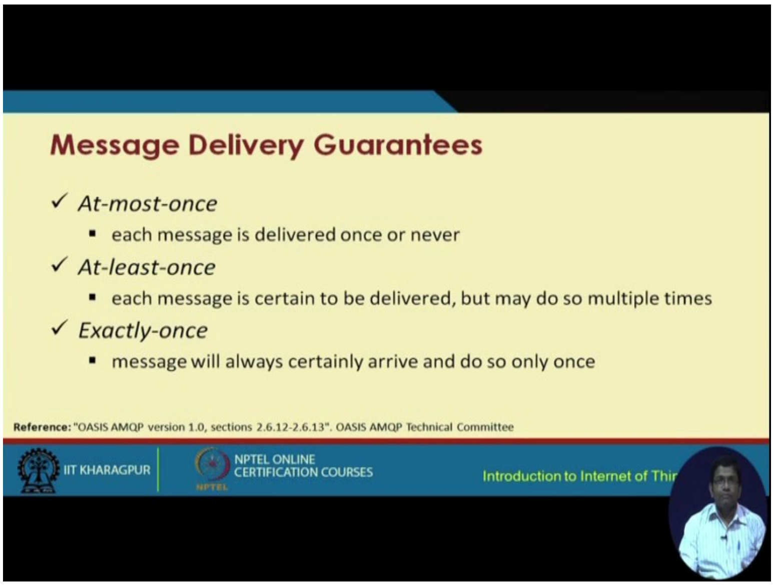
(Refer Slide Time: 04:53)



Few other features from a different perspective AMQP supports security reliability interoperability I think, security, and reliability are understood. I do not mean to elaborate on them further, but in terms of interoperability, we are basically referring to interoperability of not only devices, but also protocols, algorithms messages and so on.

So, this is the next feature and then routing of messages queuing of messages and that it follows an open standard which is based on ISO.

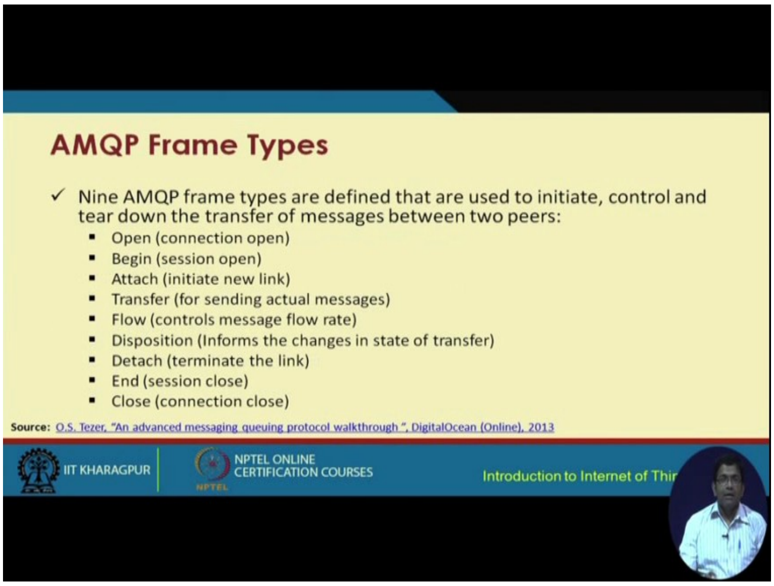
(Refer Slide Time: 05:34)



So, there are different messages that are involved in this particular protocol and what is required is to have message delivery guarantees. These message delivery guarantees can be in three different forms. The first one is at most once which means that each message is delivered at most once.

That means, once or never to the intended recipient. At least once each message is certain to be delivered, but may be multiple times, but it should do at least words exactly once messages will always certainly arrive and do. So, it is only once. So, these are the three different messages, types of message, delivery types and guarantees that are involved in this process.

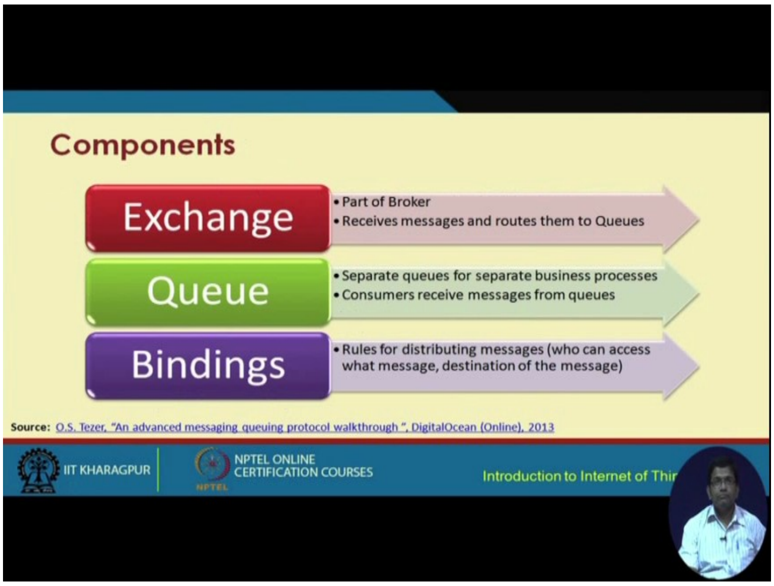
(Refer Slide Time: 06:21)



So, the different frame types there are 9 AMQP frame types that are used for defining to initiate control and tear down the transfer of messages between two peers. So, we have the first one, the first frame type is the open frame type which is used for opening a connection corresponding to this. We have the closed frame type close frame which is for closing the connection closing the connection. Then, we have the begin frame type which is for opening a session and correspondingly we have the end which is for closing that particular session.

Then, we have the attach which is basically used for initiating a new link transfer for sending actual messages flow, for controlling message flow rate and disposition that informs the changes in state of transfer and then, we have the detach which is for terminating the link. So, open, close, begin, end, attach, detach, and in between we have transfer flow and disposition frame types.

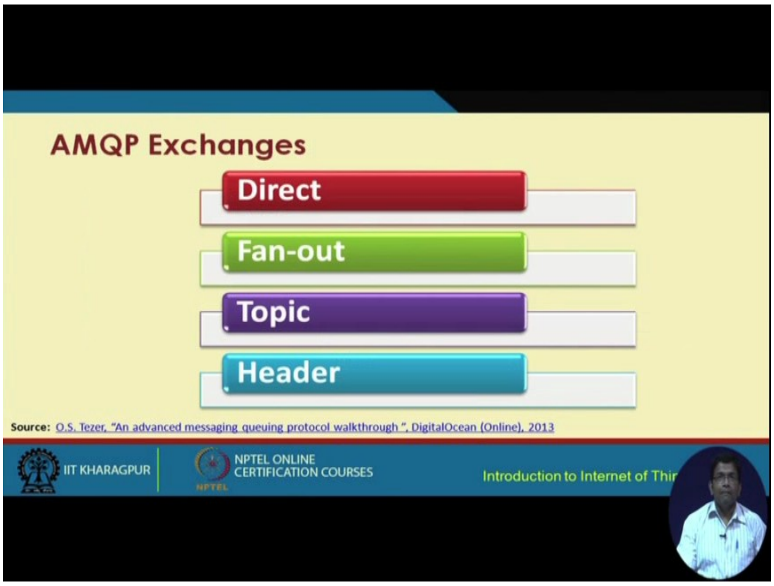
(Refer Slide Time: 08:03)



So, the different components of this particular protocol include three things, three primary things. One is exchange, the second is queue and a third is bindings. So, the exchange component is basically part of the broker that is in that is task to receive messages and route them to the queues. Queues are basically separate for different business processes.

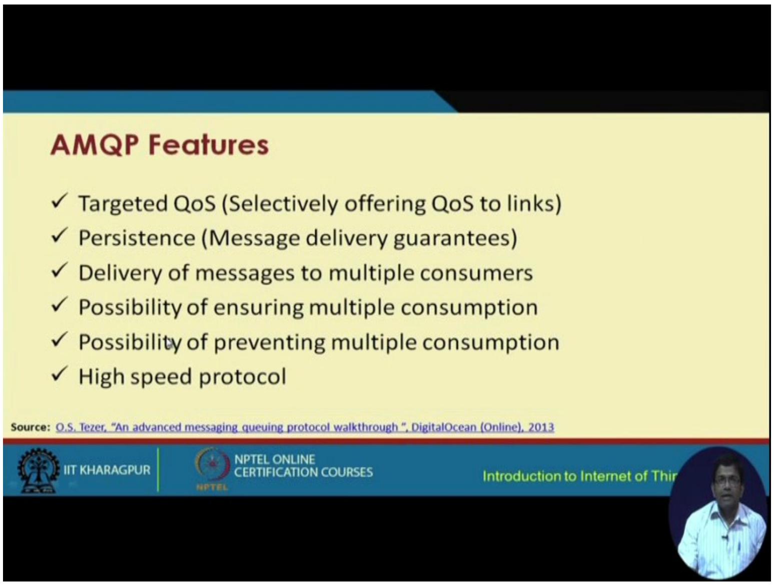
So, different separate queues are used for different or separate business processes and the consumers receive the messages from the queues. Bindings are rules for distributing the messages which means that who can determine who can access what message, the destinations of the message and so on.

(Refer Slide Time: 08:54)



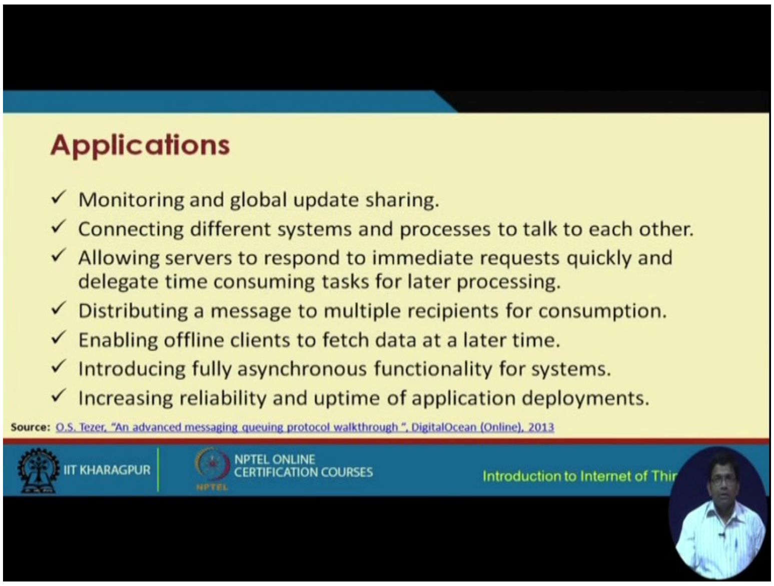
So, we have you know different exchange types in the case of AMQP. AMQP has basically four different exchange types. One is the direct, the second is basically the fan out, the third is the topic and fourth is the header. So, these are the four different AMQP exchanges. So, direct exchange, fan out exchange, topic exchange and header exchange, we are not going to go through these in detail just to keep things simpler and easily remembering. So, that is the reason we have not discussed these in further detail.

(Refer Slide Time: 09:39)



So, these are some of the features of AMQP. It offers targeted QoS which basically targets selective offering of QoS to certain links persistence which basically implies MES offering message delivery guarantee, then we have the delivery of messages to multiple consumers, the possibility of ensuring multiple consumption, possibility of preventing multiple consumption and high speed.

(Refer Slide Time: 10:10)



In terms of the applications, it can be used for monitoring and global updates, sharing applications, connecting different systems and processes to talk to one another, allowing the servers to respond to immediate request quickly and delegate time consuming tasks for little processing, distributing a message to multiple clients for consumption, enabling offline clients to fetch data at any time and increasing the reliability and uptime of application deployments.

So, this basically concludes the discussion about this protocol. So, with this we basically come to an end of the series of lectures on the Basics of IoT networking and in the next lecture, again we will look at few protocols, but the perspective from which we are going to look at is going to be different. So, there we are to look at protocols that are very much useful and that are used for establishing connectivity in IoT.

Thank you.

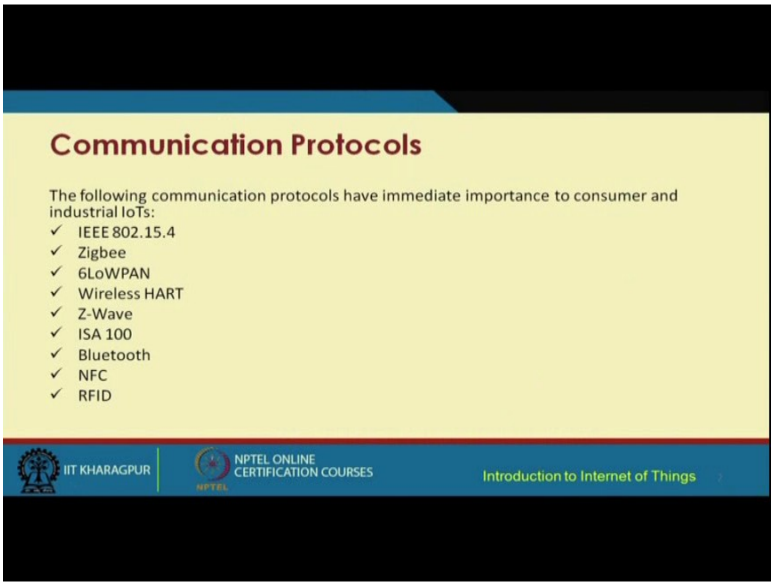
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 09
Connectivity Technologies- Part-1

So far what we have gone through and have understood what the different basic concepts that are involved in the networking aspects of IoT. So, we have gone through different protocols and these protocols include XMPP protocol, MQTT protocol, CoAP protocol cope and AMQP protocol. So, these are the different protocols that we have gone through so far and these protocols are primarily involved with service offerings.

So, they are at the higher level and now we are going to understand, we are going to go down and we are going to understand them more at the physical level. So, physical and partially are the link layer. At physical level and link layer level what are these different protocols; these protocol scan as whole offer connectivity to the different devices which can help in physical establishment of the network.

(Refer Slide Time: 01:40)

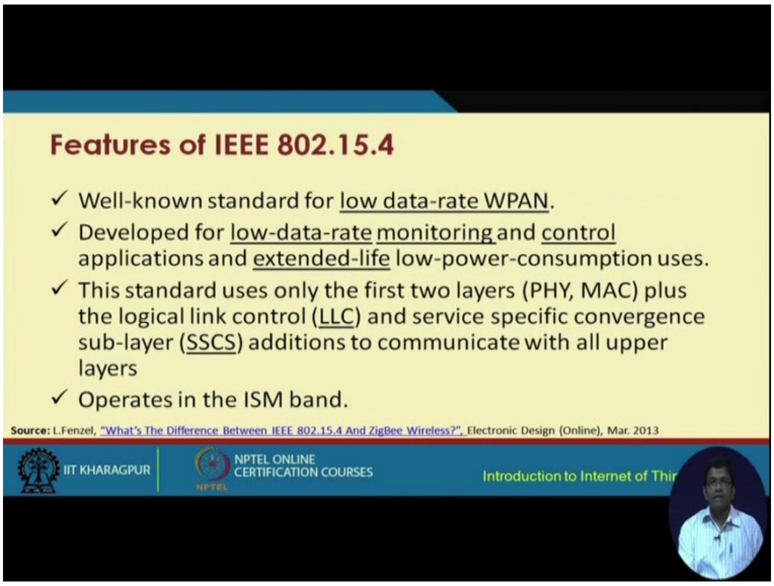


So, we are now going to go through some of these protocols. So, when we talk about these protocols, this can be used for both consumer IoTs and industrial IoT. So, consumer IoT means like smart home, then different applications of smart home, then for different serving, different applications for you know consumer devices, consumer based systems and so on, then for industrial IoT it is like connecting different Machines, industrial Machines, manufacturing Machines and so on offering different connectivity's and smart intelligence on top of those devices and so on.

So, all these different protocols that are listed in front of us for example, this IEEE 802.4 which is a protocol as well as standard as well this can be used ZigBee is very much useful, 6 LoWPAN, wireless HART, Z-wave, ISA 100, Bluetooth NFC and RFID. So, we are going to go through most of these protocols in the subsequent lectures.

So, we will start with the first one which is the 802.15.54 which is IEEE standard and this basically is used for forming Wireless Personal Area Network.

(Refer Slide Time: 03:00)

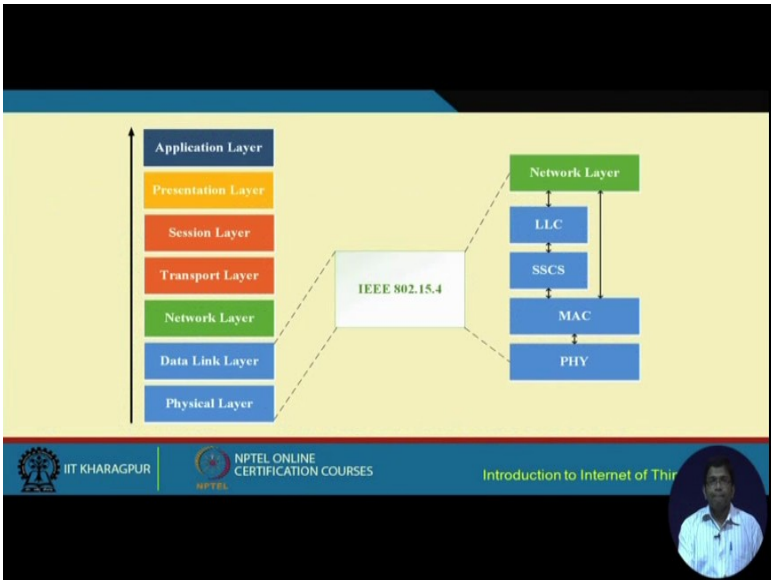


So, personal skill means like you know in the skill of person. So, personal area network are used for forming network at person skill. So, these are basically normally low data rate networks. So, these basically are developed for low data rate monitoring and control; so monitoring mean sensing low data, rate sensing, and then control maybe through actuation and so on and in the process offering because it is low data rate and is used for wireless personal area network.

These can help in offering extended life time to the networks extending the lifetime of the network because of the reduced power consumption. So, this standard uses two sub-layers, two layer sorry two layers. One is the physical layer and the other one is the MAC layer plus the sub layers like logical link control, the SSCS which is the Service Specific Convergence Sub-layer, etcetera to communicate with the upper layers, but this particular standard it focuses on primarily two layers which is the physical and MAC.

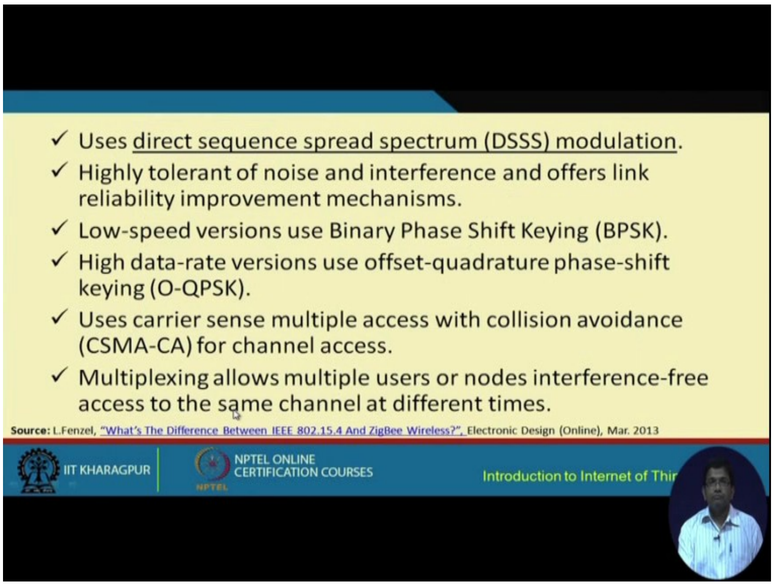
So, physical MAC partly LLC and SSCS that is it about 802.15.4 as such. So, before we go any further I would like to remind you that in this case, the communication takes place in ISM band.

(Refer Slide Time: 04:46)



So, this is what I was explaining to you. So far this particular standard, this particular protocol defines specifications. This gives specifications for operating in the physical layer, MAC layer, SSCS and LLC sub-layers and how these are going to connect with the network layer, but the main focus is on the physical layer and the data link layer of the traditional OSI stack.

(Refer Slide Time: 05:26)

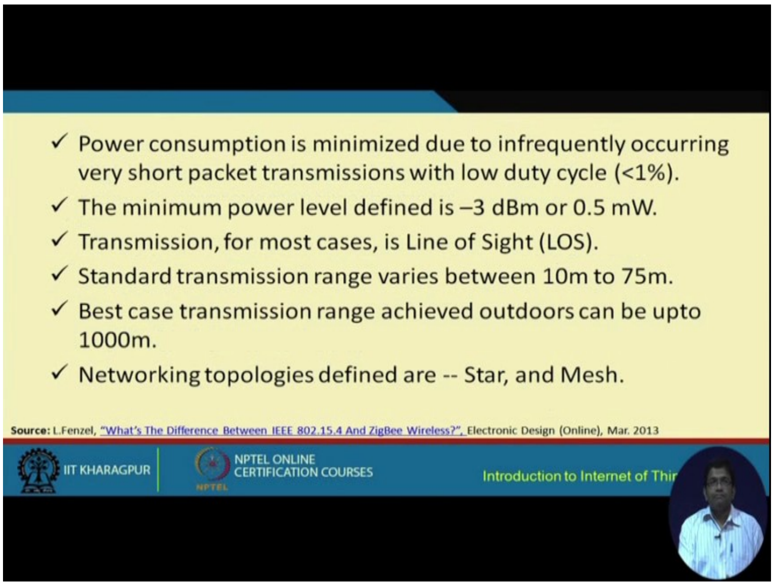


So, few features that we are going to just list over here and we are not going to go through them in detail because here I am assuming that I mean you have some basic background in networks and communication; if you have, you will be able to understand these a little better. However, if you do not have you know this is just for you to remember. We cannot go through the details of how these communication technologies, these different schemes, they work. So, this 802.15.4, it is based on the modulation schemes which is known as the DSSS which is Direct Sequence Spread Spectrum Technique. So, this is the modulation scheme that it uses DSSS modulation scheme.

So, these basically are highly tolerant of the noise and interference and offers link reliability improvement mechanisms. So, this particular standard is helpful in environments which are noise prone and have lot of interferences and in a presence of noise and interference, this particular standard can help in improving the reliability of the network.

So, it has two different variants, two different versions. The low speed version basically uses the BPSK and the high speed version uses what is known as the offset QPSK, O-QPSK and for MAC communication, it uses CSMA-CA for channel access. That means carrier senses multiple access and carrier sense multiple. CA stands for basically collision avoidance. So, carrier sense multiple access with collision avoidance is used for channel access and multiplexing basically allows multiple users of nodes to communicate with one another in an interference free banner at different times over the same channel.

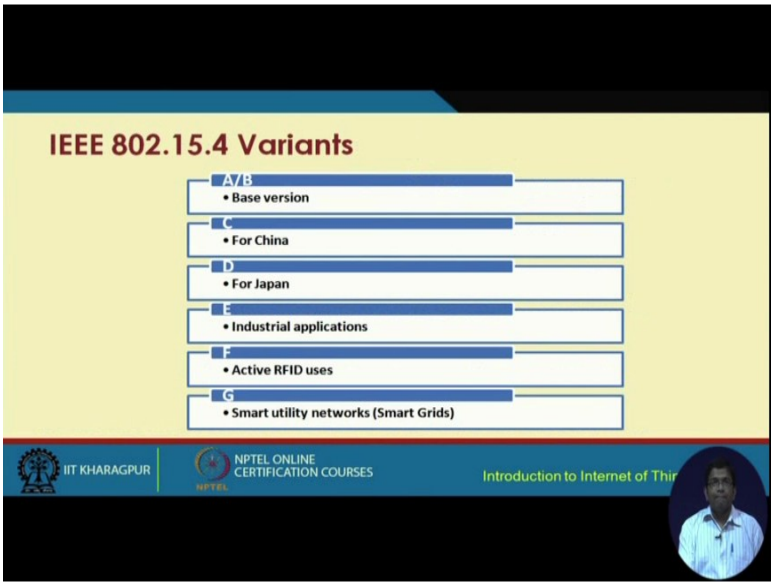
(Refer Slide Time: 07:40)



So, power consumption using this particular protocol is minimized due to the infrequently occurring very short transmissions with low duty cycle which is less than one percent. So, the minimum power level that is defined in this particular standard is minus 3 dBm or 0.5 microwatts. The transmission for most of these cases is line of sight transmission, however non-line of sight transmission is also possible, but you get better efficiency, better performance if line of sight communication is used.

The standard transmission range basically varies between 10 meters to 75 meters. 75 meters will particularly be obtained if it is used outdoors, but for indoor environments typically like 10 meters I would say above 30-40 meters and so on. So, the best case transmission that is received for outdoors can be even up to 1000 meter also in certain cases, but typically you know. So, that is a theoretical possibility, but typically you do not get that much of a transmission range even if it is outdoors that networking technologies that are supported are the star topology and the mesh topology.

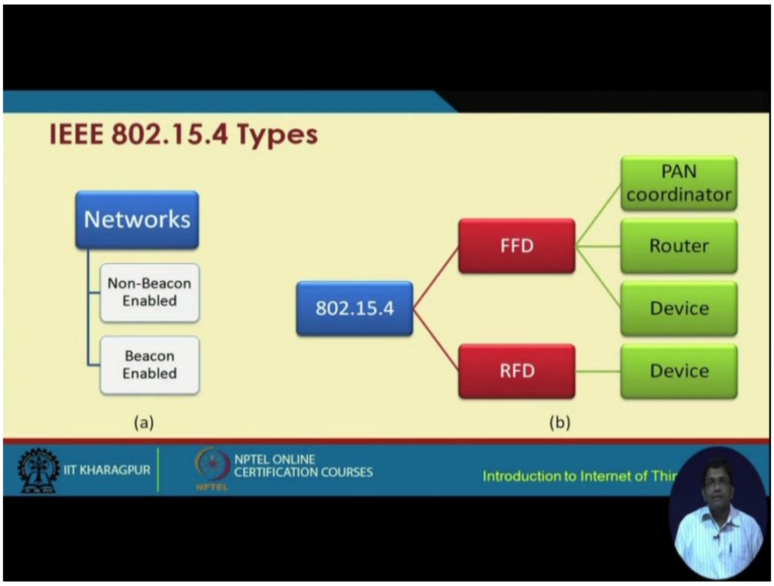
(Refer Slide Time: 09:03)



So, there are different variants of 802.15.4. So, within axel before we proceed further 802.15.4, the IEEE standard is useful for forming wireless personal area network. That means, small range low data rate, low power consuming networks, this can use the 802.15.4. Now, this basically has different variants, the base variants are a and b, but there are variants like the c variant which is used for China, the d for Japan, the e variant is used for Industrial applications, the f variant for active, RFID uses the g for smart utility networks such as smart grids.

So, these are the different variants of the 802.15.4 which are typically used for different purposes in different parts of the world.

(Refer Slide Time: 10:10)

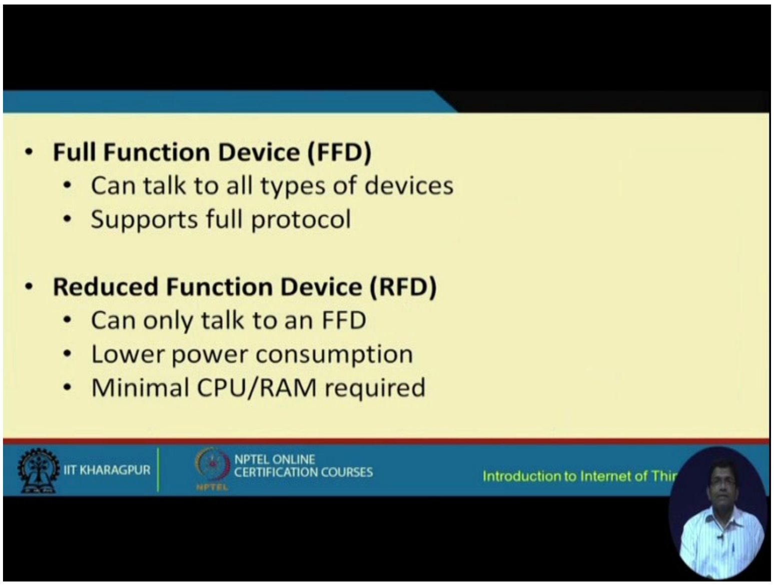


Now, 802.15.4 networks these networks can be classified into two types. The beacon enabled network and the other one is non-beacon enabled network. So, we will look at what is beacon enabled and non-beacon enabled shortly and also, these networks basically use different types of devices.

One is FFD which stands for Fully Functional Device and the other one is the Reduced Functional Device i.e. RFD. The fully functional devices include the PAN coordinator. That means, a personal area network coordinator, the router or the device, they can act as full functional device which can undertake all different types of functionalities, whereas the reduce functional device can only send something very similar.

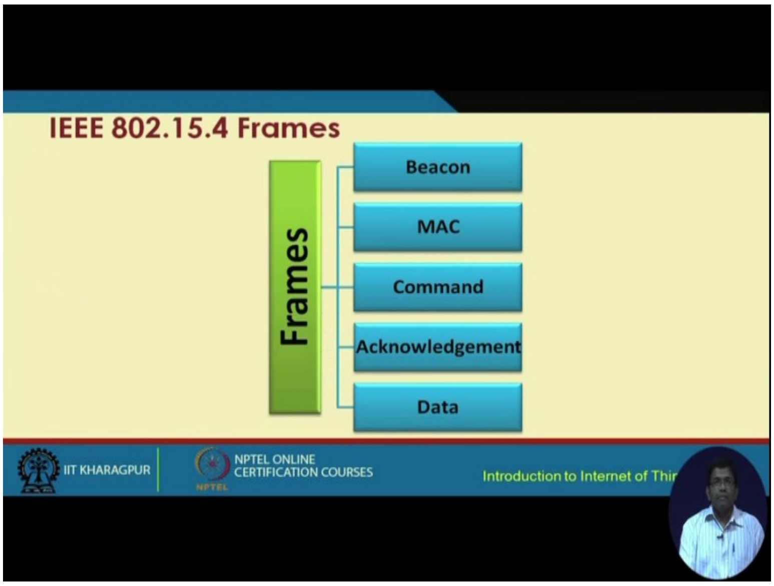
So, they have reduced functional. If they cannot route, they cannot switch, they cannot send the packets, they cannot read a packets and so on. So, they can only do very simple things. These are the RFD's Reduced Function Devices.

(Refer Slide Time: 11:22)



So, once again we have the fully functional device which can talk to all types of devices and can support full protocols. The reduced functional devices can only talk to a fully functional device and has lower power consumption and uses minimal CPU and RAM, so minimal processing and storage.

(Refer Slide Time: 11:47)

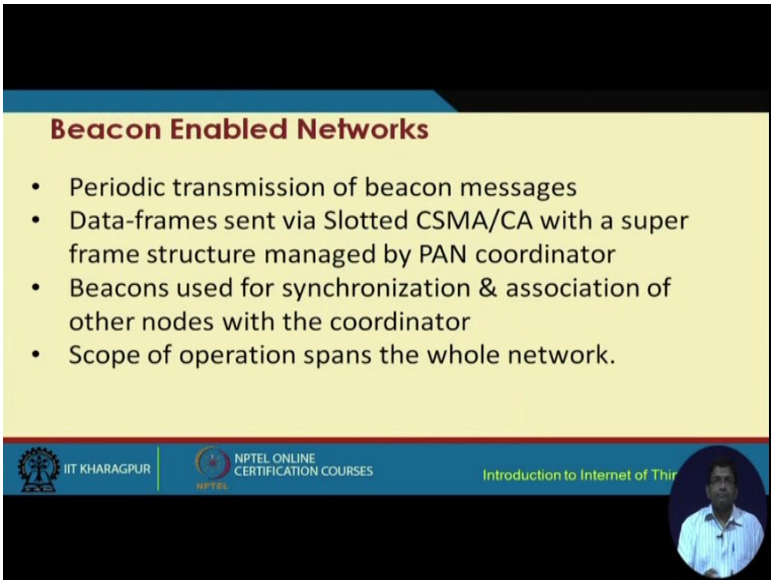


So, there are different frame formats, frame types that are defined for 802.15.4. So, there are typically five frames five frames that are defined for 802.15.4. So, we have the data frame, the acknowledgement frame, the command frame, the MAC frame and the beacon frame. So, I do not need to elaborate further because these are quite obvious.

The command frame is used for things such as different control functions, such as associating a device with a PAN coordinator or disassociating a device or performing different other control functions. So, there are command frames and then, the MAC frames also do not need to elaborate further. This is standard and then, we have the beacon frames.

This beacon frames physically what they do is this pan coordinator at regular intervals of time, they basically sends these beacons which can basically advertise its present and the different devices that are able to get the signal. That means the beacon form that is broadcast by this particular PAN coordinator. These device they know that there is this pan coordinator which is present. So, this is basically enabled, this particular functionality is enabled with the help of this beacon frames.

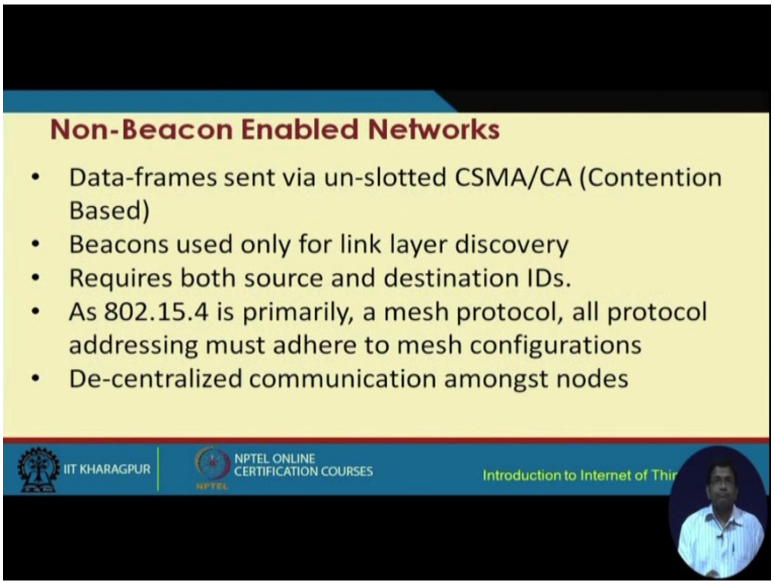
(Refer Slide Time: 13:18)



So, going back to the previous classification, we have seen that we have a beacon enabled network and the non-beacon enabled network. So, what is this beacon enabled network? So, in beacon enabled network basically periodically pan coordinator, it is going to send periodic transmissions of beacon messages. So, periodically beacon messages are going to be transmitted which are going to be received by different devices which one to get associated with the PAN and so on.

Then, the data frames are sent via slotted CSMA CA with a super frame structure that is managed by the PAN coordinator. The beacons are used for synchronization and association of other nodes with the coordinator and the scope of operation basically span the whole network.

(Refer Slide Time: 14:11)

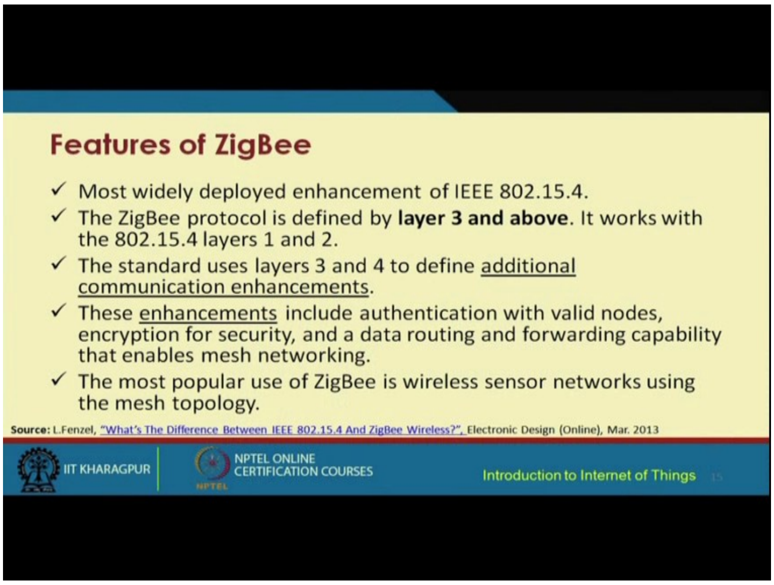


In the context of beacon enabled networks, in case of non-beacon enabled networks, the data frames are sent via un-slotted CSMS CA. The previous one for beacon enabled network, it was the slotted CSMA CA, but in the case of non-beacon enabled network, it is the un-slotted CSMS CA. The beacons are used only for link layer discovery and that means, whether there is any connectivity where is there is any link from one device to another and so on. So, beacon messages basically will help in the discovery of these different links from the PAN coordinator to the different devices and so on.

So, basically these network, this type of network that means the non beacon enabled network request both the source and the destination ids. So, as 802.15.4 is primary mesh protocol, it is primarily based on a mesh protocol. All the protocol addressing must adhere to the mesh configuration. So, this is basically in a excel how the 802.15.4 protocol functions and the different features of it.

We are now going to look at the ZigBee protocol which is heavily used for IoT applications for establishing connectivity between the different nodes and this ZigBee as we will see shortly is basically, it works on top of the 802.15.4 for extending this functionalities to the different other layers. So, if you recall 802.15.4 is useful for establishing connections and function functionalities in the physical layer and the MAC layer. ZigBee basically will take these functionalities to the higher layers network and beyond network layer and beyond.

(Refer Slide Time: 16:08)



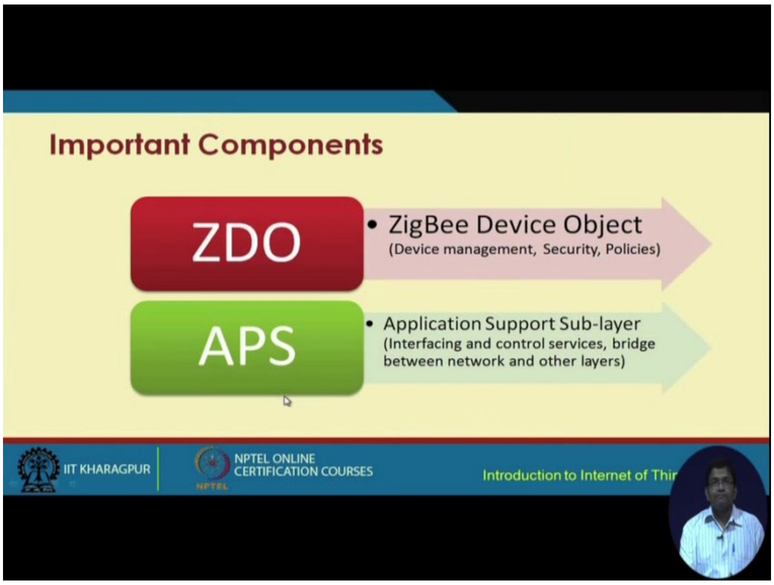
So, let us look at how ZigBee basically functions. So, ZigBee protocol is defined by the layer 3 and above. So, it works on top of layers 1 and 2 of 802.15.4 and extends to layer 3 and above and ZigBee basically works on top of 802.15.4. So, this is something that we have to understand and we have to remember that there is a difference between 802.15.4 and ZigBee.

This is what many people often confused. People think that ZigBee and 802.15.4 are one and the same, but it is not. So, ZigBee is definitely based on the 802.15.4, but it has its own distinct identity. So, the ZigBee basically uses layer 3 and layer 4 to define additional communication enhancements and these enhancements include authentication with valid nodes encryption for security and data routing and forwarding capability that enables mesh networking and ZigBee is typically used in wireless sensor network applications. It is heavily used in wireless sensor network applications, where mesh topologies are formed with the help of ZigBee.

(Refer Slide Time: 17:27)

So, this is a diagraph diagram which basically shows the position of ZigBee with respect to 802.15.4. So, where is 802.15.4, it focus is mostly on the 5 and the MAC layers ZigBee takes it beyond MAC beyond network layer. So, network layer and the rest of the layers all the way up to the application layer basically this extension or the enhancement is made possible with the help of ZigBee over the 802.15.4 protocol.

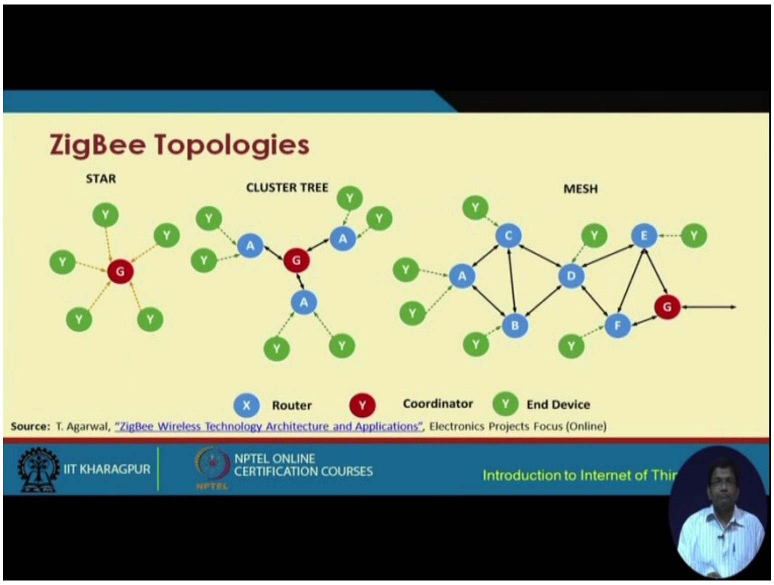
(Refer Slide Time: 18:06)



In ZigBee there are primarily two different components. The first one is known as ZDO which stands for ZigBee device object and it takes care of issues such as device management, security provisioning policies and so on. So, these are the different functionalities of ZDO and that means the ZigBee device object component.

The second component is APS which stands for Application Support Sub-layer which takes care of services such as control services, interfacing bridging between network and other layers and so on. So, these are the two distinct components with separate functionalities as we have just gone through.

(Refer Slide Time: 19:02)



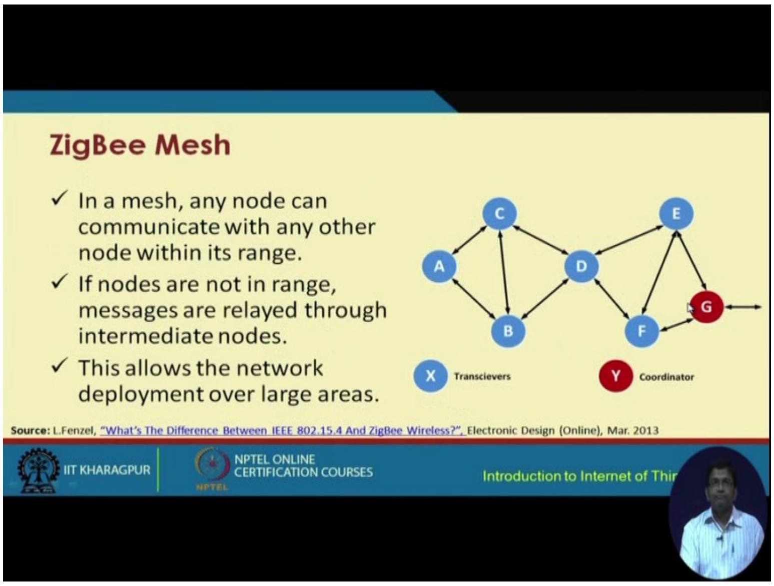
So, ZigBee basically supports star topology. So, this is the star topology that we see over here and we do not need to elaborate on this further. So, we have this controller node and we have these different age devices and these age devices, they form a star topology with the coordinator node. Sorry it is not the control; it is a coordinator node along with the coordinator.

Then, we have this coordinator node can be a gateway node also and this can be a simple local area network or local area network equivalent. Then, we have the cluster tree topology, where these are like different clusters that are formed with these different blue colored cluster head which basically in reality are things such as routers and hubs.

So, these will act as routers and these routers will form a tree like structure with the coordinator node. So, this is why this is known as the cluster tree topology and then, we have the mesh topology which is forming a mesh network with the help of these different routers. These different routers, they form a mesh backbone kind of network and to each of these routers, these different devices are attached.

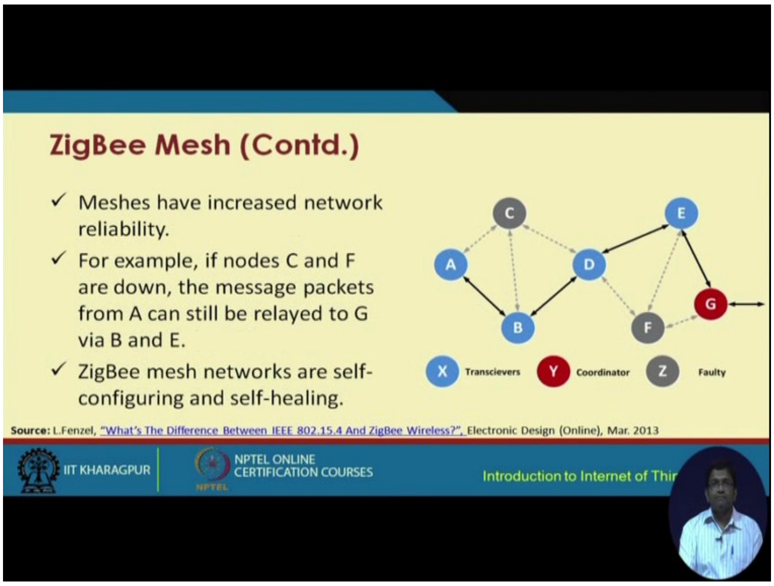
So, basically these green device are the end devices in this particular diagram and these green devices attached to these blue devices which basically denote the the routers and at the end of this mesh network on one end, we have this coding and then, node which acts as a gateway and from this point on it offers connectivity to the outside network such as the internet

(Refer Slide Time: 21:17)



So, in a mesh any node can communicate with any other node within its range. So, this is the main advantage to offer faulty tolerance, reliability. Meshtopologies are very much useful. So, if the nodes are not in the range, messages are relayed through intermediate nodes. So, this allows the network deployment over large areas. So, using mesh topology you can extend the network to larger areas, you can span across larger area. So, this is possible with the help of the meshtopology.

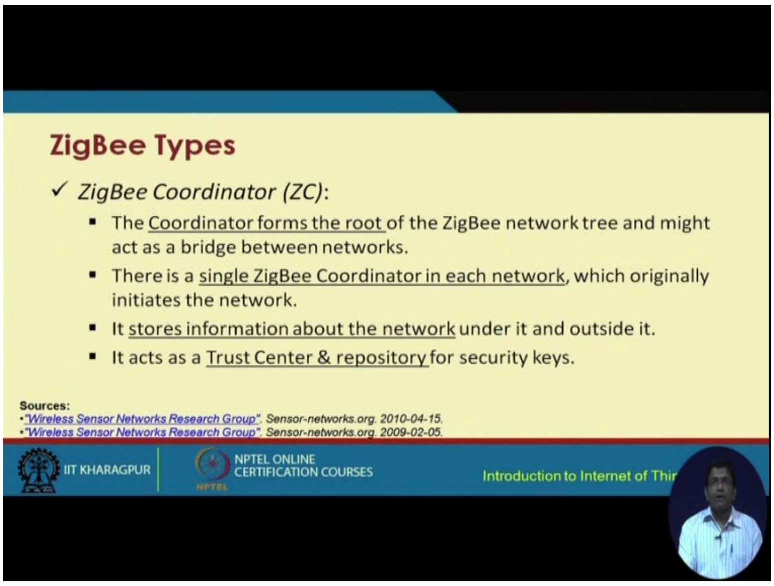
(Refer Slide Time: 21:52)



So, the meshes have increased network reliability. For example, if nodes C and F are down in this particular scenario, so let us say that initially we had this kind of a mesh. Now, if the nodes C and F, these routers are down for one reason or another, the messages can still go from A to Z using this particular path because an alternative path was possible to have in because it is a mesh network.

Now, the ZigBee mesh networks are self-configuring and self-healing. Self-healing is quite obvious because if there is some link failure or node failure or something, it is possible to have other alternative routes and yes they can configure on their own, they can form the network on their own. So, this is the advantage of the ZigBee mesh network.

(Refer Slide Time: 22:49)

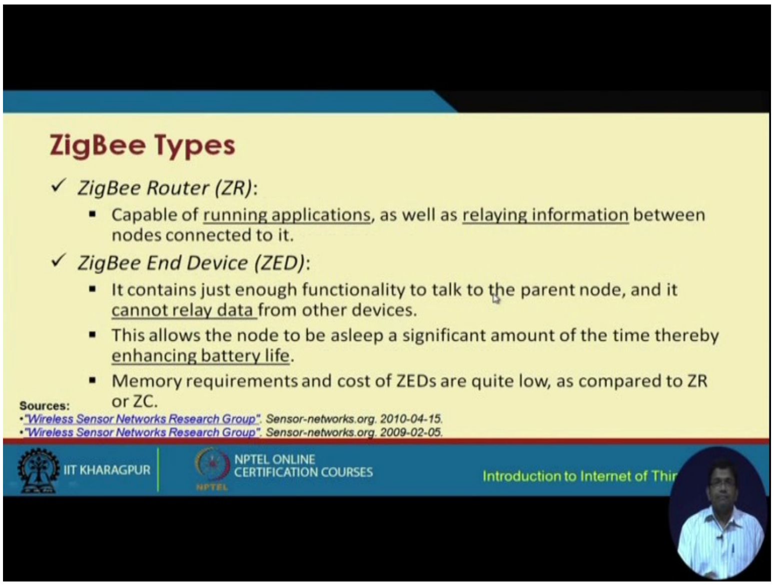


So, in ZigBee there are different entities. The first one is the ZigBee coordinator, ZC. The ZigBee in the coordinator basically forms the root of the ZigBee network.

So, the entire network or the network tree has a route and these routes are known as the ZigBee coordinator and form this coordinator. So, first of all there is a single coordinator and from this coordinator, there is single hop connectivity to the end devices. So, this coordinator basically stores information about the network which is under it and which is outside it.

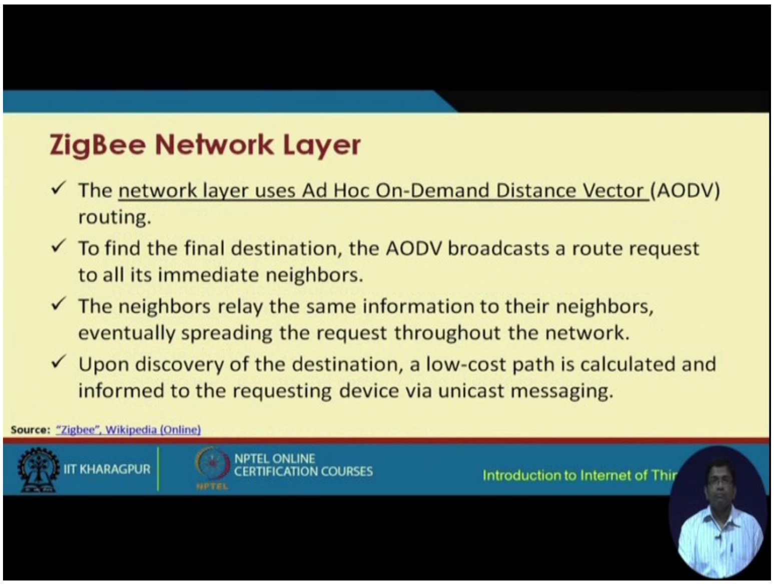
So, basically you know it is sort of buffers some of this information that I received from these end devices and stores with it for certain time. It buffer for some certain time. So, it also acts as a trust center and repository for the security keys.

(Refer Slide Time: 23:54)



Then comes the ZigBee router which is capable of running applications as well as relaying information between the different nodes that are connected to it and then, we have the end device which contains just enough functionality to talk to the parent node and it cannot relay data from other devices. So, it has reduced functionality. So, it is a reduced functionality device.

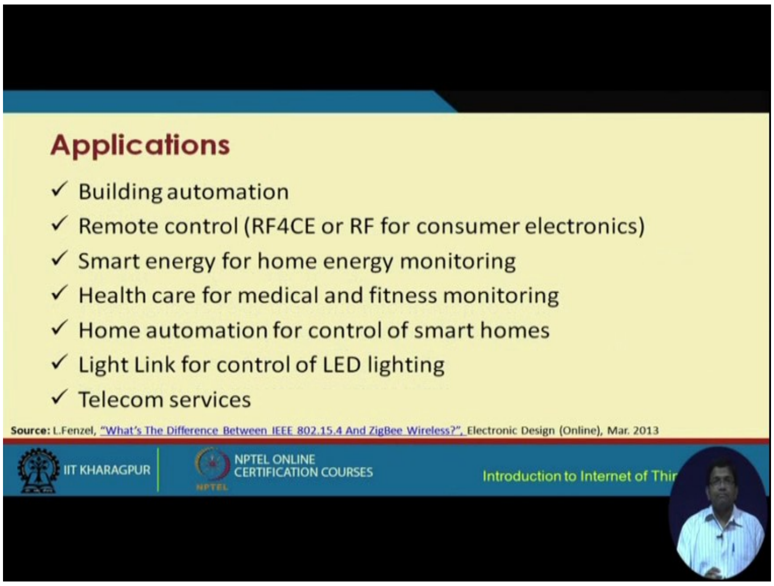
(Refer Slide Time: 24:21)



Now, ZigBee also incorporates a network layer. So, this network layer uses the ad hoc on demand distance vector routing protocol which is the AODV protocol and it is been popular in the case of ad-hoc networks. It is used mostly in the ad hoc networks for as a routing protocol that operates in the network layer and it used to find the final destination. So, how it can be found? AODV basically this particular protocol, it broadcasts a route message to all its intermediate neighbors.

These neighbors basically they relay the same information to their neighbors intern and eventually this message space across throughout the network. Upon discovering of destination, a low cost path is calculated and is informed to the requesting device via the unicast messaging. So, this is how this particular protocol functions.

(Refer Slide Time: 25:20)



So, ZigBee has different applications and it can be used for building automation smart homes, smart health care, telecom services, offering link connectivity to led lighting systems, then smart energy for home, energy monitoring, building automation. I think I have already mentioned remote control and so on so forth.

These are the different applications where this ZigBee protocol can be used. So, we come to an end of this. So, we have discussed two very important protocols IEEE 802.15.4 and the ZigBee protocol in this particular lecture. We have seen that where as the 802.15.4 it is primarily restricted to the physical and the MAC layers ZigBee basically extends it or enhances its functionality beyond network layer and all the way up to application layer.

So, ZigBee basically uses the protocol AODV for routing purposes and it is one of the very popular protocols that is used for sensor networking applications particularly using the mesh topology and we have all seen that there are different types of topologies are there i.e. star topology, cluster tree topology, mesh topology and so on. Mesh topology is particularly useful when there is higher reliability that is required from the network deployment for the application for which it is being used.

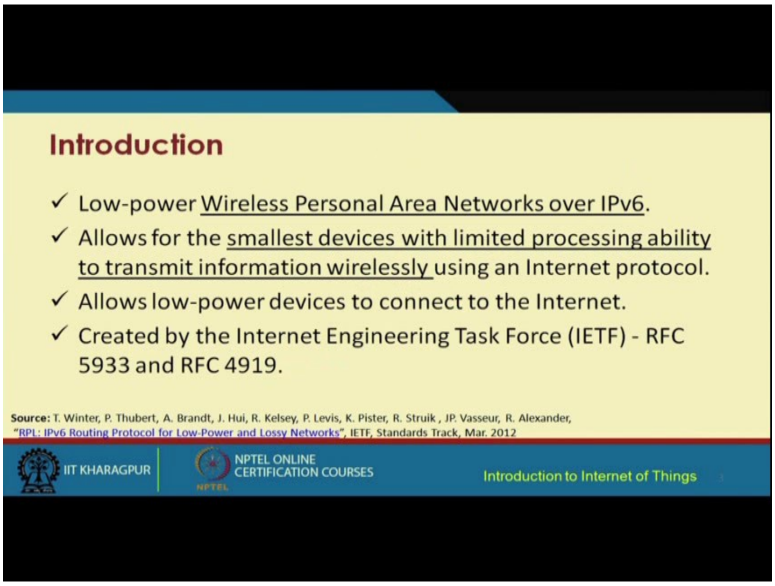
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 10
Connectivity Technologies- Part-II

The next protocol that we are going to go through is also for offering connectivity between different devices forming the connectivity and this protocol is the 6LoWPAN protocol. So, this 6LoWPAN protocol is basically it runs over IPV6 that is from where this 6 figure comes. So, it is from IPV6. So, it runs over IPV6. So, it offers radio connectivity, radio linkages over IPV6 protocol. So, using IPV6 protocol and IPV6 as we know is for addressing, it is an addressing protocol and it is very popular for use for addressing in the case of IoT networks because of the large address space that is required for IoT. So, let us look at this 6LoWPAN protocol.

(Refer Slide Time: 01:16)

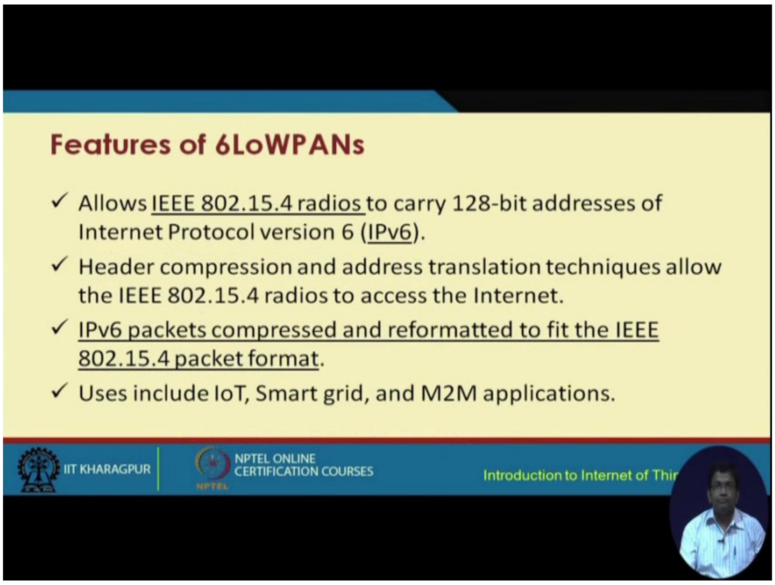


So, it stands for 6LoWPAN stands for Low Power Wireless Personal Area Network over IPV6 and it allows for the smallest devices and each of these devices having limited processing ability to transmit information wirelessly over the internet protocol.

So, we have low power small devices limited processing capability as is typical of IoT systems and wireless communication being present. So, it basically helps in establishing connectivity in this kind of networks. So, it basically helps this 6LoWPAN protocol, it helps and allows to have this low power devices to connect over the internet because IPV6 is going to be used for addressing.

So, at the network layer, that is the reason why this protocol is useful for connecting this IoT network. These low power devices to the internet, it is basically created out of the IETF RFC 5933 and RFC 4911. So, these are two different RFC based on which this 6LoWPAN protocol is specified. So, this specification is available in these RFC's.

(Refer Slide Time: 02:48)

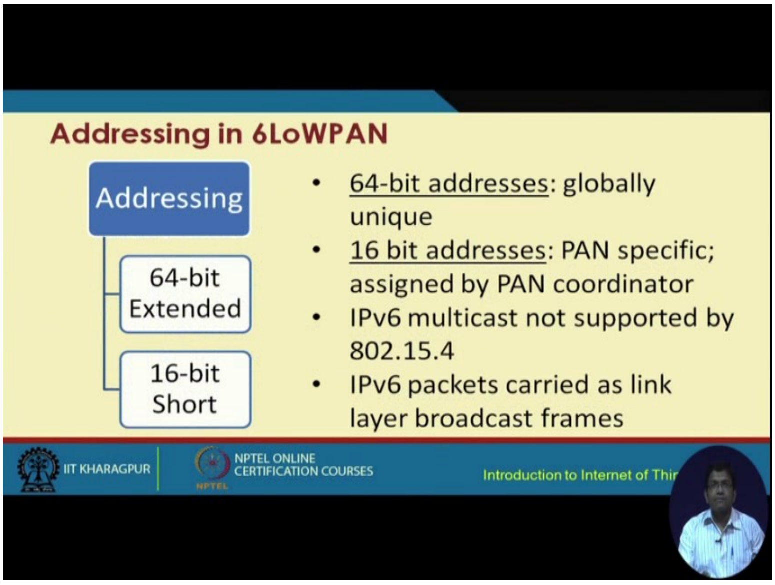


So, these are some of these features of 6LoWPAN and it allows IEEE 802.15.4 radios. That means, in the previous lecture we have gone through this particular protocol which is useful for setting up connectivity between the different nodes and it primarily operates at the physical and the MAC layers. So, the radios of the 802.15.4 is used to carry 128 bit addresses of the IPV6.

So, basically 6LoWPAN is an application or its joining you know conceptual joining of 802.15.4 radios with IPV6, but how it is made possible because you know 802.15.4, it is low powers in light weight protocol and IPV6 is not lightweight. So, how it is made possible? So, the header it is possible with the help of header compression and address translation techniques that basically helps to convert 802.15.4 radios to access the internet.

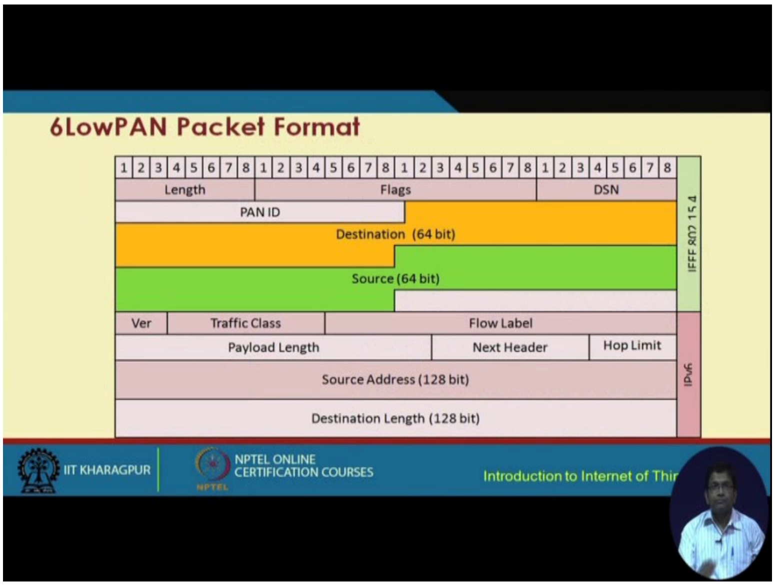
So, it will help this 802.15.4 radios to access the internet using header compression and address translation techniques. IPV6 packets are compressed and reformatted to fit the 802.15.4 packet structure. So, this is what is done. IPV6 packets large in size, they have to be compressed, they have to be reformatted and they have to be mapped with the packet format of 802.15.4 which is primarily meant for low power networks, small scale low power networks as is typical of IoT.

(Refer Slide Time: 04:58)



So, it can be used for, IoT 6LoWPAN can be used for IoT smart grid applications, smart home applications, M2M applications and many other different, similar applications. So, for addressing in 6LoWPAN, there are two types of addresses that are used i.e. 16 bit short address which is for PAN specific communication. That means, it is assigned by the PAN coordinator for communicating within the PAN, the personal area network and 64 bit extended address which is used for global unique connectivity, global unique addressing throughout the network.

(Refer Slide Time: 05:45)

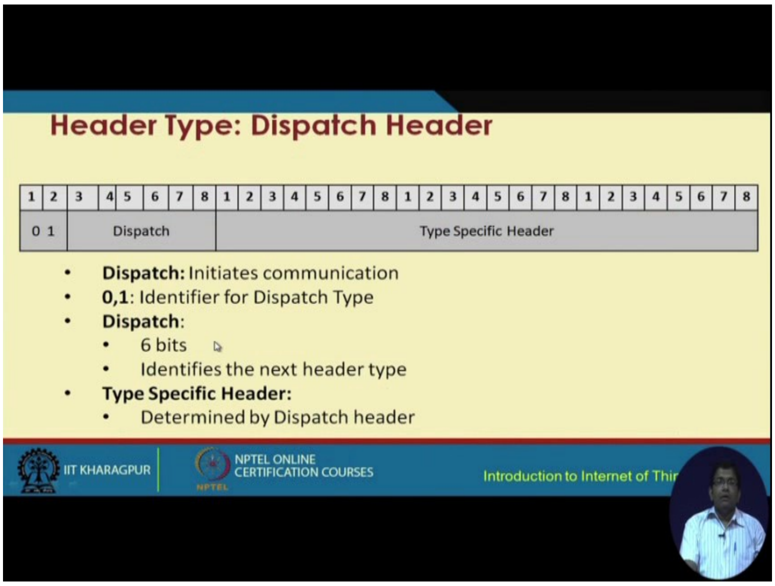


So, IPV6 multicast is not supported by 802.15.4 and IPV6 packets are carried as link layer broadcast frames in the case of 6LoWPAN. So, we have in front of us the packet format of 6LoWPAN. So, as we can see over here if you look very closely, we have 802.15.4 and IPV6 club together 802.15.4 radio and IPV6 for addressing over the internet and these corresponding fields are also shown over here.

So, what we have for corresponding to IPV6? We have the source address, the destination address and these different other IPV6 fills that are typical in this particular protocol IPV6 protocol and for 802.15.4 as well, there is this source, the destination both of which are 64 bits. That means, source and destination together will become 128 bits.

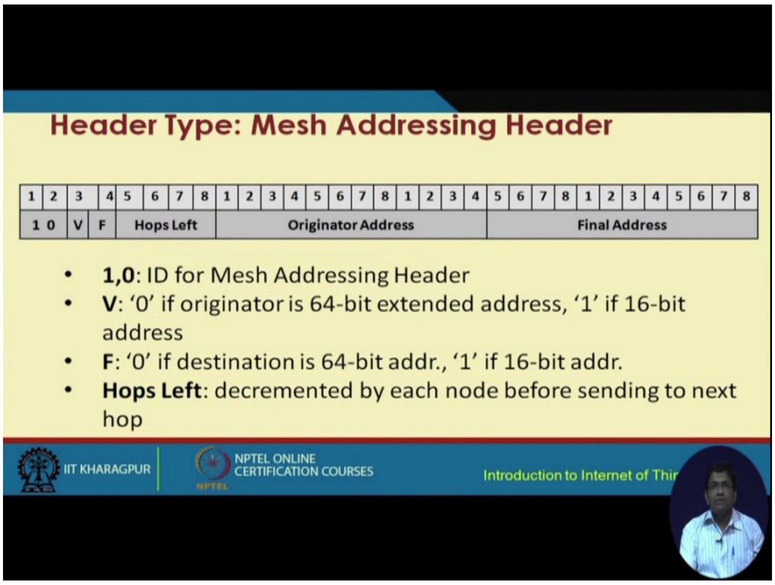
Then, we have this PAN ID because you know when we are talking about 15.4 networking mode go to personal area network. So, the PAN ID is basically stored in this particular field. So, this is how the 6LoWPAN packet format looks like.

(Refer Slide Time: 07:06)



So, that is the packet format. Now, what about the header? There are three different types of headers. One is known as the dispatch header, the second one is known as mesh addressing header and the third one is known as fragmentation header.

(Refer Slide Time: 07:17)

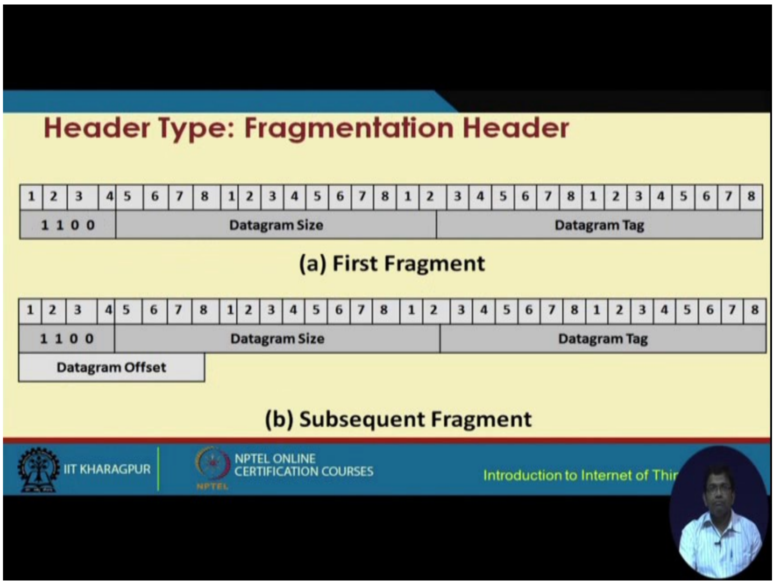


So, let us look at these three different headers. The format of these headers is given over here. So, how many bits we have? We have 8, 16, 24, and 32. So, the header is 32 bits long, out of which the first two bits are used to identify the dispatch type and this dispatch type basically helps in the dispatch communication initiating the communication resetting the communication.

Now, this dispatch field has 6 bits. So, it is 6 bits long field and these basically identifies the next header type and there after the next list of the bits are used to specify the type specific header and that is determined by the dispatch header. So, then we have the mesh addressing header and here basically the first two bits are used to store the ID of the mesh addressing header.

The next field, the V field is 0. If the originator is 64 bit extended address and we have seen that both of these are possible to have 16 bit as well as 64 bit address. The F field is 0 if the destination is 64 bit address and 1 if it is 16 bit address and hops left are decremented by each node before sending to the next hop.

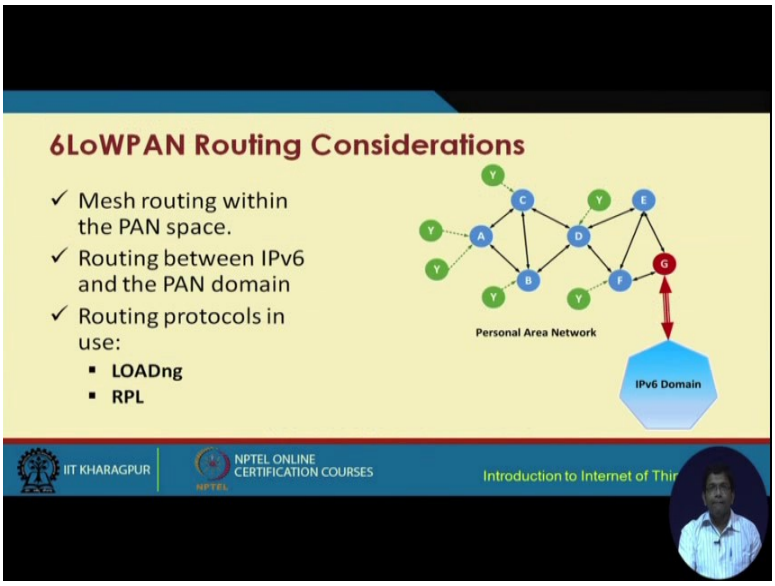
(Refer Slide Time: 09:49)



So, how many hops are left until the final destination node? This is basically stored in this particular field and is decremented as I said hop by hop when one hop is over, it is complete, that field the value is decremented by 1 and third fragment type is a fragmentation header and the corresponding fields are shown over here. So, in this case, the first fragment has this structure, the header has this structure as shown over here and the subsequent fragments have this particular structure.

So, as you can see over here, the main difference between the first fragment and the subsequent fragments is the inclusion of the datagram offset.

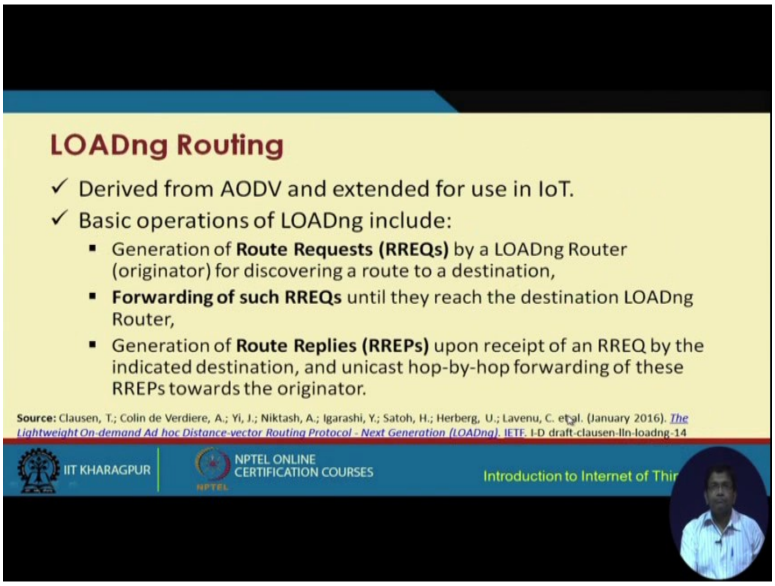
(Refer Slide Time: 10:42)



So this datagram offset basically shows that it will give the value of what are the subsequent frames that are there. So, this will basically help to connect with the first frames; so 6LoWPAN because it involves a strong network layer component and it takes care of routing.

So, the most important type of routing is a mesh based routing and this mesh based routing is used in the context of a PAN topology, Personal Area Network Topology. So, routing is used, routing basically is based on the IPV6 protocol in the personal area network domain and there are two protocols that are used in 6LoWPAN for routing.

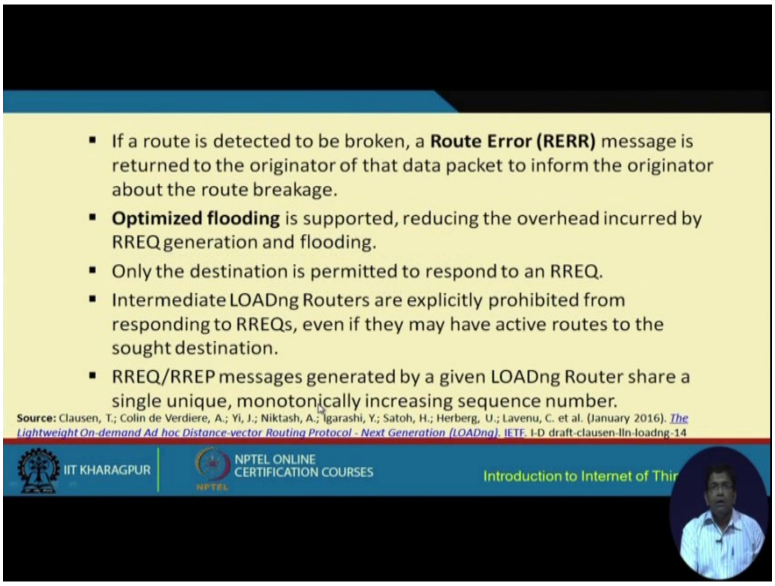
(Refer Slide Time: 11:40)



One is the LOADng protocol and the other one is RPL protocol and as you can see over here from this particular figure, we have this IPV6 domain and we have this personal area network PAN and with the help of this coordinator of the gateway, it connects to the IPV6 network. That means, the IPV6 based internet, the LOADng routing protocol, it is primarily a derivation from the AODV protocol that is available and was proposed for ad hoc networks and this has been used and extended for IoT networks.

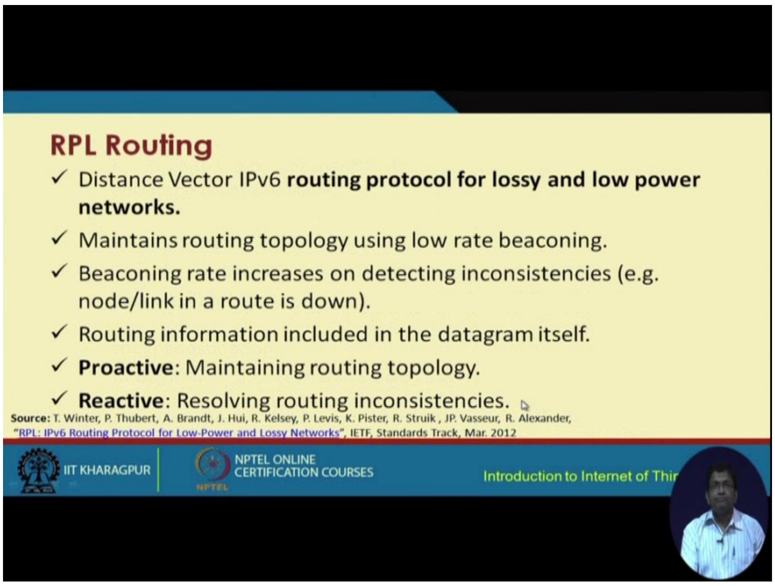
So, this LOADng protocol has few different PDOs. The first one is the load request PDOs and it is generated by a LOADng router, the originator for discovering a route to the destination. So, the forwarding of such route requests take place until they reach the destination LOADng router, then comes the route replies which is generated upon receipt of the route request by the indicated destination and unicast hop by hop forwarding of these route replies towards the originator.

(Refer Slide Time: 12:48)



There is also this route error message that is used to return errors to the originator of the data in the event that there is some route breakage that take place. So, optimized routing is supported reducing the overhead that is in cut by the route request generation and flooding only the generation is permitted, sorry only the destination is permitted to respond to the route request. Intermediate routers of LOADng are explicitly prohibited from responding to the route request even if they have been very active in terms of seeking routes and generating routes in the network.

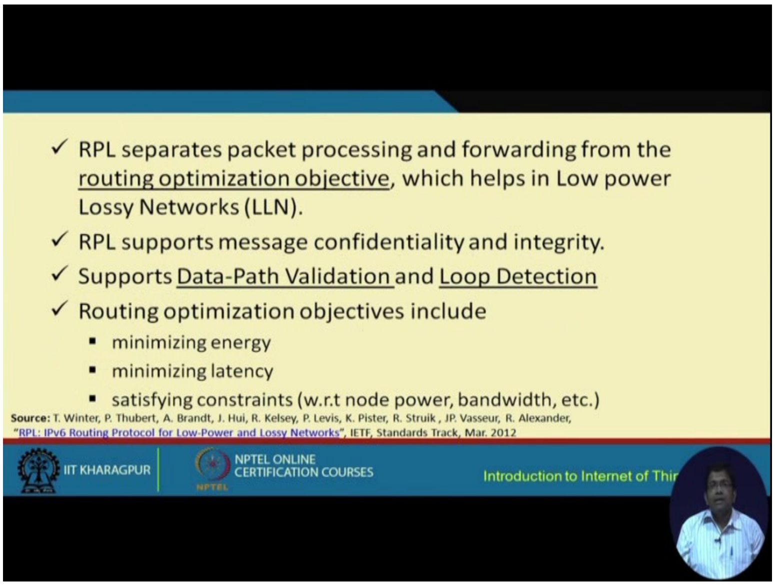
(Refer Slide Time: 13:40)



The route request and route reply messages are generated by a given LOADng router and this share a single unique monotonically increasing sequence number. Next comes RPL, Routing Protocol which is based on the distance vector routing for lossy and low power networks. So, this is where this l comes from this lossy. So, it is used for lossy networks as well as low power networks for routing.

So, it maintains routing topology using low rate beaconing. Beaconing rate over here increases on detecting inconsistencies with respect to situation such as load failure or link failure. Routing information is included in the datagram itself. It uses two types of routing proactive i.e. routing for maintaining, routing topology and reactive for dissolving routing inconsistencies.

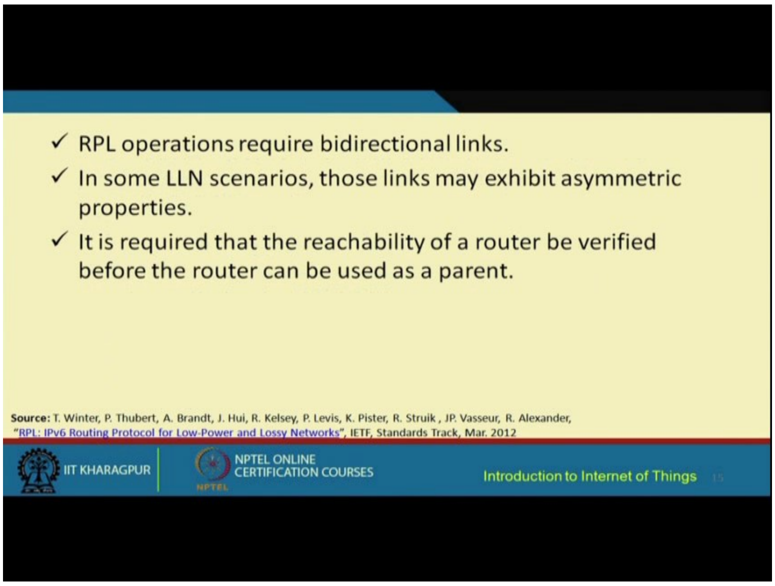
(Refer Slide Time: 14:31)



The RPL basically separates the packet processing and forwarding from the routing optimization objective which helps in Low Power Lossy Networks, LLN.

So, this particular protocol, it supports features such as confidentiality, integrity, ensuring integrity, validating data paths and detecting the presence of loops. The overall optimization objectives of routing include minimizing the energy minimizing.

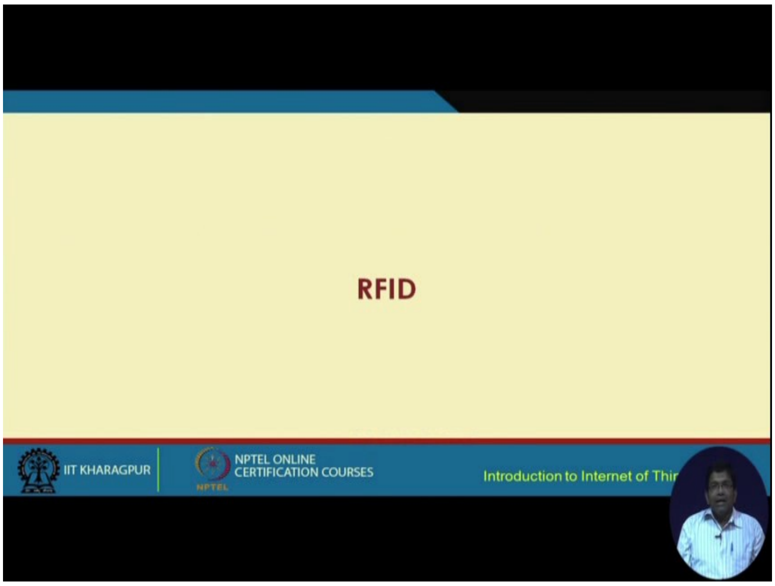
(Refer Slide Time: 15:16)



The latency and satisfying the constants with respect to node power bandwidth etcetera, this RPL protocol operates using bi-directional links. So, there is bi-directional flow of communication of messages.

So, in some LLN scenarios, that mean the lossy scenarios, these links may exhibit asymmetric properties, right. So, basically asymmetric property means that while the message is sent from the source to the recipient, it flows through one route may be directly, but because of all these environmental situations or whatever the response or the flow of message in the other direction does not take place through the same route. Maybe it comes back through another route. So, it is asymmetric. So, it is required that the reachability of a router is verified before the router can be used as a parent.

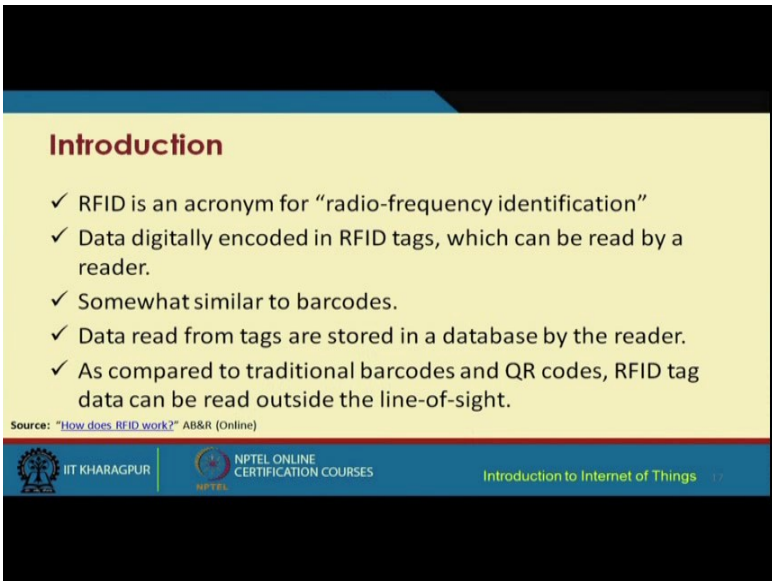
(Refer Slide Time: 16:05)



Finally for this particular lecture, we are going to go through the protocol RFID. RFID is very popular. It is commonly used. It has been in use for long, it is still used in shopping malls. What places you know? For example, the ID cards are fitted with RFID tags. RFID tags can be scanned in the RFID readers. Similar things happen in the shopping malls like when we go for purchase in certain items, for example, clothing sensors these also are fitted with these RFID tags and these RFID ID tags can be used to scan against RFID readers to get further information and so on.

So, how does RFID work? RFID is we have to remember that sensor networks and RFID sensor networks we have not yet covered. We will cover in a subsequent lecture, but RFIDs and sensor networks and also other technologies, such as zigbee, 802.15.4, for w PAN, NFC also which is very similar to RFID. These are different other connectivity offering mechanisms that are popularly used for IoT applications. So, these are the core for establishing connectivity in IoT networks.

(Refer Slide Time: 17:36)

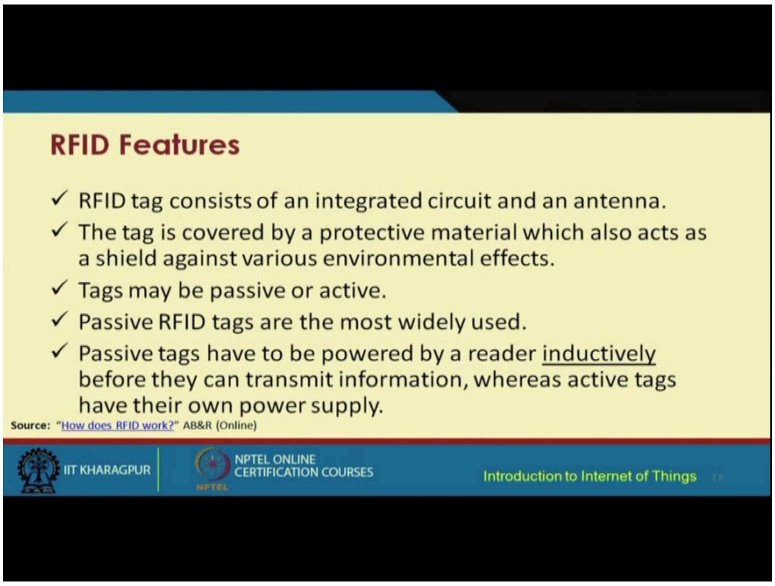


So, going back to RFID, we have first of all RFID, its an acronym for Radio Frequency Identification, where the data is digitally encoded in these RFID tags and these data can be read from the RFID tags. So, RFID tags are encoding the data and these data can be scanned from RFID tags by the RFID reader. So, these are very similar to the bar coding schemes and QR coding schemes.

So, in a barcode what happens in a barcode like in libraries ecetera, in a bar, bar coding schemes are typically used to store information about the books and you know having the identifiers for the books. So, the barcode basically are like vertical lines, right. So, there is a barcode reader which can read those vertical lines. Similarly there is QR code which is sort of like that square square kind of thing which is used for scanning the data, right. So, these are the QR codes.

So, there is that reader which can take that image and it can basically process that image to identify the data that is embedded in that particular code. So, RFID tags are also very similar in operation to the barcodes and QR codes, but the functionality or the way these operate are vastly different. So, let us now try to understand how RFID tags, the RFID principle works.

(Refer Slide Time: 19:30)

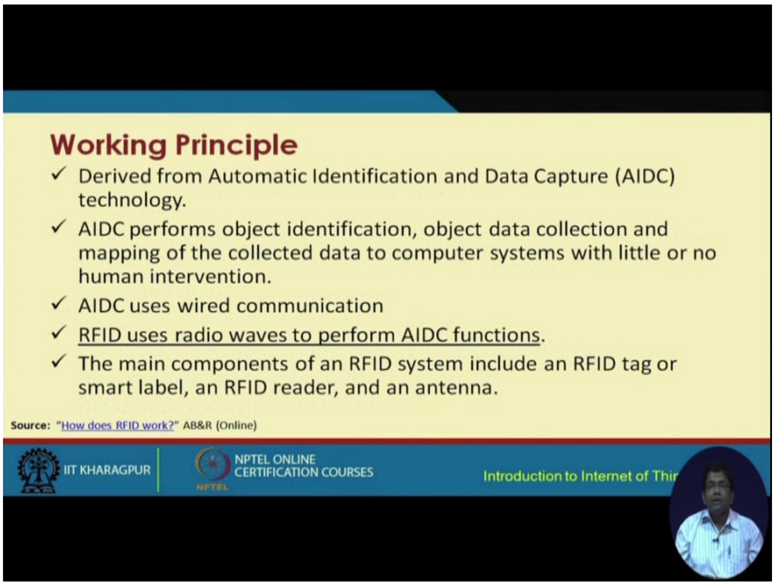


So, every RFID tag consists of an integrated circuit and an antenna. So, basically it is a very small tag. So, tag inside the tag, there is some circuitry that is there and a small antenna which is embedded into it, inside it. So, this antenna, is going to be used it is going to be used for communication with the outside world. That means, outside the tag and the circuitry basically does number of things including storing the information in that particular tag, may be the RFID tag could be for a smart card that can be used for storing employee information.

So, you know employees in an organization have different identification for different identifiers and those identifiers, the different data can be stored in electronic form inside the chip that is built into this RFID tags. So, the RFID tag consists of integrated circuit and an antenna. The tag is covered by a protective material. So, outside the tag is some kind of a shield protective material which can also act as a shield against various environmental effects.

The tags can be of two types. One is the passive tag; the other one is the active tag. So, passive tags are more common and the way these passive tags are operated are through the process of inductivity. So, inductively when these passive tags, when these tags come in proximity to the RFID reader, there is some inductive effect, some magnetic force fields are created due to which the information is transferred from the tag to the reader or vice versa. So, it is from the tag to the reader and vice versa. Those are the passive tags.

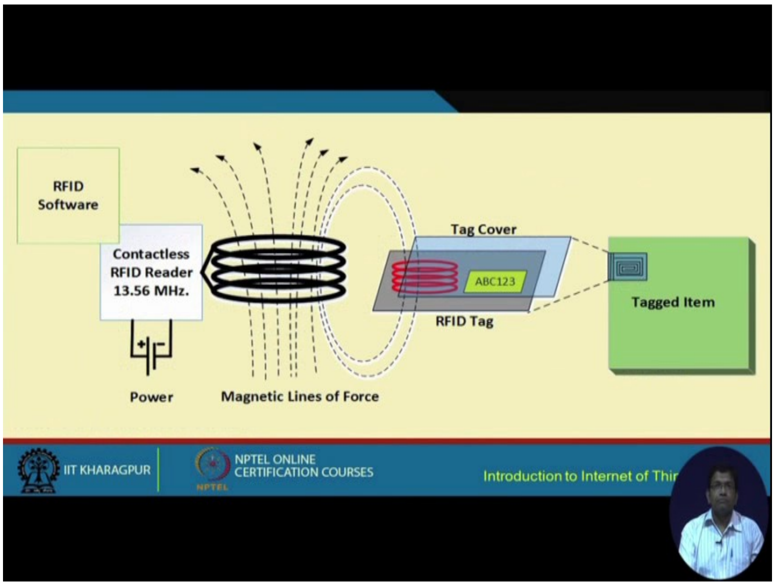
(Refer Slide Time: 21:39)



On the other hand, the active tags, they have their own little source of power supply. The working principle of RFID is similar to its predecessor which is called AIDC. The AIDC full form is Automatic Identification and Data Capture Technology. So, it performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention.

So, the concept of RFID is basically adopted from AIDC which is its predecessor. So, AIDC is no longer very common, however the difference is RFID is mostly wireless, not mostly it is fully wireless. On the other hand, AIDC uses wired communication. So, RFID basically uses radio waves that mean wireless communication to perform different functions which are also performed by AIDC.

(Refer Slide Time: 22:44)



So, let us try to understand how RFID works. Let us say that there is a tagged item like clothing or something in a shopping mall, some kind of a cloth. So, this cloth is tagged with this RFID reader, no sorry RFID tag. It is tagged with this RFID tag; it is attached to the RFID tag. This RFID tag consists of the circuitry some kind of a quailing mechanism and the cover.

This cover is some kind of a polymer, some plastic or some other polymer and the circuitry is basically stored inside this particular tag. Then, we have this one if we look over here. So, we have this part, we have this part which basically is for the reader. So, this part is for the RFID tag and this part is for the RFID reader. As we can see over here, this RFID reader has a software and a source of power supply and it also has a coil and when you bring that reader which has a coil inside some magnetic coil, then there is this magnetic inductive effect producing this magnetic lines of force are created.

(Refer Slide Time: 24:37)

So, this is how the data that is there in that small chip inside the RFID tag is transferred to the RFID reader with the help of this force field magnetic force, field RFID tags. RFIDs in general are useful for supporting different IoT applications such as inventory management, asset tracking in an organization, personal tracking you know who is coming when, who is living when in an organization, what is the attendance.

So, attendance tracking systems for example, controlling access to restricted areas. So, you know whoever is authorized will be having an RFID tag and they can bring it in close proximity to the RFID reader and if it is a valid tag, then the door is going to open for that person and the person can get in. So, it is used for controlling access to the restricted areas.

Id badging as basically you know identity badges, smart cards in an organization, it is used for that supply chain management counterfeit prevention particularly in the pharmaceutical industry. So, these are different applications of the RFID tags.

So, with this we come to an end of this particular lecture and there are few other protocols that are also very much useful, and we are going to go through them in the next lectures.

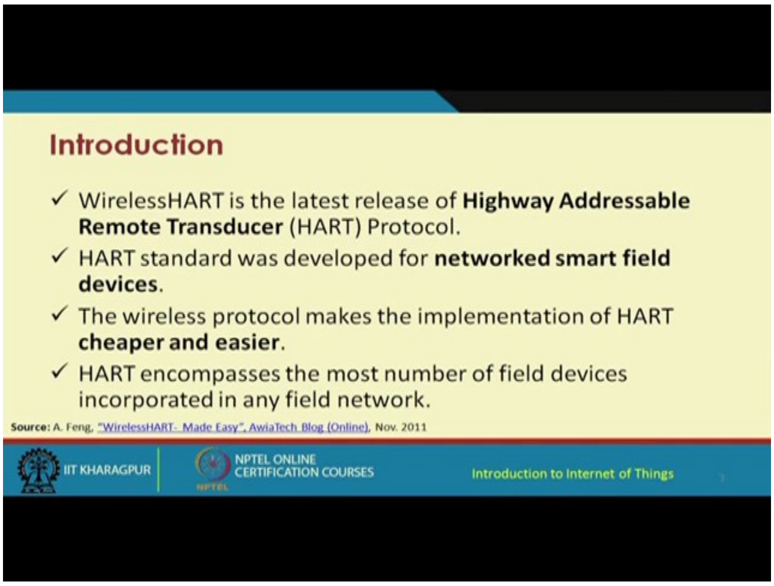
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 11
Connectivity Technologies – III

For connectivity we have already gone through different technologies, which offer communication in IoT. Technologies such as zigbee, 6LoWPAN and the like. They are based on either they use either they are developed on top of 802.15.4 for instance the way zigbee has been developed. Or they use 802.15.4 standard the way 6LoWPAN does. Likewise there are other technologies which are sort of derived from or are based upon the IEEE802.15.4. Technologies such as hart and wireless HART, are 2 such technologies that we are going to cover in this particular lecture. So, HART the full form of, the full form of HART is highway addressable remote transducer protocol.

(Refer Slide Time: 01:37)

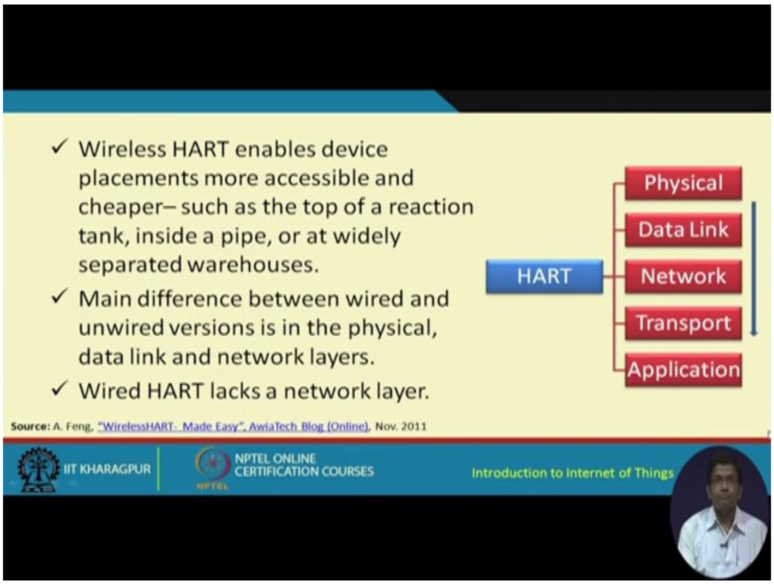


So, highway addressable remote transducer protocol HART and it is latest version which is a wireless version of it which is a wireless HART are 2 such technologies which are sort of derived from 802.15.4 standard. So, all these 802.15.4 standard based technologies and the protocols they are very useful for setting up IoT communication. The reason is that they enable short range you know, different data rate communication between low power devices as are found in IoT systems.

So, we will go through the HART and the wireless HART and the overview of it to understand how it functions and what are it is different features. So, the genesis of HART and wireless HART goes back to industrial IoT IIoT industrial IoT which is again one of the lectures that we are going to have in the future in this particular course. So, for many of these industrial applications such as industrial plants or vehicular networks connected vehicular etcetera. So, what is required is to set up some kind of is network between different field devices, to form a smart system a smart network. And this is what is required in IoT.

So, HART basically helps in the same way as zigbee does for establishing connectivity between different IoT devices. And the special the special focus of HART is on industrial applications. So, the HART protocol has been designed and is implemented in such a way so that it becomes cheaper and easier to implement in an IoT system. So, HART basically encompasses the most number of field devices incorporated in any IoT network.

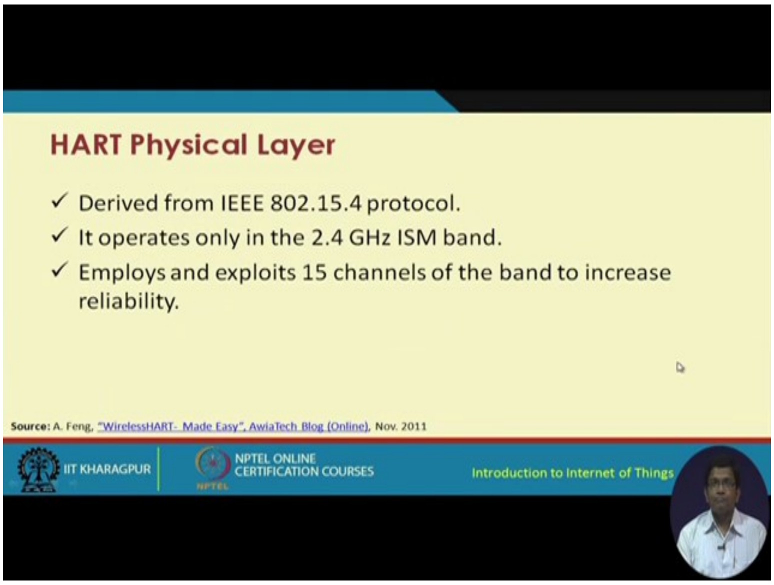
(Refer Slide Time: 04:13)



So, talking about HART and wireless HART it basically helps to, ensure accessibility of different devices. And the placement of such devices in such a way that it becomes cheaper to develop the overall system. The system becomes overall efficient and typically this protocol is implemented on top of a reaction tank inside a pipe or at widely separated warehouses, to have connectivity between these different components or different parts of the warehouse or the reaction tank or the pipes etcetera.

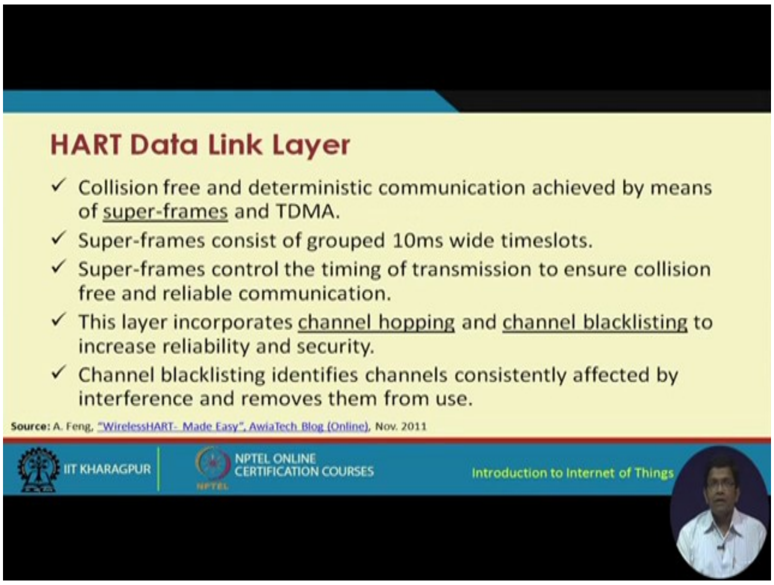
So, the main difference between HART and the wireless HART is in the physical data link and network layers. So, the wireless HART and the HART they are almost the same except that there are certain differences in these specific layers of physical data link and network, and we are going to go through them in a little bit more detail. So, we have to also keep in mind that wired HART basically does not have support for a network layer. So, looking at HART and the wireless HART what we have is a physical layer, data link layer, network layer, transport layer and application layer.

(Refer Slide Time: 05:43)



So, the physical layer as I said, is derived from the basic standard the most popular standard for IoT implementation the 802.15.4 IEEE standard. And this protocol the HART protocol functions in the ISM band, or the more specifically the 24 gigahertz ISM band. It implies and exploit is 15 channels of the band in this particular ISM band to increase the reliability of the network. So, that is the physical layer with support for 802.15.4 derived reduced.

(Refer Slide Time: 06:20)

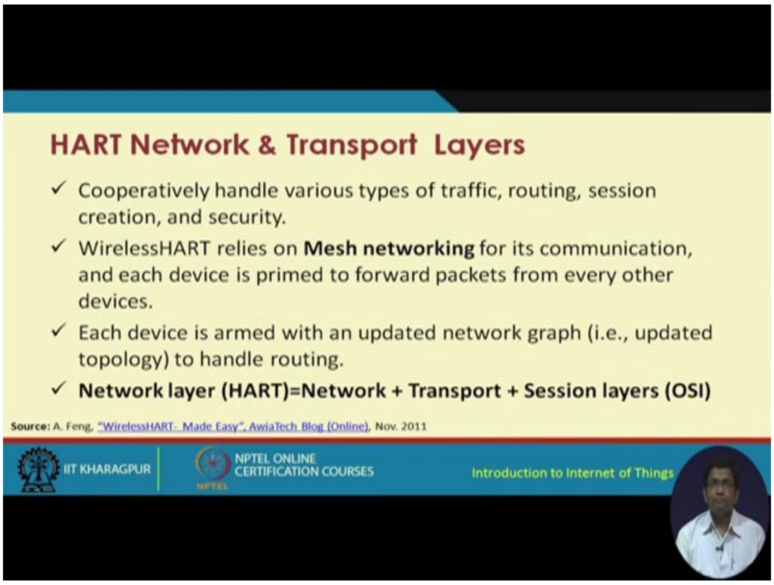


Then comes the data link layer. The data link layer has a concept of something known as the super-frames. And the super-frame basically helps in ensuring reliable communication, collusion free and deterministic communication between the different nodes of the network. And it is based on this particular layer it works using a TDMA like protocol, time division multiple access protocol where there are different time slots, when the different devices are able to communicate in those allotted time slots.

So, these super-frames that we are talking about they are grouped into 10 millisecond wide time slots. And the super-frames basically control the timing of transmission to ensure collision free and reliable communication. This layer the data link layer incorporates channel hopping and channel blacklisting to increase the reliability and security. How is it done? How is the reliability and security increased? Because there is channel hopping. So, you know what happens is, a transmission takes place in one of the channels then basically the transmission takes over in another channel at the next time instant. So, there is basically channel hopping. There is something similar to you know oh what happens in frequency hopping, frequency hopping spread spectrum. So, a similar kind of approach is adopted in this particular case as well.

So, because there is channel hopping at different time instance etcetera, that improves the security. You know and also improves the system from being hacked network from being hacked by different intruders or malicious agents. Channel blacklisting basically what it does is it identifies the channels consistently affected by interference and removes them from use.

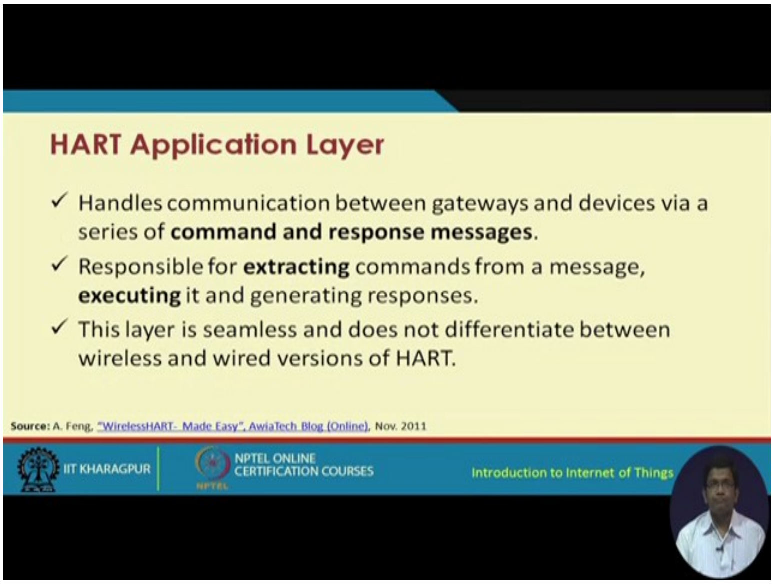
(Refer Slide Time: 08:39)



Now, looking at the network and transport layers after the physical and the data link layers. We see that these two layers they cooperatively handle various types of traffic, routing, session creation and security functions. Wireless HART is based on the mesh networking in communication.

So, a mesh network at the network layer is set up using wireless HART. And each device is primed at different time instants to forward packets for every other device. Each device in wireless HART is armed with an updated network graph; that means, the topology gets updated at subsequent time instants, and that way that particular topology is used to handle routing. So, the network layer in HART basically consists of the OSI network layer, the transport layer and the session layers, put them together and that is what is the network layer of the HART or wireless HART protocol.

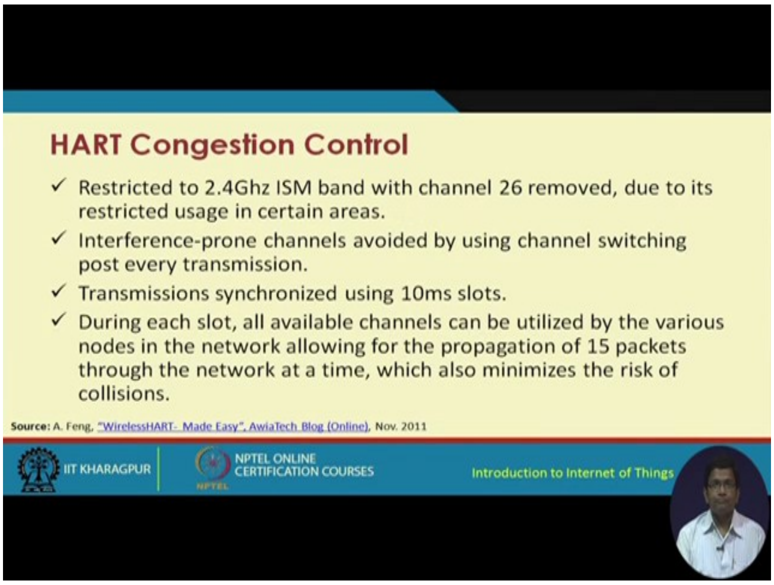
(Refer Slide Time: 09:54)



Application layer in HART handles communication between gateways and devices via a series of command and response messages. So, there are different command messages, response messages and a chain of such message flows take place to implement the application layer. This application layer is responsible for extracting commands from a message, executing it and generating responses. So, in extract the commands from the message, execute those commands and then respond to those commands. So, this layer is seamless and does not differentiate between the wireless and wired versions of HART.

So, irrespective of what is down underneath in the different bottom layers as I said, that there is certain difference between the HART and the wireless HART protocols at the network layer transport layer data link layer and the physical layer. In fact, as I said before pure HART the wired HART does not even have the network layer implemented. So, essentially the most of most of the difference comes in the other three layers which is basically the physical layer, the data link layer and the transport layer.

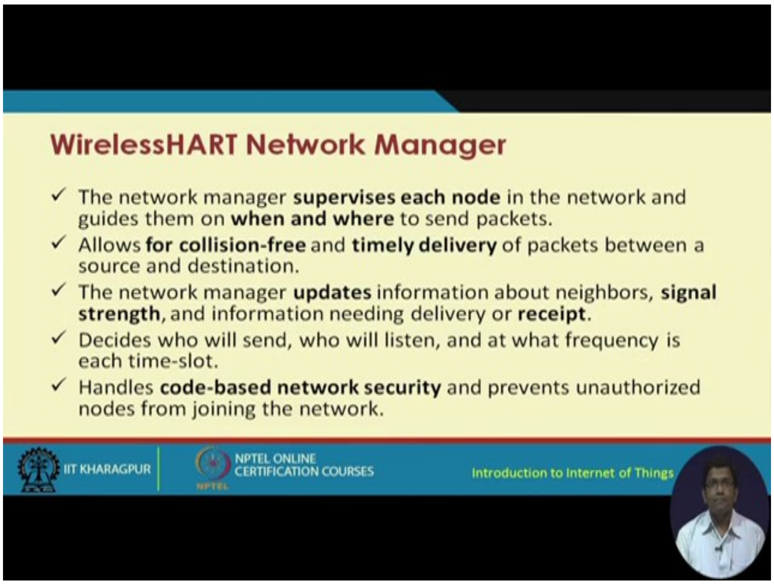
(Refer Slide Time: 11:09)



Now, one of the very important issues of use of HART or any such like protocol is how do you handle congestion. So, congestion is basically handled in different ways. So, we are talking about a 2.4GHz ISM band with channels with channel 26 removed from it.

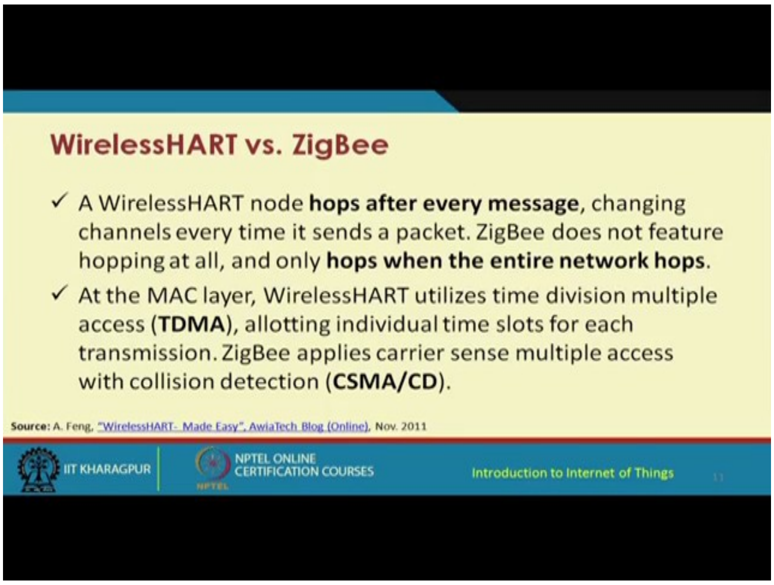
So, there is no channel 26, due to the restricted use of this particular channel in certain areas. So, what we have is interference prone channels avoided by using channel switching post every transmission. The transmission is synchronized using 10 millisecond slots. During each such slot all available channels can be utilized by the various nodes in the network, allowing for the propagation of 15 packets through the network at a time, which also minimizes the risk of collisions. So, this is how congestion is controlled collisions are avoided and not avoided, but minimized and so on.

(Refer Slide Time: 12:14)



Wireless HART uses a something known as the network manager agent. The network manager agent supervises each node in the network and guides them when and where to send the packet. When to send the packet? And where what is the intended destination? So, this is what is the job of the network manager entity in the wireless HART. It allows for this network manager allows for collision free and timely deliver your packets between a source and the destination. The network manager updates the information about the neighbors the single strength and the information needing delivery of receipt. So, wireless HART basically uses something called known as the code based network security to prevent from unauthorized access or unauthorized attempts of different nodes from joining the network.

(Refer Slide Time: 13:12)



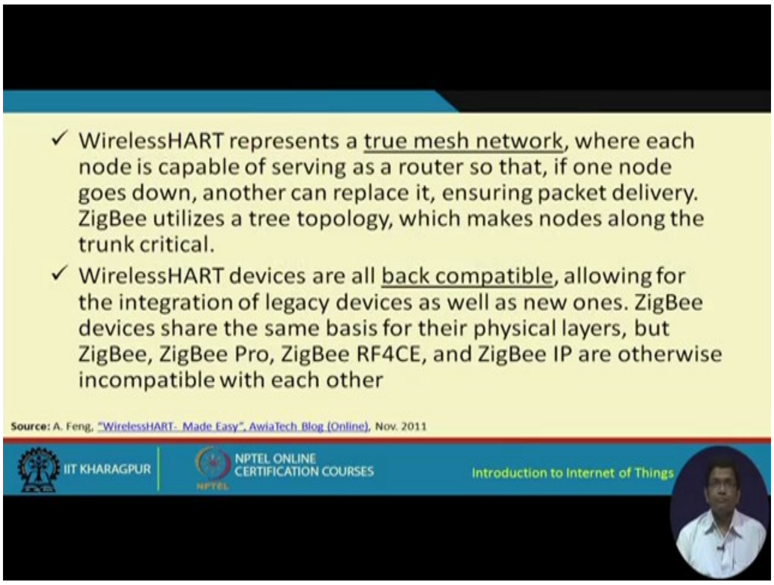
Now, as I in started at the very beginning, that these are all like you know protocols like zigbee or you know IPv6 or wireless HART. The IPv6 protocol has a little bit of different you know functionality from these protocols, but you know if you look at all these protocols, they are all meant for use in low power, low specification, resource constraint, bandwidth constraint, networks and this is where their usefulness in IoT comes into picture.

So, we now need to compare between for instance the popular zigbee protocol and the wireless HART. One thing is zigbee is primarily consumer based IoT. You know zigbee is primarily used for consumer based IoT whereas; HART is primarily used for industrial IoT applications, although nobody limits the use of either of these protocols for consumer or industrial application domains.

So, they can be used interchangeably, but primarily they are based on their implementations consumer iot, zigbee and industrial IoT HART and wellness HART. So, going back a wireless HART node basically hops after every message. And that as I said before improves the security of systems from being attacked or from unauthorized access to the network. Zigbee does not feature hopping at all on the contrary. And it only hops when the entire network hops. So, this is one of the primary points of difference between zigbee and wireless HART. Now at the mac layer wireless HART utilizes TDMA allotting different time slots for each transmission on the other hand, zigbee is primarily based on the MAC protocol CSMA plus, so CSMA/CD or CSMA/CA.

So, CSMA class of protocols. So, zigbee is based on CSMA class of protocols contention based protocols. And TDMA is basically applied in the case of wireless HART.

(Refer Slide Time: 15:44)

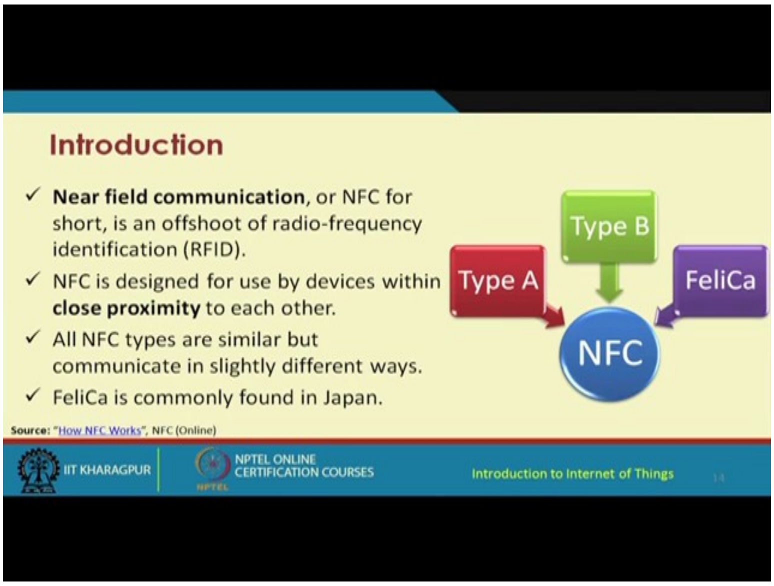


In wireless HART what is used is the mesh network topology where each node is capable of serving as a router. So, that if one node goes down another node can replace it. So, that basically in fact, this mesh networking topology improves the overall delivery reliability of packet delivery in the network. Zigbee use utilizes a tree topology which makes nodes along the trunk critical.

Wireless HART devices are all backwards compatible and that basically allows for the integration of legacy devices as well as the new one. So, this is one of the very important and attractive features behind using wireless HART because, you do not have to totally forget the legacy and the contemporary systems, because it is backwards compatible you can use wireless HART in conjunction to the legacy systems and protocols. Zigbee devices share the same basis for their physical layers, but zigbee zigbee pro zigbee RF4CE and zigbee IP or otherwise incompatible with each other. So, this is also a very attractive or important difference between zigbee and wireless HART

Another very important technology is NFC and this NFC technology as you will see shortly has lot of similarities with the RFID. RFID are also based on something known as magnetic induction. Magnetic induction between the card reader; that means, the RFID card reader and the RFID tag RFID card. And in the case of NFC as well we will see that there is a similarity of this sort.

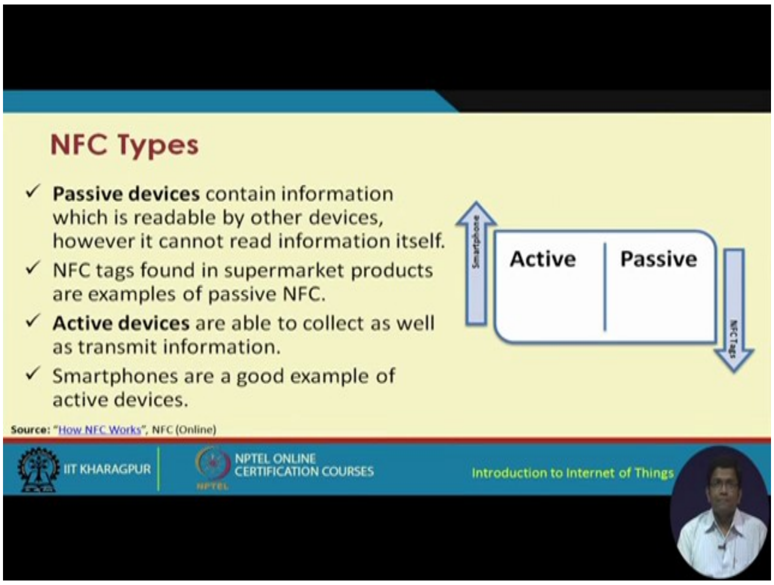
(Refer Slide Time: 17:42)



So, NFC one the full form of NFC is near field communication. And this is basically as I said, is very similar to the RFID technology and this is something the RFID technology is something that we have discussed previously in a previous lecture.

So, NFC is designed for use by devices within the close proximity to each other. All NFC types are similar, but communicate in different ways, a very allied NFC technology, which is known as the FeliCa is commonly found and is used mostly in Japan. The contemporary ones type A and type B NFCs are used in the rest part of the world.

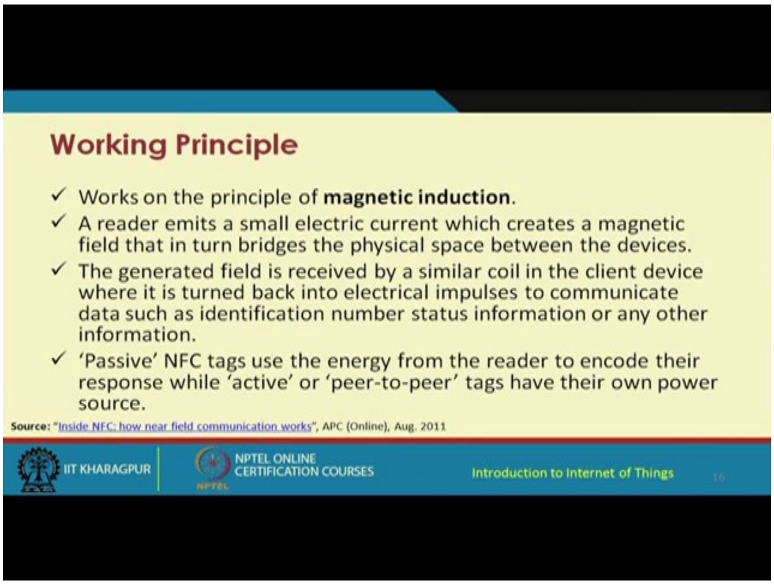
(Refer Slide Time: 18:31)



There are different primarily 2 types of NFC devices. One is the passive device, and the other one is the active device. Passive devices are more common than the active devices. Active devices are typically implemented in smartphones and so on.

So, you have an NFC support along with your smartphone in which are basically you know these NFCs that are implemented in the smartphones are basically active collectors of of information, and they are also active transceivers, you know rather transmitters of the information. So, we have active devices. An example as I as I just said is the use of NFC in you know active NFCs in smartphones. And all the passive devices are typically used in NFC tags and so on. And these are very similar to the RFID tags and very similar kind of technology which is based on magnetic induction. These RFC tags sorry these NFC tags, they contain information which is readable by other devices; however, it cannot read information it itself and these NFCs like in the case of RFIDs are typically used and are implemented in supermarkets.

(Refer Slide Time: 20:00).

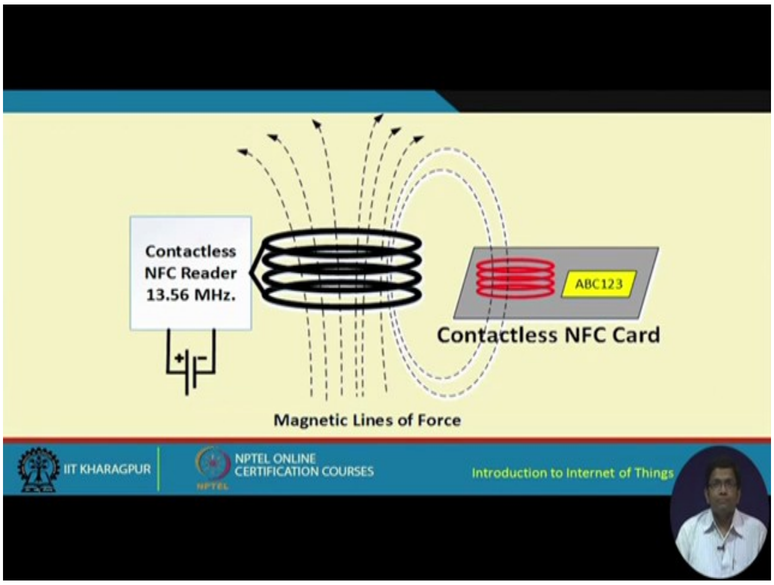


So, as I was just saying in a short while back, NFCs are based on the physical principle the scientific principle behind the functioning of NFCs is the concept of magnetic induction.

So, here basically there is a NFC reader, which emit is a small electric current which creates a magnetic field, which in turn bridges the physical space between the devices. So, you bring the NFC reader close to the NFC device there is a magnetic induction that basically goes on between these two entities and that is how the information that is encoded in these NFC tags are transmitted, are sent to the NFC reader. The reader basically emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices, this is what I will just saying short while back.

The generated field this magnetic field is received by a similar coil in the client device, where it is turned back into electrical impulses to communicate data such as identification number status information status information or any other information. NFC tags are used in the case of supermarkets and similar kind of libraries etcetera. They use the energy from the reader to encode their response while the active or peer to peer tags have their own power source.

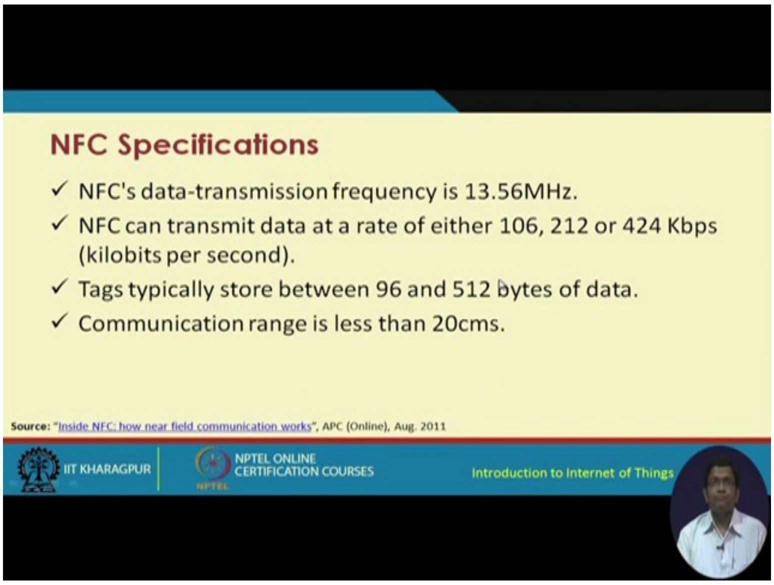
(Refer Slide Time: 21:50)



So, in this particular figure this particular physical or scientific principle that I just mentioned is shown over here. So, what we have pictorially as it is shown what we have is the NFC card

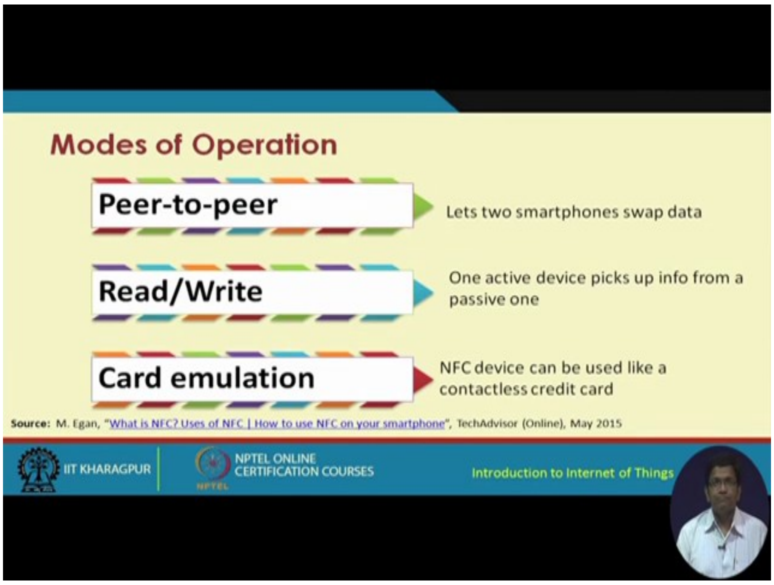
So, this has some magnetic coil kind of and then we have this NFC reader, through which current is passed. So, a magnetic field is generated and that is how the information transfer between these two entities the card as well as the card reader takes place.

(Refer Slide Time: 22:31)



The NFC specification, NFCs data transmission frequency is 13.56 sorry megahertz. NFC can transmit data at the rate of either 106, 212 or 424 Kbps. That is typically stored between 96 and 512 bytes of data, and the communication range is less than 20 centimeters.

(Refer Slide Time: 22:59)



There are primarily three modes of operation of NFC. The first is the peer to peer mode. The second is the read write mode, and the third is the card emulation mode. In the peer to peer mode two smartphones they can for example, swap data between themselves and this is this particular mode which helps these 2 smartphones to be able to exchange the data between themselves. The read write mode, here one active device picks up information from a passive one.

So, active device from passive device picking up information is an example of read write mode of operation. And card emulation, the NFC device can be used like a contactless credit card. So, in credit cards also and very similar to the way it is done. So, in credit cards also you know these kind of things are implemented the RFCs are implemented. So, that what you have is payment through these NFC enabled credit cards. So, there is a contactless credit card. So, these NFC basically makes it contactless the functioning of NFC basically makes it contactless.

(Refer Slide Time: 24:31)

So, we have three modes of operation the peer to peer mode, the read write mode and the card emulation mode. So, I already mentioned about payments using smartphones, parcel tracking, information tags in posters and advertisements, computer game synchronized toys, low power home automation systems these are all different examples of NFC applications. NFC reader the card and the NFC reader being used for all these different types of applications is something that makes NFC very useful and effective for IoT applications.

So, to conclude what we have gone through are primarily two protocols the HART and it is wireless variant the wireless HART, and NFC, which is the near field communication. In HART and wireless HART basically there are the layers physical layer, the data link layer, network layer, transport layer and application layer. HART the wired HART basically does not have it does not have the network layer. Wireless HART does and, wireless HART basically works on top of the IEEE 802.15.4 or rather to be more precise and correct, wireless HART works as a derived protocol from the 802.15.4.

It is derived from 802.15.4 because it has different features that I have been suggested in 802.15.4 and is implemented over here, in HART and wireless HART rather. Whereas, in NFC basically works very similar to RFIDs, and you have an NFC reader and a NFC card and there is magnetic coupling that you know magnetic induction that helps these two entities to transfer information between them, to read information let us say from the card to the reader, so these are all very attractive technologies that can be used for implementing internet of things.

Thank you.

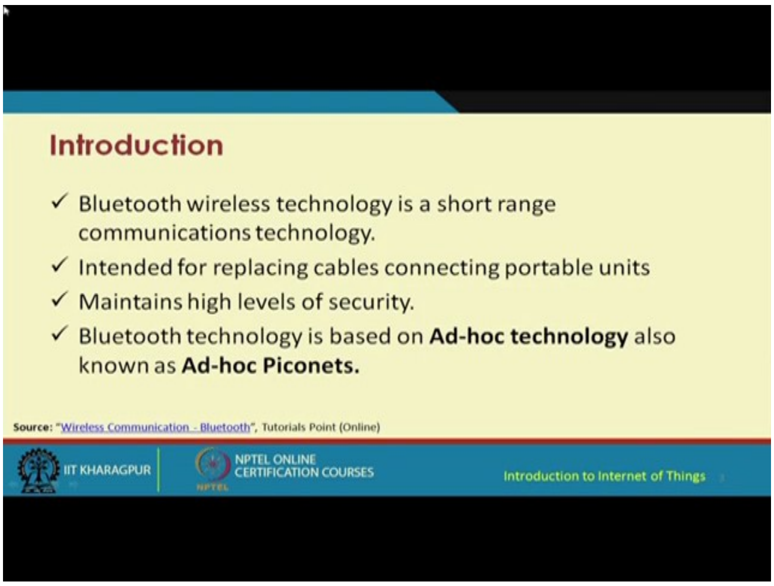
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 12
Connectivity Technologies – IV

Another very important protocol is Bluetooth this Bluetooth technology is heavily used for building IOT connectivity. We have already gone through zigbee we have also gone through different other allied technologies, such as 6LoWPAN such as HART wireless HART RFID and also NFC. And this particular technology, Bluetooth is typically used for bit of different kind of applications, where it is required to form a personal area network, maybe to replace the wireless wired connectivity between the different devices wired connectivity, if you want to replace the cables between different devices Bluetooth can be used.

So, you move the cables have wireless connectivity between them that can be done with the help of Bluetooth and this is this protocol that we are going to discuss in this particular lecture.

(Refer Slide Time: 01:49)



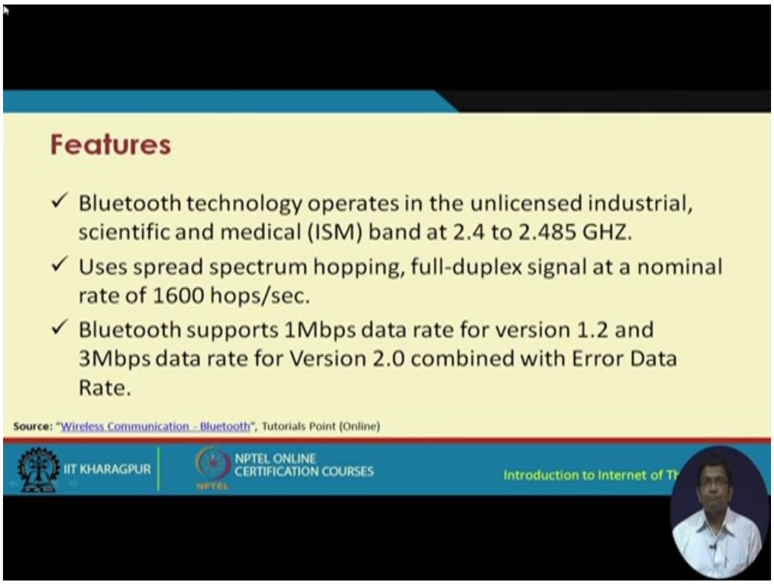
So, if we look at the Bluetooth technology, this is particularly used for short range communication. Personal area network for instance connecting different peripherals to a computer peripherals to a computer using Bluetooth is a very commonly used application of Bluetooth the second could be to transfer data using Bluetooth between 2 mobile devices these mobile devices of course, need to have the Bluetooth radio to be supported, but if it is supported and now it is most of the mobile phones particularly the smartphones they are all enabled with Bluetooth.

So, you know one can transfer files music videos. So, on and so forth and this is something very common, that we do commonly we transfer files we transfer different things between 2 Bluetooth devices a very simple form of Bluetooth configuration where we have 2 Bluetooth devices a client and a server, and the data is transferred between these 2 devices, a very simple kind of configuration now in this particular course in this particular lecture we are going to go through all these different applications.

So, it is used Bluetooth is used for short range communication. And it is typically used for instances where it is required to replace the cable the existing cables have to be replaced. So, what is required is to have cable replacement protocols. And that is why as we will see shortly that we have an entirely different and entirely different protocol stack, which is basically proposed for using Bluetooth. Of course, it does match with the OSI layers TCP/IP and OSI layers to a great extent, but then we have a completely different set of layers with different names in the Bluetooth architecture, and also we have separate protocols that are that function in each of these different layers.

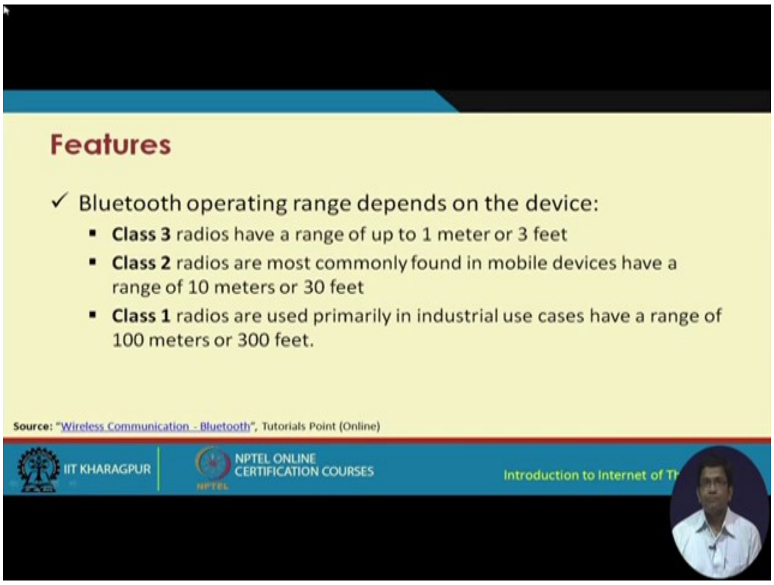
So, we will go through it in a short while. So, Bluetooth one of the very good things about Bluetooth is security. Bluetooth basically ensures high level of security, and another very distinctive feature is that Bluetooth helps in forming Ad-hoc networks. So, concepts such as Ad-hoc technology Ad-hoc Piconets are basically commonly used in the case of Bluetooth.

(Refer Slide Time: 04:22).



Bluetooth technology also like the previous ones like HART etcetera that we covered in the previous lectures operate in the ism band 2.4 gigahertz to 2.484 gigahertz, it uses spread spectrum hopping full duplex signal at a nominal rate of 1600 hops per second.

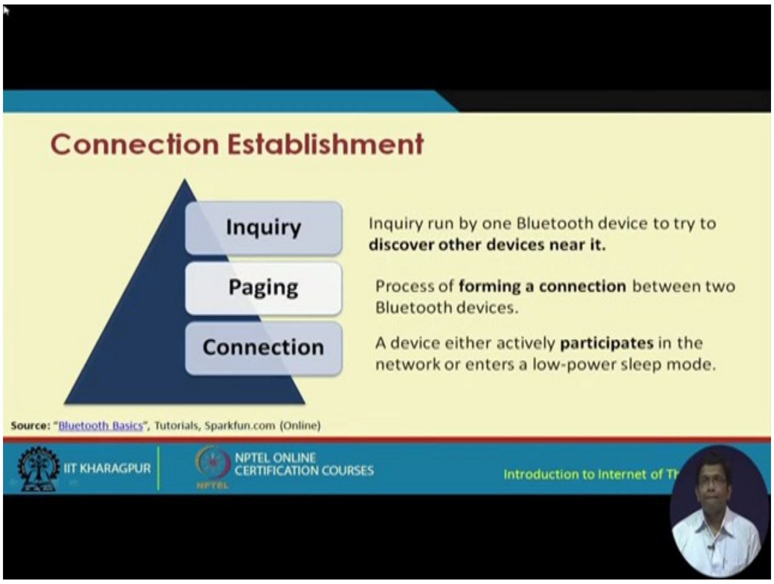
(Refer Slide Time: 04:58)



It supports one mbps data rate which is quite attractive short range high data rate communication is supported. In Bluetooth there are 3 types of radios that we will typically find and they all operate in different ways. We have the class one radios class 2 radios and class 3 radios. Class 3 radios have a range of up to 1 meter or 3 meters. Class

2 radios are most commonly found in mobile devices having a range of 10 meters or 30 feet and class one radios are used primarily in industrial use cases having a range of 100 meters or 300 feet.

(Refer Slide Time: 05:32)



In terms of connection establishment using Bluetooth there are 3 different phases. The first one is the discovery or the inquiry phase. This next one is the paging phase, and the third one is the connection phase. So, basically for connection establishment there are only 3 phases in the inquiry phase, there is some kind of inquiry that runs from one Bluetooth device and that particular Bluetooth device basically what it does is it tries to discover other devices in it is vicinity.

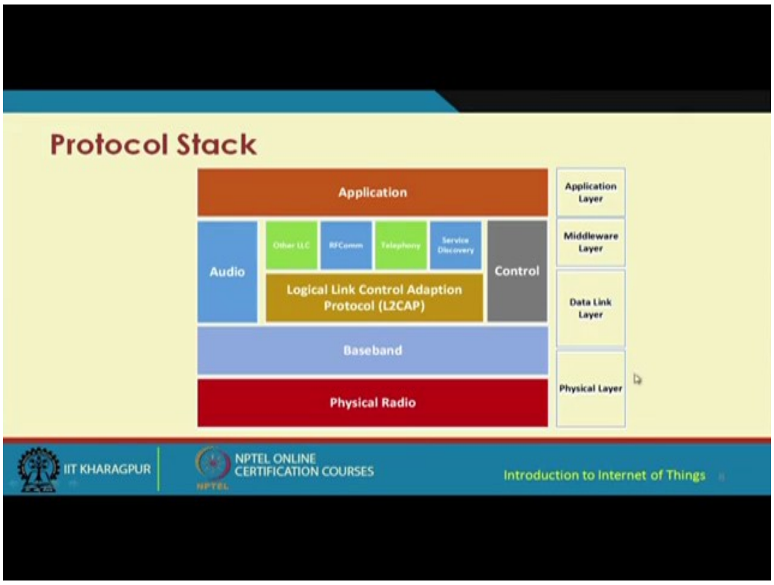
So, this is, one Bluetooth device it is trying to explore what are the other devices in it is vicinity. So, this is basically this discovery phase or the inquiry phase very simple the next one, is the paging phase where some kind of connection is formed between 2 Bluetooth devices that want to talk to each other. So, some kind of connection is formed, and the third one is the connection phase where a device either actively participates in the network or enters a low power sleep mode.

(Refer Slide Time: 06:44)

There are different modes of operation of Bluetooth devices, one is the active mode and this is the mode where the device basically is fully active fully functional in all different respects it actively transmit is data it actively receives data and so on and so forth. So, it is fully functional fully active the other 3 phases the sniff mode the hold mode and the park mode all these 3 different modes are basically power saving modes, and they differed in very minute ways in very fine in different ways. In a sniff mode the device basically sleeps and only listens for transmission at a particular predetermined predefined interval.

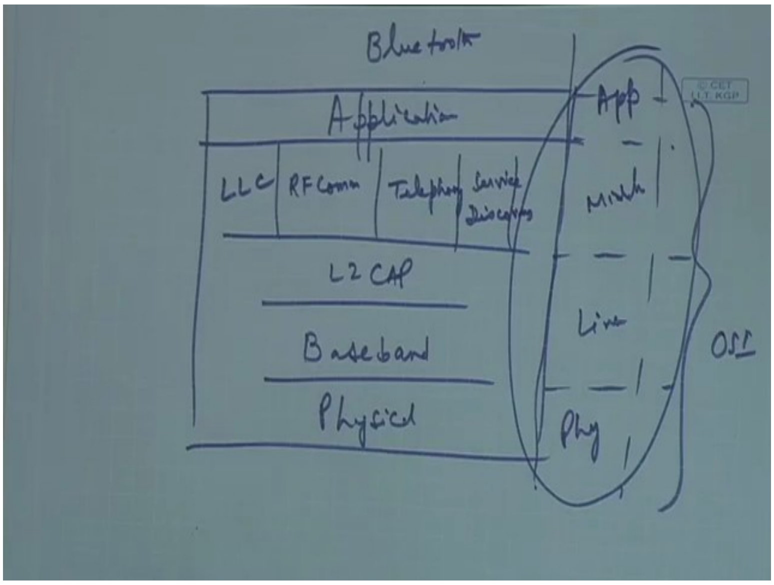
In the hold mode, this is also a power saving mode where a device sleeps for a defined period and then returns back to the active mode. And in the park mode the slave will become inactive until the master tells it to wake back up. So, we have all these different 4 modes of operation of Bluetooth devices, the active mode fully functional, fully active, fully transmitting, fully receiving. And the other 3 modes the sniff mode hold mode and park mode are all essentially power saving modes of different types.

(Refer Slide Time: 08:22)



So, this is the protocol stack that I was talking to you about earlier. So, what we have the physical layer, then we have the baseband layer.

(Refer Slide Time: 08:35).

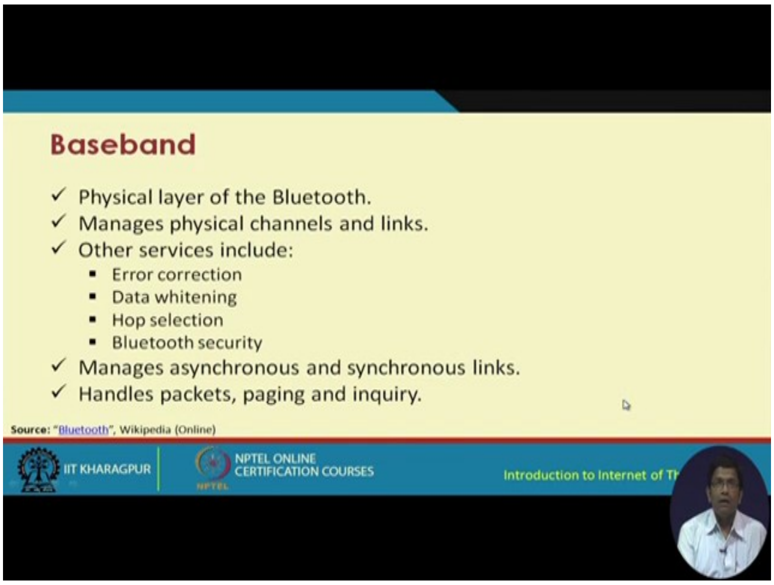


We have the L2CAP and then there are some different other layers and corresponding protocols that are supported in the top layers and then we have the application layer. So, these are the different layers in the Bluetooth protocols. I was telling you about cable replacement there are protocols such as RFComm, protocols which will support traditional telephony, protocols that will support service discovery, protocols that will support other link layer functionalities such as LLC.

So, these are the different functionalities that can be supported on top of this that the physical baseband L2CAP layers in Bluetooth. Now this basically can be mapped to the traditional OSI layers and so these are the OSI layers. So, here again you have the physical layer you have the link layer, you have the different middleware, you have the application layer. And the exact form of mapping is basically shown in this particular figure in the slide. So, this is how it maps ok.

So, we have physical radio layer or physical layer baseband layer L2CAP, and this you know LLC RFComm telephony service discovery and the application layer and this is how they map to the OSI traditional OSI layers.

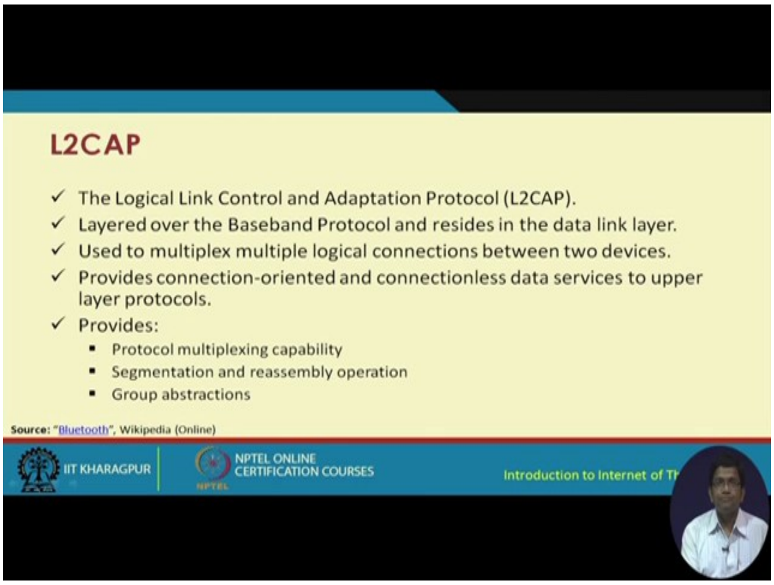
(Refer Slide Time: 10:51)



So, baseband layer or the physical the one that is above the physical here basically. So, physical is basically nothing, but the radio and you know we do not need to really understand baseband is the physical layer of Bluetooth it manages physical channels and links and different services such as error correction data whitening hop selection Bluetooth security we are not going through a details of it, it is not even required for you to know because you know if it is required, then really you know this is just you know we are just getting exposure to different protocols in this particular course.

So, it is not required to really dig into too much deep of each of these protocols we just have to be exposed and things like you know adding Gaussian noise. Or you know error correction etcetera. These are difficult these are basically you know the different functionalities data whitening you know with the help of white noise, you know Gaussian noise etcetera you know. So, these are the things that are basically supported in the baseband layer.

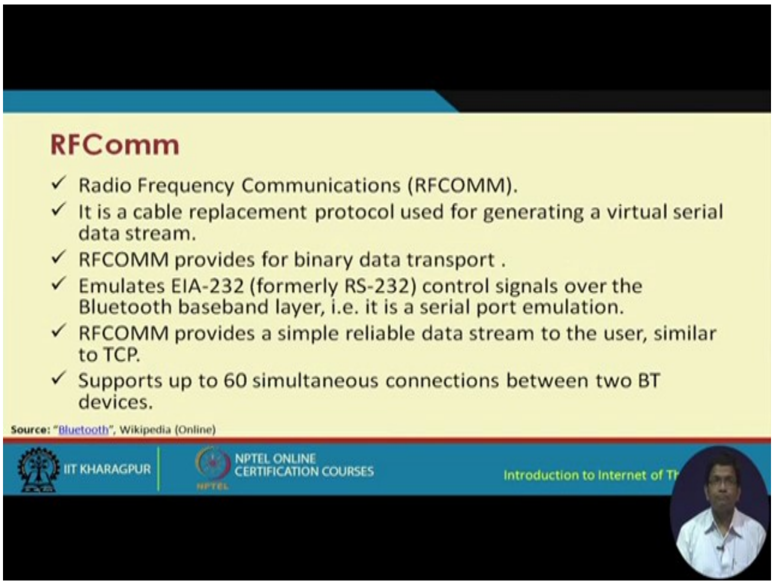
(Refer Slide Time: 12:03).



Then we have the L2CAP. And in the L2CAP which basically is on top of the baseband layer, functionalities such as multiplexing, multiple logical connections between 2 Bluetooth devices is functioned is made possible, in this using this particular layer.

So, this particular functionality is implemented in the L2, cap layer L2CAP provides connection oriented and connection less data services to upper layer protocols provides protocol multiplexing capability segmentation. So, because basically you know when you are sending a video for instance. So, it cannot be send to all at once right. So, it has to be segmented fragmented and segment wise it has to be transmitted and then area assembly also has to be done in a subsequently. So, segmentation and reassembly and group abstractions you know. So, together forming of the groups abstracting them and so similar kind of functionalities are all done at this higher up layer, which is the L2CAP layer.

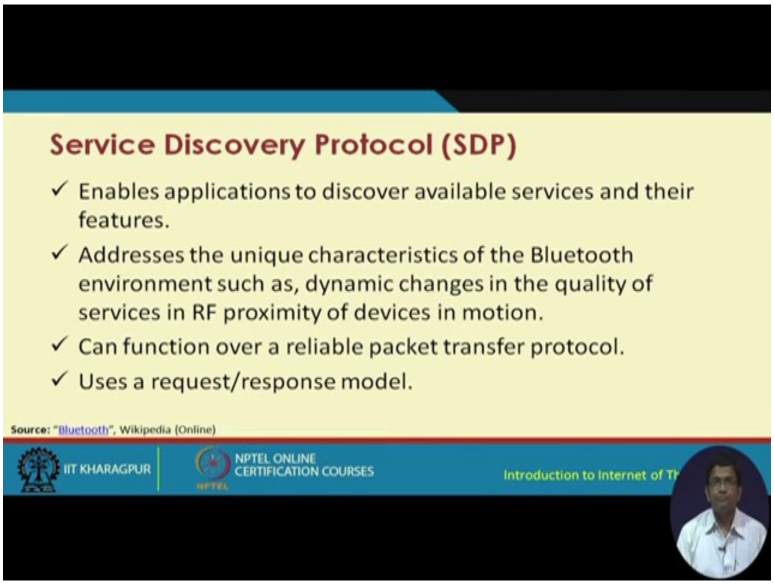
(Refer Slide Time: 13:08).



Then we have on top different protocols such as RFComm the full form is radio frequency communication protocol, which is basically a cable replacement protocol and the main purpose of RFComm or more specifically in you know. So, Bluetooth and more specifically RFComm is basically to replace the serial cables that are already. There that is to be traditionally used. So, use do away with the cables and introduce these protocols and that will basically make Bluetooth a cable replacement technology.

So, this RFComm it works as an emulation of the RS-232. And if you remember RS-232 are presently it is also known as EIA 232. RS-232 is basically you know it is a serial port communication protocol serial port communication protocol the traditional serial port communication protocol is RS-232. So, this RS-232 it is emulated, it is behaviors are emulated in this particular protocol the RFComm protocol, RFComm protocol it provides a simple reliable data stream to the user very similar to TCP and supports up to sixty simultaneous connections between 2 Bluetooth devices.

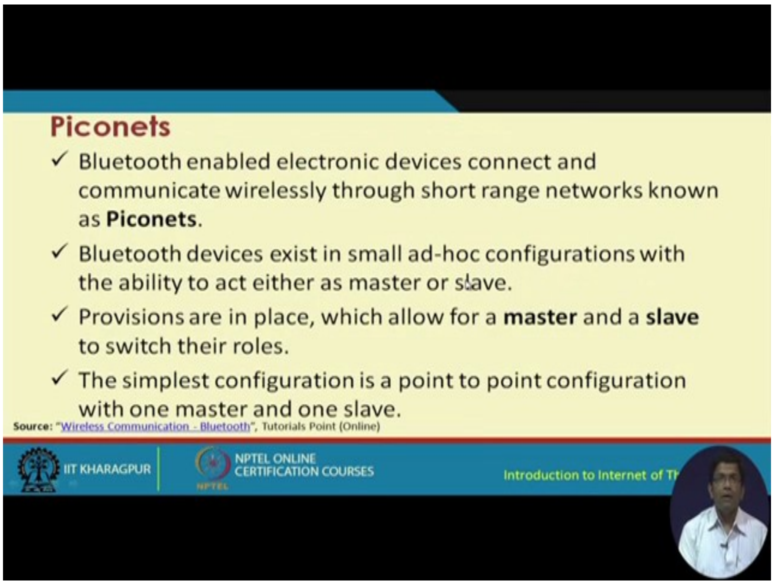
(Refer Slide Time: 14:34)



Then finally, we have the service discovery protocol and there are some telephony protocols etcetera, because which has to support the traditional telephony functions. So, we are not going through them service discovery protocol is very important because ultimately, we are going to use Bluetooth for offering different types of services to different applications. Some sort of service discovery has to happen. So, SDP enables the applications to discover available services and their features, and SDP addresses the unique characteristics of Bluetooth environment such as dynamic changes in the quality of services in RF proximity of devices in motion and can function over a reliable packet transfer protocol.

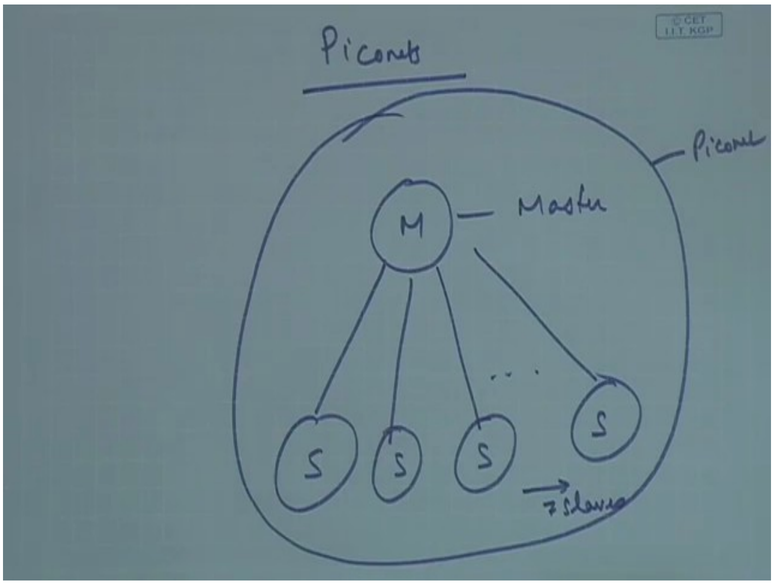
So, SDP it uses a service request response kind of model a request is sent a response is received back ok.

(Refer Slide Time: 15:31)



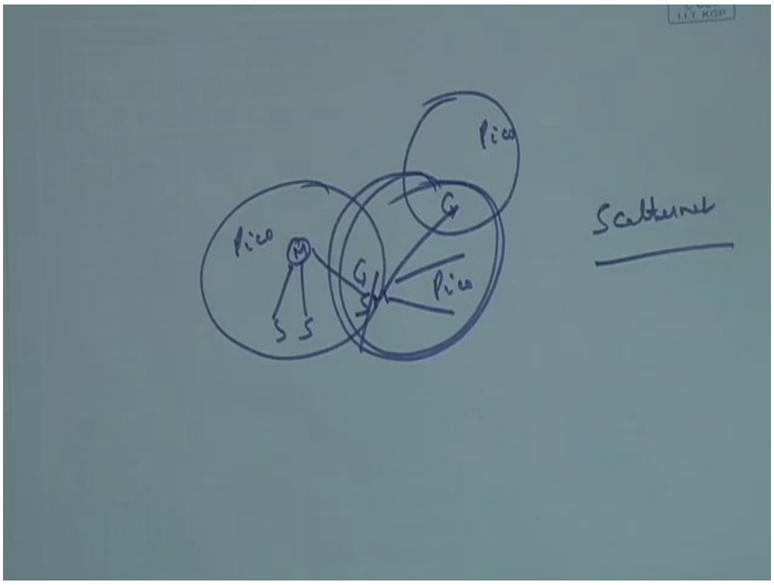
Now, a very important concept, I am going to explain to you which is very much important in order to understand Bluetooth. And this is known as the concept of piconets. Piconet is some sort of a unit you know unit form of network in Bluetooth, unit form of network what does it mean. So, we have let us say let us look at this particular example. So, we are going to go through we have to understand how piconets work.

(Refer Slide Time: 16:08)



So, what we have is something known as the master. So, we have m Bluetooth node a Bluetooth device which will act as a master. And there can be different slave devices. So, we have a master we have different slaves. So, this entire thing is a piconet. This is a piconet. And how many of in a particular unit; that means, in a particular piconet, in one piconet there can be only one master. Only one master and one or more slaves. How many up to how many 7 slaves, so 1 2 3 up to 7 slaves. So, there can be one master and one up to 7 slaves in a piconet.

(Refer Slide Time: 17:39).

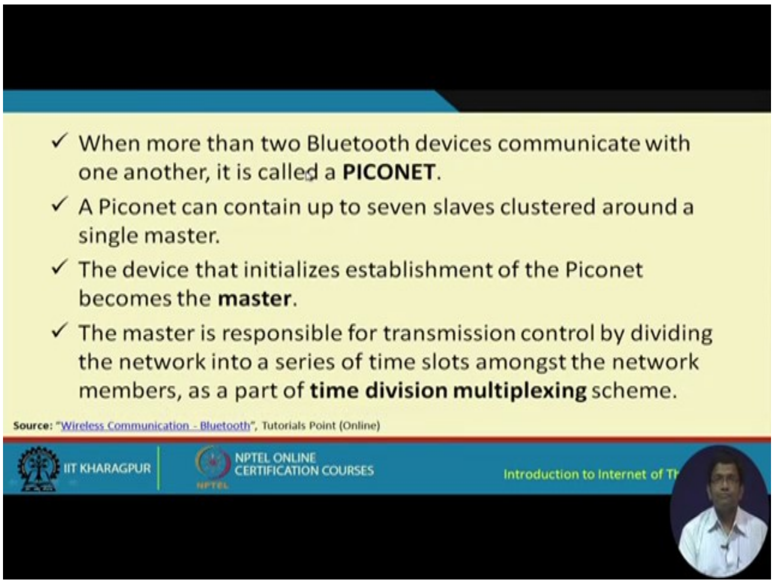


Now, so, this piconet, we have one piconet. We have another piconet, we have another piconet. So, this is one piconet this is another piconet this is a third piconet. So, what we have are 3 different piconets and together all these piconets put together is known as scatternet. So, this is the concept of scatternet in a scatternet you have several piconets put together working together. And these piconets basically talk to each other via the gateway and this gateway nodes can be anything like you know. So, it might. So, happen that you have a master over here (Refer Time: 18:25) say that this is a master and then you have different slaves slave here, there can be another slave and this slave of this piconet can act as a master in this particular piconet.

So, you know the slave in one piconet can be a master in another piconet and then again it can have one or more slaves, and this is the way you know this chain continues and together we have the concept of piconets and scatter nets, so going back. So, we have Bluetooth enabled devices that connect and communicate wirelessly for short range communication, unit form of it unit network of it is the piconet. The Bluetooth devices exist in small Ad-hoc configurations with the ability to act as either the master or the slave it provisions to have one master and one or up to 7 slaves in a particular piconet.

The simplest configuration is a point to point configuration, with one master and one slave and where we get it this is something, that we typically use a single master single slave kind of configuration is something that we use typically to exchange files to exchange videos to exchange images graphics and so on, between our mobile devices. So, when we are using our smartphones we turn on the smartphones to turn on the Bluetooth in our smartphones to of you know 2 devices. And then from one such device a image can be sent a file can be sent to another such device after the discovery or the initiation phase it can be sent, using this particular configuration.

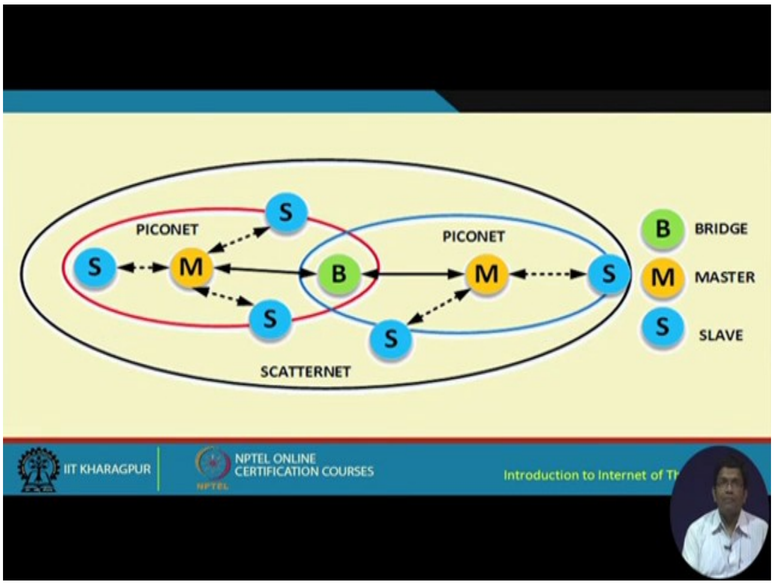
(Refer Slide Time: 20:27)



So, we have one master one slave kind of configuration. So, when more than 2 Bluetooth devices communicate with one another. It is called a piconet a piconet can contain up to 7 slaves clustered around a single master. The device that initializes establishment of the piconet becomes the master, and the master is responsible for transmission control by dividing the network into a series of time slots using TDMA. So, basically what happens is within a piconet we have a master and we have you know up to 7 slaves.

So, what the master does is it will have to divide the time that is allotted into different slots. And we will have to distribute those slots among the slave nodes in that piconet and the master will have to ensure that periodically, this thing is done and is distributed to the different slaves in it is piconet. So, this is the job of the master in a piconet.

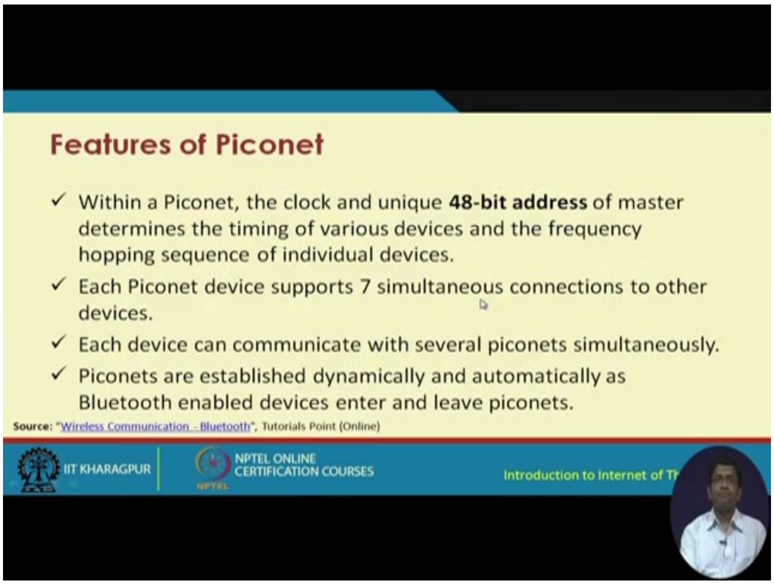
(Refer Slide Time: 21:26)



So, this is the diagram showing the configuration of piconet and scatter net. So, we have within a piconets, we here what we see we have a scatter net consisting of 2 piconets this is one piconet, this is another piconet. And we see that there is a master and there are 3 slaves rather 4 slaves and this slave is acting as a bridge between these 2 piconets, and these are again 3 different slaves for this particular piconet.

And here as you can see over here we have distinct masters in each of these piconets, it is not like the same master. In fact, what we could have had is this bridge which is a slave for this piconet would have also been configured in such a way, that it would act as a master for this piconet this is also possible.

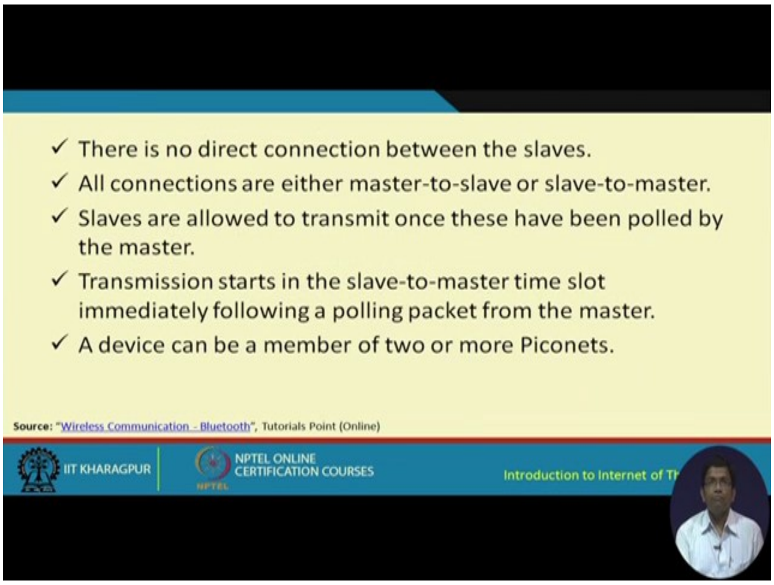
(Refer Slide Time: 22:26)



So, the master of the slave they use the 42 bit addressing. So, this is the addressing scheme that is used each piconet device will support 7 simultaneous connections to other devices each device can communicate with several piconets simultaneously. And piconets can establish dynamically and automatically as Bluetooth enabled devices enter and leave piconets.

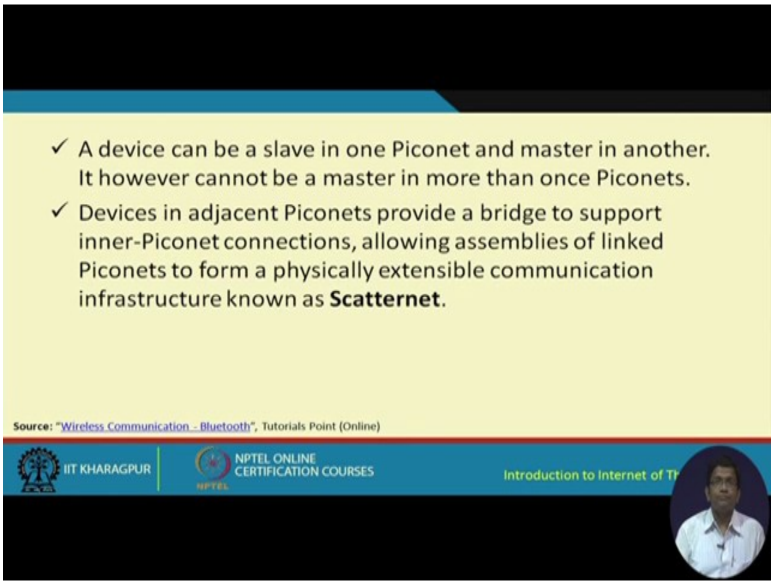
So, they can basically configure self configure, they can change you know devices can not the Bluetooth devices can get into a piconet can go out of the piconet dynamically. And the topology changes accordingly. So, all these things are featured in a piconet.

(Refer Slide Time: 23:07)



There is no direct connection between the slaves all connections are either through the master to slave or slave to master mode slaves are allowed to transmit. Once these have been polled by the master transmission starts in the slave to master timeslot immediately following a polling packet from the master and the device can be member of 2 or more piconets, and this is something that I explained earlier as well.

(Refer Slide Time: 23:42)



In one piconet that that particular device can be a slave in another piconet, it can even act as a master and together you put all these piconets and what you get is a physically extended infrastructure comprising of several piconets known as the scatternet.

(Refer Slide Time: 23:58)

Applications of Bluetooth are quite common. Audio players, home automation systems, smartphones, toys, hands free headphones, sensor networks they all are users of Bluetooth. So, the Bluetooth is a very important technology, that we have just covered and it is quite heavily used for building IOT systems. Zigbee, hart Bluetooth, NFC RFID these are all like different technologies that can be used for establishing connectivity between different nodes for building up IOT.

They all have their different distinct features and we have already seen that in the previous lecture we have seen that how hart wireless hart and zigbee differ from each other. And now it is also quite evident how Bluetooth differs from zigbee. So, for Bluetooth, we can have high data rate communication compared to no data rate in the case of zigbee, but zigbee is consumes much lower power compared to Bluetooth. So, there are pros and cons depending on the application. In fact, what can also happen is we could be using all of these technologies together in parallel, and we can have a Bluetooth working with zigbee, zigbee working with hart etcetera and so all these things are possible.

Zigbee primarily consumer IOT hart wireless hart primarily industrial IOT, but it does not even matter you can even put all of them together for maybe industrial IOT or on the other hand consumer IOT. So, this can also be done. So, these are that all these powerful technologies that can be used for building IOT systems.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

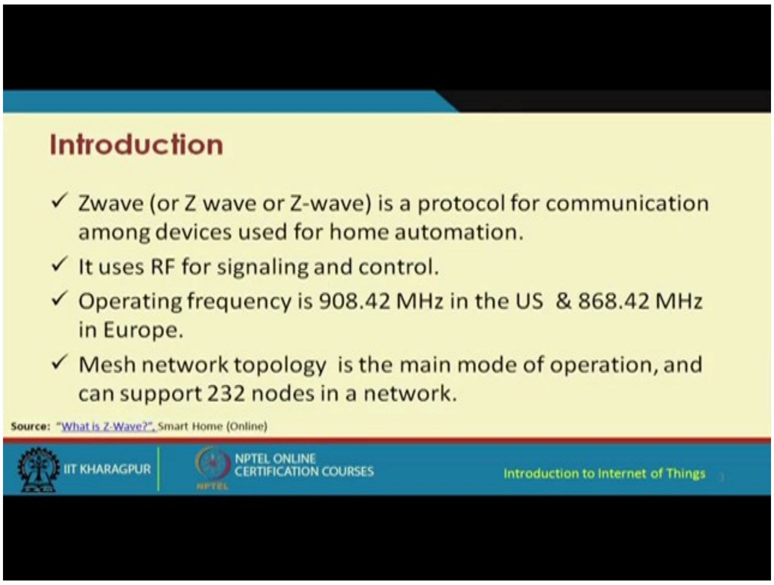
Lecture – 13
Connectivity Technologies – V

We will now in this particular lecture cover two important protocols Zwave and ISA100.11a. These are two very important protocols that, in addition to zigbee HART wireless HART Bluetooth RFID NFC are also used for building IoT systems; however, whereas, zigbee is more popular for all sorts of all sorts of IoT systems use in IoT systems. Zwave is particularly attractive for building home automation systems. And as you know by now in this course that home automation is one of the important application areas of IoT. Home automation, home automation includes what? Home automation includes things such as having some kind of a robot, or having mobile phones that will do number of different things, different day today functions at homes can be done spontaneously and so on and so forth.

So, how can it be done? This is what home automation does. So, automating different functions in at home, is something that is of primary concern of home automation. So, I was talking about Zwave. Zwave is a technology which comes from the Zwave alliance. So, this Zwave alliance in the same way as we have a zigbee alliance we also have a Zwave alliance. And this Zwave alliance is particularly pushing for making this technology very attractive to support different home automation appliance applications. Different home automation functions.

And we are going to look at how using Zwave we could be able to improve the automation of different functions using different IoT devices at home.

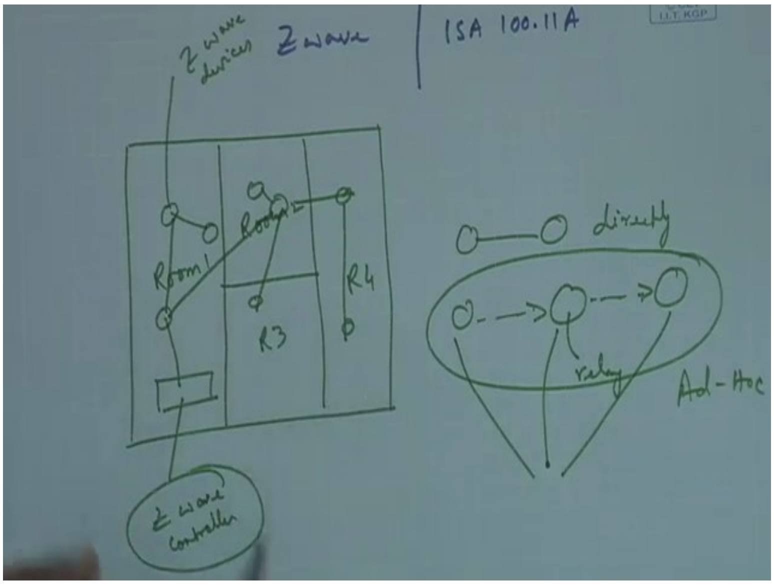
(Refer Slide Time: 02:42)



So, we look at this Zwave. Zwave is also written in different ways, we could be writing Zwave altogether or using a space in between Z and wave, or using a hyphen in between Z and wave. And this is a protocol that is used for communication between different IoT devices for home automation as I just said before it uses RFs for signaling and control. And the operating frequency for it is different from the ones that we have seen. We have seen that primarily the other things like HART or you know NFC etcetera, they all operate in the 2.4 GHz band.

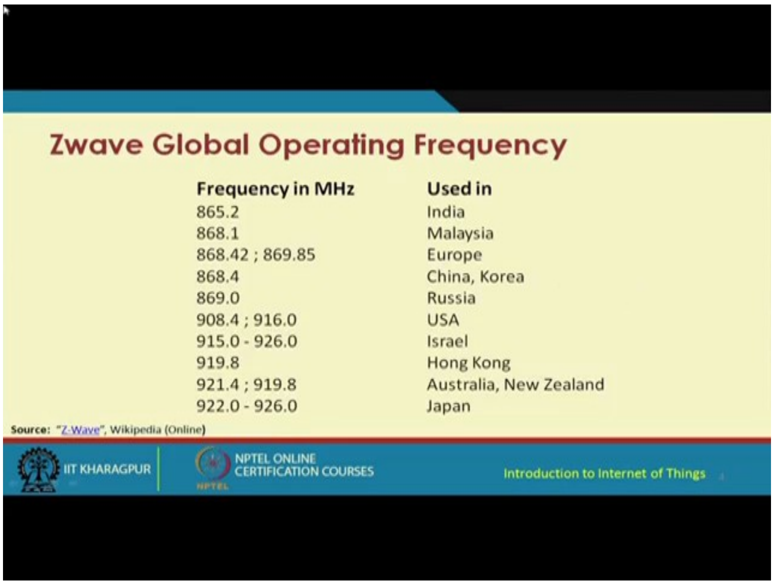
And for Zwave the operating frequency is 908.42 megahertz in US 868.42 megahertz in Europe, and for different other countries I will show you in a short while. That for different other countries there are different other frequencies of operation. So, in Zwave there is some kind of a mesh network topology that is formed and maintained between different nodes which can be up to about 232 in number in a single network. Now let us look at some interesting points in Zwave.

(Refer Slide Time: 04:19).



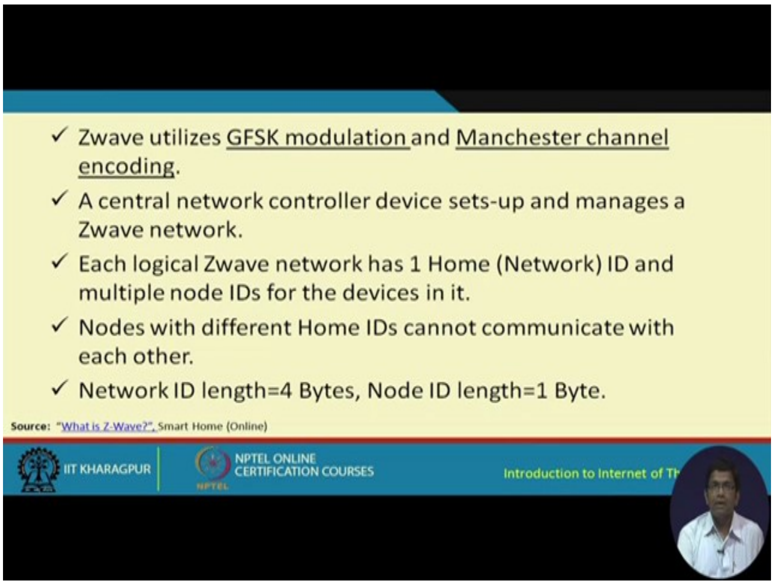
So, we have let us say, we have we are talking about home automation. In a particular home there could be different rooms. Let us say this is room 1 room 2 room 3 and room 4. In Zwave if we are using Zwave, there is something called the Zwave controller. And there are different Zwave devices that are there. So, typically in a single home there is only one Zwave controller and there could be different. So, these are all Zwave devices one Zwave controller and one or more; that means, several Zwave devices. These Zwave devices they could be either connecting directly or they could be connecting with the help of a relay node in between. So, this is one Zwave device, this is another Zwave device and this could be a third Zwave device. And this could be something like an ad hoc mode of communication. So, this is how Zwave basically functions.

(Refer Slide Time: 06:10)



So, I was telling you that in US 908.4 and 916 frequency bands. In Europe 868.42 and 869.85 megahertz frequency band. And for other countries these different frequencies of operation are shown over here in this particular table. So, as we can see that for India it is 865.2 megahertz operating frequency.

(Refer Slide Time: 06:48)

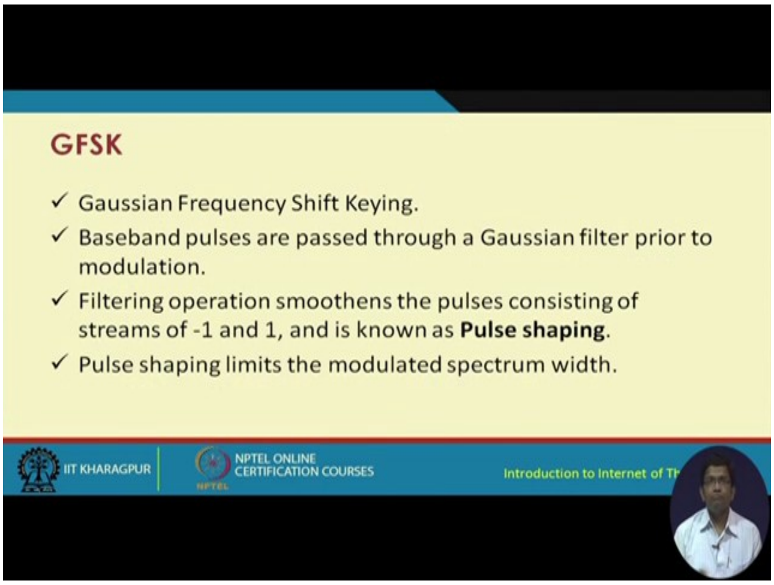


A very interesting and important concept is Zwave does not use FSK modulation directly. What it does is it passes through a Gaussian filter. So, essentially what happens is it becomes Gaussian FSK modulation. And the channel encoding scheme that is used is Manchester encoding, this is one concept. The second thing is as I was mentioning earlier, there is an entity a single entity called the network controller the central network controller, that sets up and manages a Zwave network. Each logical Zwave network has one home ID and multiple node IDs for the devices in it. And that home ID basically corresponds to a single network ID.

So, essentially because there is only home ID which is unique to a particular home. The other networks in other homes will not be able to communicate through between these different homes. I hope that my point is clear. So, what I am saying is that every home has it is unique home ID or network ID. And in that particular home only that other Zwave devices will be able to communicate. So, they will not be able to communicate with other homes, the Zwave devices in a particular home will not be able to communicate with other homes.

So, we are restricting this communication of Zwave devices to specific homes. So, nodes with different home ids cannot communicate with each other. And we also have to keep in mind that, the node ID length in Zwave there is 1 byte, and the network ID length is 4 bytes.

(Refer Slide Time: 08:50)

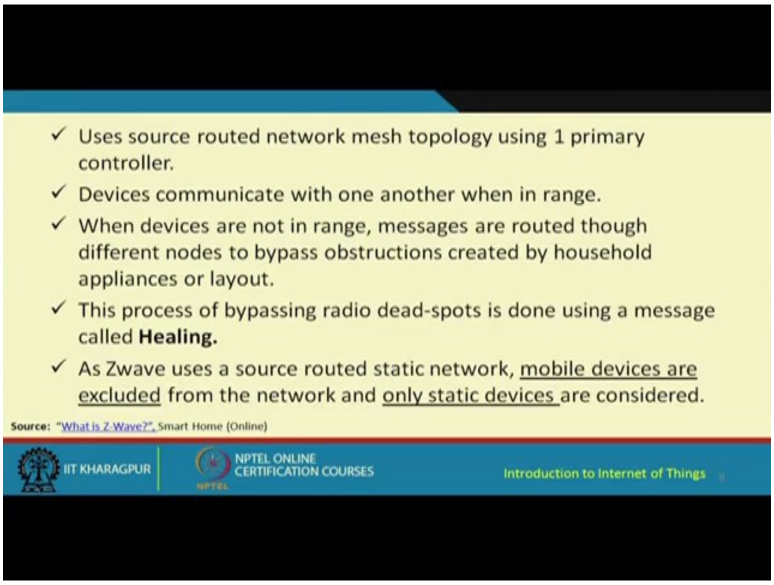


So, I was talking to you I was mentioning about these GFSK modulation, which is Gaussian frequency shift keying. So, what happens is there is a Gaussian filter prior to FSK you pass it pass the signal through a Gaussian filter to smoothen to smoothen the pulses. So, that you have will formed pulses which will occupy limited spectrum width and this process is known as pulse shaping.

(Refer Slide Time: 09:23)

So, in here in this figure as we can see this is a typical figure of a home. In this home we have different rooms. We have bedrooms, we have a living room, we have a kitchen, we have bedrooms and so on. And as we can see that if we have to implement Zwave, we need a Zwave controller and these different red colored and green colored nodes which are the Zwave n devices, the Zwave nodes. So, the controller basically sets of connectivity between each of these different nodes, as we can see in this particular example. The controller has one hop communication with these green colored nodes; however, the controller to these red color nodes are multi hop, they are not within the one hop communication range.

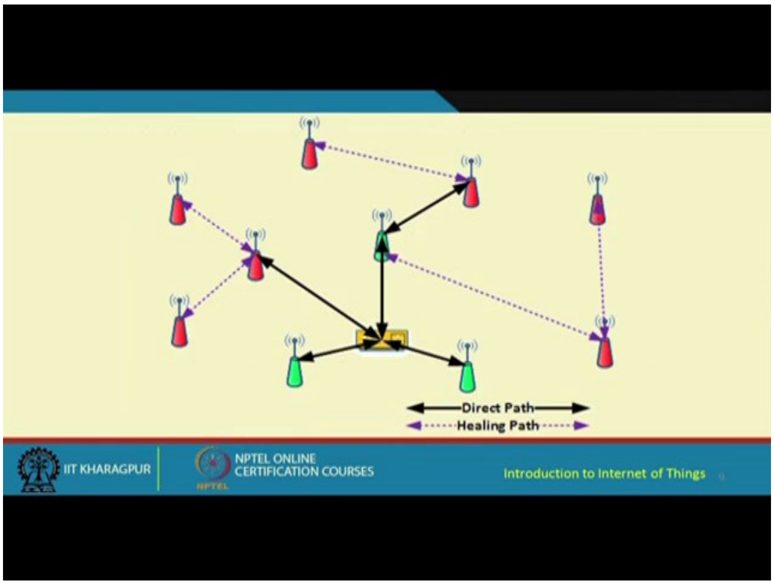
(Refer Slide Time: 10:38)



So, if this controller has to communicate with this red colored node in this particular room then it has to do via this green color node. Zwave uses mesh topology and it also uses source routing. So, source routing means that even before the packet is sent, the entire route is basically encoded or embedded before the packet is sent forward. So, before the packet is sent the entire route information is embedded to it. So, the entires route is known to the source and is given to the packet. So, the packet will know how it will traverse through the entire network or until it reaches the intended destination. So, the devices they communicate with one another when they are in range when the devices are not in range, as I was showing you using those red colored Zwave nodes in the previous figure.

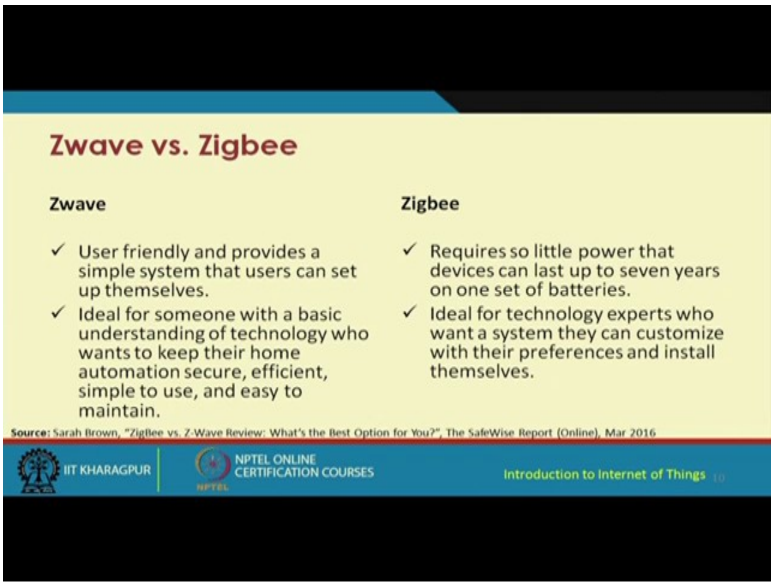
The messages in such a case are routed through different nodes to bypass the obstructions that are created by household appliances or layout. And this is very important because, you know so, there are so many physical obstructions in the in the home. Right, there are walls between different rooms etcetera. So, what happens is there will be these different nodes, which will be acting as sort of gateways or relay nodes to facilitate communication between these remote Zwave nodes that are not within the direct transmission range with the controller.

(Refer Slide Time: 12:08)



and now we have remove the sketch of the rooms and this is what is shown over here. We have the green color nodes and this one which are within the direct communication range the direct path. And then there are these nodes which are within not within the direct communication range, and there they can communicate with the help of the healing path. So, this is known as the healing path, and this is known as the direct path. Zwave and zigbee how do they compare?

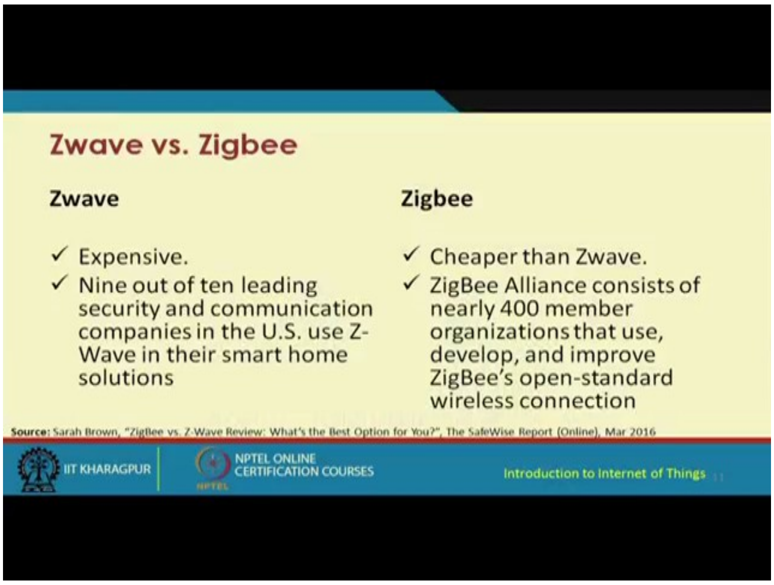
(Refer Slide Time: 12:43)



So, Zwave is user friendly. It provides simple system that users can set themselves. On the other hand zigbee requires. So, little power the devices can last up to 7 years on a single set of batteries. Zwave is ideal for someone with a basic understanding of technology who wants to keep their home automation secure efficient simple, And easy to maintain.

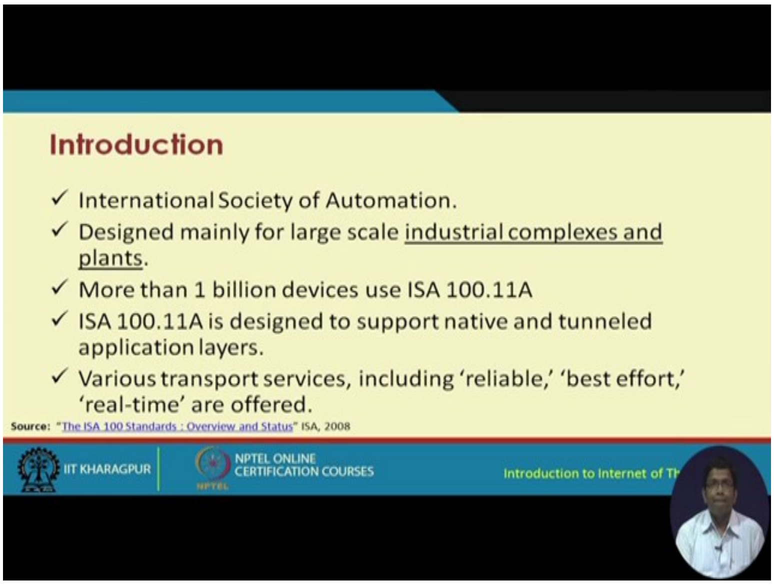
On the other hand using zigbee. Zigbee is ideal for technology experts who want a system that can customize with their preferences and install themselves. So, lot of sophistication can be done with the help of zigbee. On the other hand Zwave is more user friendly more customer friendly.

(Refer Slide Time: 13:55)



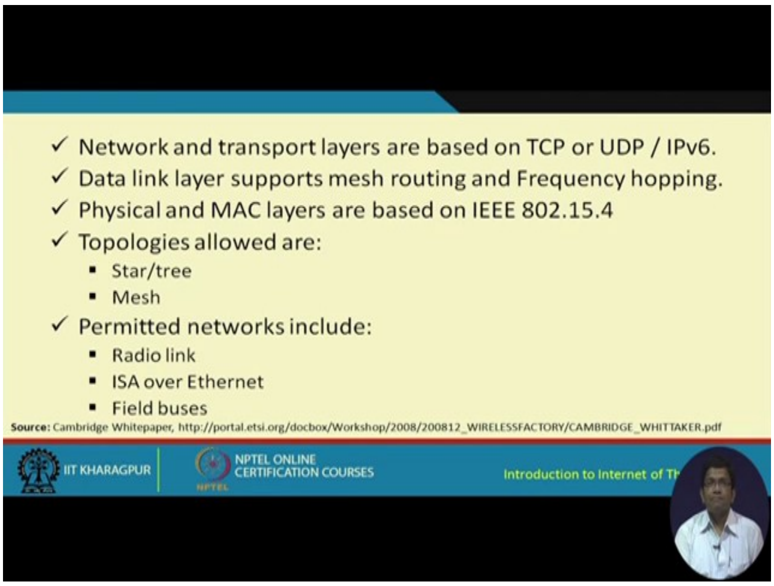
But a limited set of things can be done with the help of Zwave compare to zigbee. Zwave is expensive in compare to zigbee. And 9 out of 10 leading security and communication companies in us use Zwave for smart home solutions. On the other hand for zigbee there is zigbee alliance that consists of more than hundred member organizations that use develop and improve the open standard that is offered by zigbee.

(Refer Slide Time: 14:30)



Now, we come to the second very important protocol which is the ISA100.11A. So, it is protocol that has been designed by the international society of automation. And this is particularly used for plants in the industries, industrial complexes, industrial plants and so on and so forth. There are more than one billion devices that use ISA100.11a at present it is designed to support native and tunneled application layers various transport services including reliable based effort real time services are offered with the help of ISA100.11A. So, ISA100.11a is primarily attractive as a consequence in industrial sectors particularly for implementing industrial IoT systems.

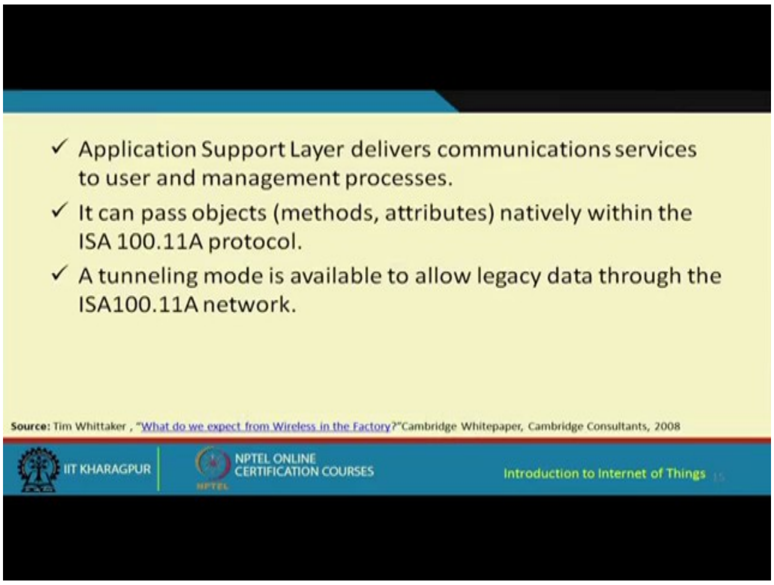
(Refer Slide Time: 15:26)



The network and transport layers are based on TCP or UDP or IPv6 and the data link layer supports mesh networking with frequency hopping.

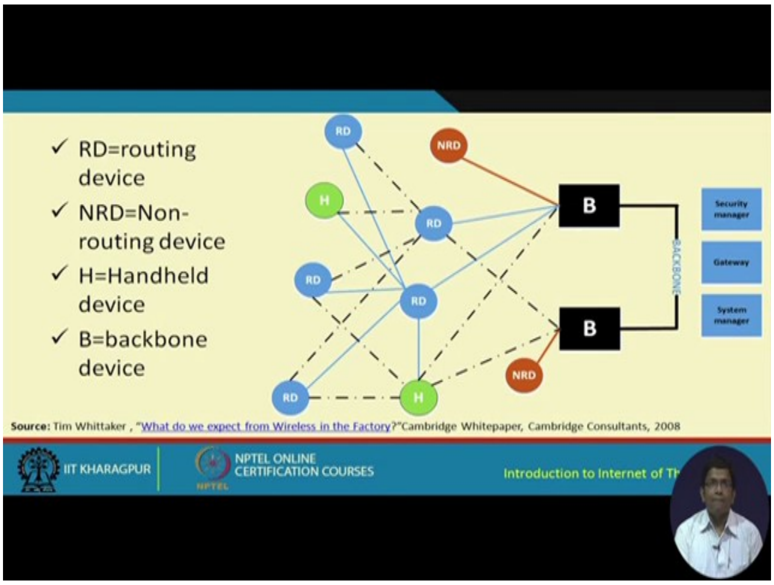
So, frequency hopping spread spectrum is typically used in ISA100.11a. The different topologies that are used for implementing this particular standard is, the star or the tree topology or the mesh topology as well. So, all these topologies can be used for implementing it and the radio that is used beneath underneath is based on 802.15.4 again. The permitted networks in include radio link ISA over ethernet and fill buses. Fill bus means that it is a bunch of wires and bunch of wires you know running between different devices as we see in the data centers or server rooms and so on.

(Refer Slide Time: 16:35)



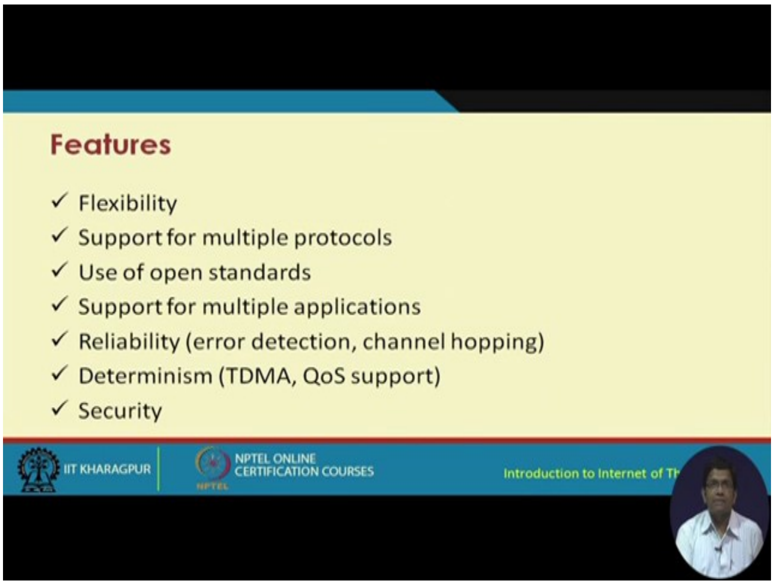
We have these buses and filled buses means between different filled buses we have this high bandwidth high capacity links that run between them. The application layer supports delivery of communication services to the users and the management processes. The this particular thing can pass objects methods or attributes natively within the ISA100.11a protocol. A tunneling mode is available to allow legacy data through this particular network.

(Refer Slide Time: 16:59)



So, what we have is a scenario like this. We have these backbone devices the black colored rectangles here. We have the back backbone devices. We have this non routing devices the red colored ones. The blue colored once are the routing devices and these green colored once are the handle devices, and then we have the security manager the gateway and the system manager which, basically function from beyond the backbone. So, this is the typical architecture of this particular use of ISA100.11a protocol in industries or smart factories.

(Refer Slide Time: 17:46)

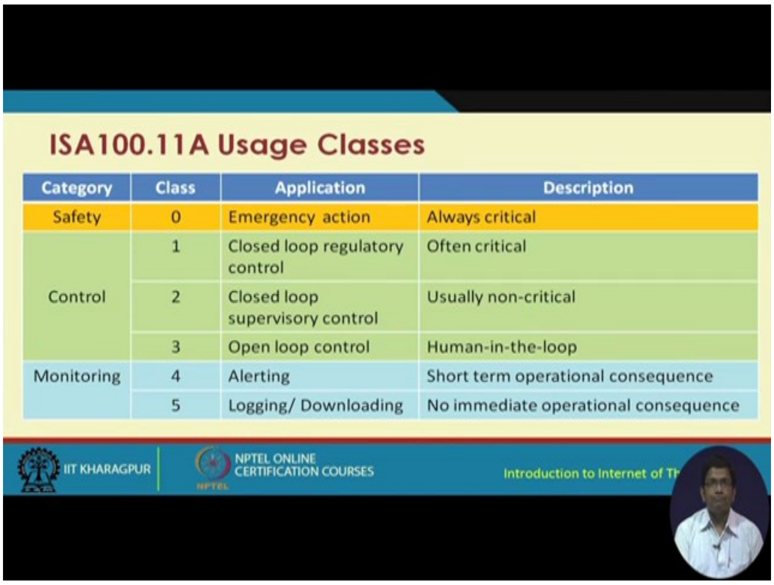


The features of this particular protocol include flexibility, support for multiple protocols, use of open standards, support for multiple applications, reliability including error detection channel hopping, determinism using TDMA, QoS support is also implemented in the case of u use of this particular pro protocol. QoS support is very important QoS guarantee is more specifically because, this is what basically ensures the determinism. TDMA we understand time slots predefined people know what is going to happen next. QoS support also is very important, QoS guarantees are important Because, you know we need to know that at least this is what is going to happen in the future by running this particular network using this standard. And security is also a very important feature of this particular protocol.

(Refer Slide Time: 18:40)

So, security is fully been built into this particular standard the ISA100.11a standard. Authentication and confidential services are independently available. A network security manager manages and distributes the keys. So, key management including key distribution key revocation etcetera. These are all taken care of by the network security manager. So, twin data security steps in each node include data link layer encrypting each hop transport layer securing peer to peer communication.

(Refer Slide Time: 19:16)



So, these are the different usage classes corresponding to different categories of applications. For safety the classes are 0 and one 0 stands for application such as emergency taking some emergency applications. Emergency action in some critical situation 1 is for closed loop regulatory control which may also be critical. Then we have category control category which has classes one 2 and 3. 1 stands for closed loop regulatory control for closed loop supervisory control, and 3 for open loop control. And then we have the category monitoring where the class 4 basically stands for applications such as alerting and plus 5 which is for logging and downloading. And this particular class the logging downloading class does not have any immediate operational consequence. So, with this we come to an end of this particular lecture. And we have not only gone through the ISA and ISA100.11a protocol, but also the Zwave protocol in this lecture. And we have also gone through previously in the connectivity technologies different protocols set such as zigbee which is based on 802.15.4.

Then we have gone through IPv6. We have gone through RFID we have gone through we have gone through NFC. We have gone through Zwave. We have gone through HART wireless HART, and we have gone through all different types of technologies that can be used for offering connectivity between different devices. These different connectivity protocols they all have their own distinctive features which make them very attractive for use in diverse applications of IoT implementation.

So, we come to an end not only of this lecture, but also the series of lectures on connectivity technologies.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

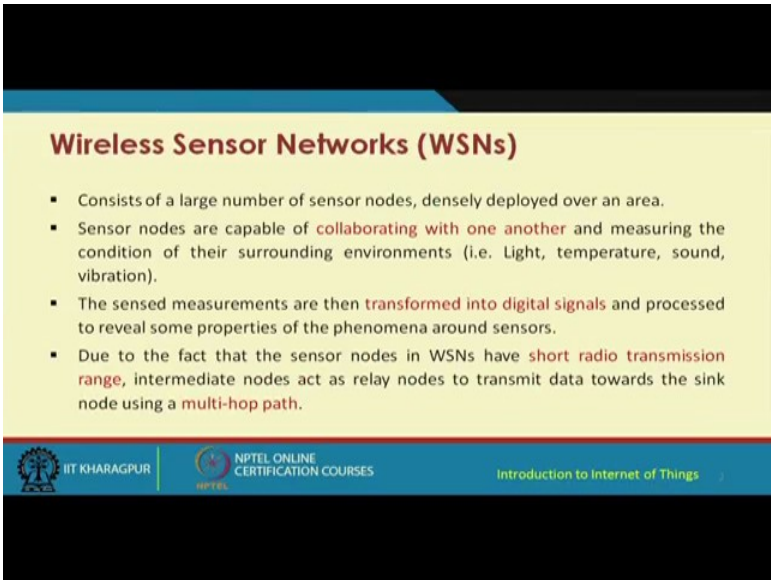
Lecture - 14
Sensor Networks – I

Now a very interesting series of lectures we are going to have, it is on sensor networks. So, the first part is going to be on some of the basic concepts in sensor networks. Sensor network is a very, very important technology that is used for building IoT. Sensors, transducers, actuators these are all very important things for realization of IoT systems. But, when we talk about sensors when we talk about actuators, these are the things that we have already gone through in one of the previous lectures. So, these are stand alone devices that we talk about, but if we can have these sensors connect with one an another we can derive important information continuously, in real time remotely, from a larger terrain. And, this is the benefit of sensor network. And sensor network I would say is one of the most important enablers of IoT.

So, in sensor networks what we have? In sensor networks we have individual sensors, which are embedded in something known as sensor devices or sensor nodes, or sometimes also known as sensor modes. So, these modes or nodes or devices they have one of their components which is the sensor, and they have other components as well. So, these components taken together they comprise that particular node or the device which can help them to communicate. And one device communicates with another device, that device communicates with another device, the third device with a fourth, fourth with the first and so on. And so, we can expand we can expand the sensing we can expand the sensing by having them communicate with one another.

So, what we have are different types of topologies. We can have all sorts of topologies that we have already heard of in networks being implemented in the case of sensor networks as well we can use a star topology. We can use a mesh topology we can have a mesh of we can have a mesh of sensor nodes that are all put together. Right, so we can have star we can have ring we can have you know any kind of topology that you can think of, and mesh is particularly very attractive for obvious reasons that basically includes reliability, security, fault tolerance of the topology itself

(Refer Slide Time: 03:15)

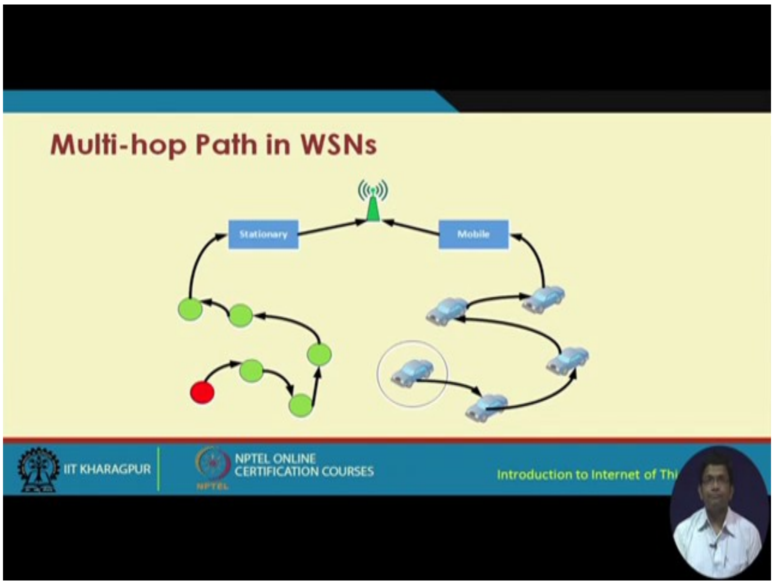


So, let us look at the different basics of sensor networks. So, in a sensor network we have sensor nodes. Every sensor node has a sensing unit. The sensing unit basically senses. Senses what? Senses the particular physical phenomena that it is supposed to sense. A temperature sensor would be sensing the temperature fluctuations. A humidity sensor will be sensing the humidity fluctuations. A camera sensor would be sensing; that means, taking the images of what is around you know what is happening around it.

A vibration sensor will be sensing the vibration. A light sensor will be looking at will be sensing the illumination conditions and so on. But each of them is sensing locally and, every other node that is deployed they are all doing their own tasks separately individually. And now, in a sensor network we all have to we have to put them all together; we have to put them all together how it is possible to put them together? We have to just have some kind of radio connectivity between these different devices. These devices means their sensor nodes and, this is how we build up a sensor network. And what is the main motivation of building a sensor network? To have greater coverage of sensing and, continuously we can monitor in real time we can monitor remotely we can monitor what is going on in a particular terrain, without actually having somebody humanly sitting and monitoring that particular region or space.

So, the sensor nodes are capable of collaborating with one another. And measuring the condition of the physical phenomena that are occurring around them with respect to what into what they are supposed to sense. For example, the lighting condition, temperature, sound, vibration etcetera the sense measurements are then transformed into digital signals and process to reveal, some properties of the phenomena that are occurring around them. So, due to the fact that the sensor nodes in sense WSNs wireless sensor networks have short transmission range. Immediate nodes act as intermediate relays and, they transmit the data that they receive from these other frame nodes the other neighboring nodes in a multi hop manner, until the data is received at the sink node.

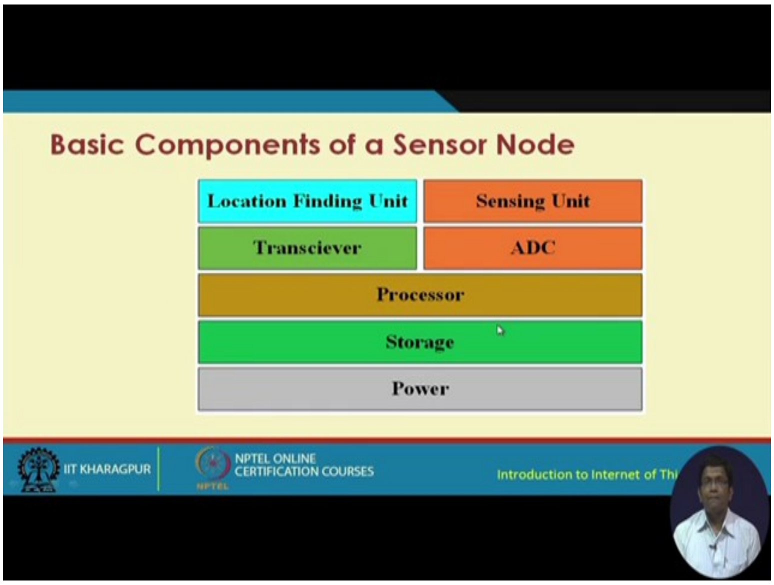
(Refer Slide Time: 05:55)



So this is how the entire sensor network concept functions. So, what we have is multi hop communication. So, let us consider a stationary sensor network. Stationary means what? Stationary means that, the node all these nodes, when they are deployed they will maintain the position at subsequent instants of time after deployment. So, they will all maintain their own respective positions. And they will not move they are all stationary the nodes are all stationary. So, this is an example of a stationary sensor network. Mobile sensor network on the contrary, have the sensors and the sensor nodes that move around like this.

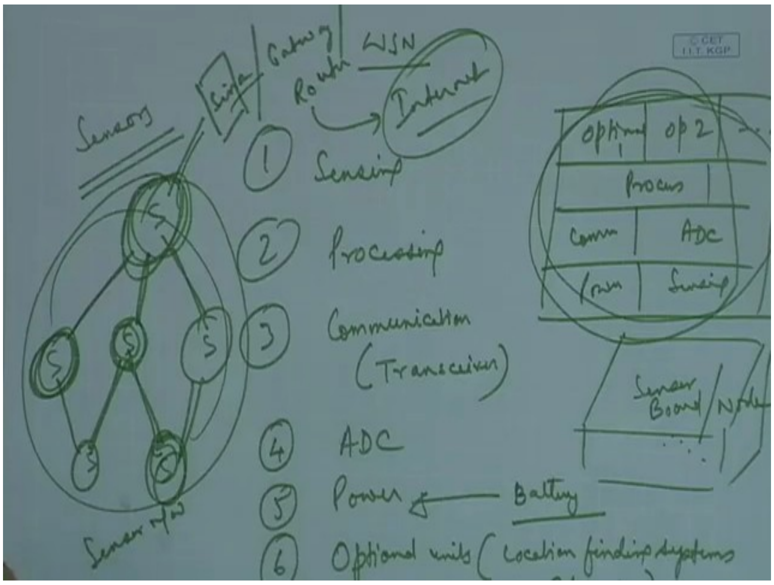
So for example, the sensors that are fitted to a car, to an airplane, to a truck to, a bus and so on. These become mobile sensors mobile sensor nodes because, they are fitted to devices which move with time. So, they become you know together when you connect them in this manner, what you get is a mobile sensor network.

(Refer Slide Time: 07:16)



So, if we look at in a sensor network, what we have? In a sensor network we have different units. So, WSN we have different units.

(Refer Slide Time: 07:28)



So, the first thing that is required is to have some kind of sensing unit. Then we have some kind of a processing unit. Third is we need some kind of communication to take place between these different nodes. So, we have a communication unit, you with the help of transceiver devices. Then we have different other units such as, the analog digital converter, we have the power unit, we have, power unit will do what? Are in it includes things such as battery and so on, which is going to power these devices. So, these are the different units. And then we have other optional units optional units such as the location finding systems for example, GPS etcetera.

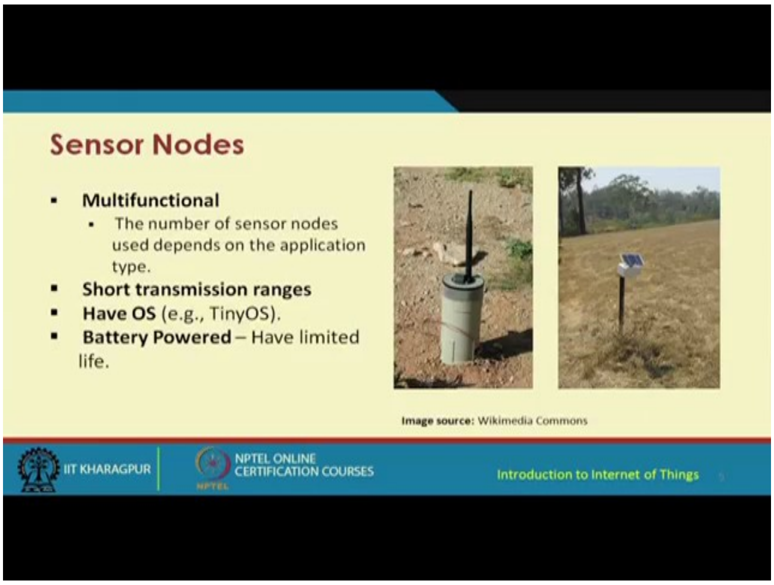
So, this is how a sensor node looks like. So, we have you know in all these optional units optional unit 1 optional unit 2 etcetera. We have a processor, we have a communication unit, we have analog digital converter, we have a power unit, we have what did I miss out a sensing unit, a processing unit, it is already given and so on and so forth. This is how a sensor node looks like. So, if you recall in one of the previous lectures when we talked about sensors, we also talked about the different types of sensors. So, what happens is you know we have to develop something like a sensor board. So, this becomes a sensor board or a sensor node or a sensor device.

So, this sensor board the hardware of it has different components. All these different components that I just mentioned, all these different components are basically built into this hardware device. So, you need to have a particular circuit design for building these sensor nodes with these different components. So, essentially what are we trying to do, we are trying to have, so let us say the this is one such sensor node communicating with another sensor node, with another sensor node, with another sensor node sorry, with another sensor node and right.

So, we are going to form a sensor network. So, what I these are all sensors, these are all sensors, sensor nodes. So, mind you that in every sensor node we have a sensing unit. And sensing unit has the sensor that we are. So, temperature sensor is basically built into that sensing unit of that sensor board.

So, then what happens? So, through a multi hop path all these sensed information are sent to the sink node or the gateway or this router for further dissemination to the internet. So, then what happens is finally, all this sensed information they will all go through the sink to the internet for further use. This is the whole purpose of this sensor node.

(Refer Slide Time: 11:48)



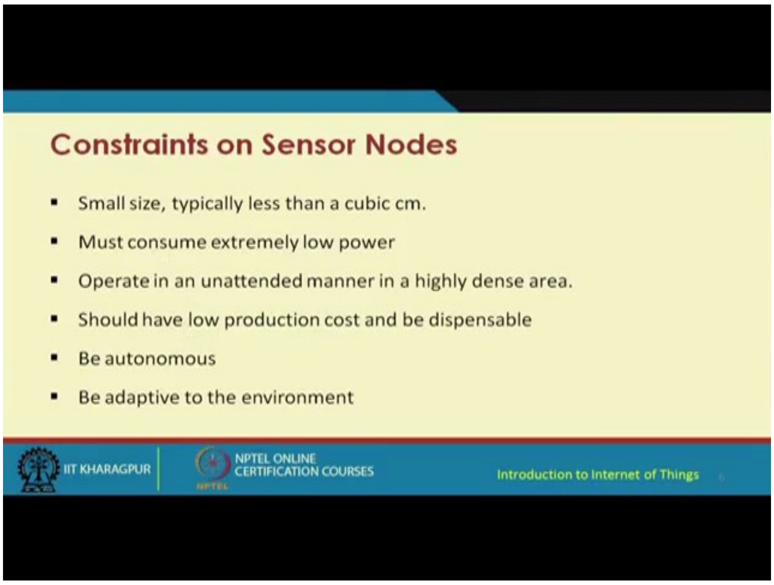
So, this is these are some of the pictures of sensor nodes as you can see in this particular figure. So, this is one such figure. One such sensor node here is another sensor node. I will show you a sensor node that we have basically deployed for different purposes. One of one such purpose is for agriculture. In our agricultural field we have sensor nodes that are deployed and these are all solar powered.

So these are solar powered you know sensor nodes. So, the power unit basically has a battery which basically hardnesses. Not battery but, you know it basically hardnesses the solar energy through the solar panel and powers the rest of the components of the node. The sensor nodes are multifunctional. So, they can be used for different purposes. In fact, the sensor board you know you can change different sensors and you can use the sensor board the different components of it, put together, you can remove the sensor, you can put another sensor and typically you know it will work for serving different types of applications.

So, the number of sensor nodes that are used depends on the application type. The sensor nodes they have short communication range, may be powered by zigbee. A zigbee has very short communication range. So, this short communication range means that the sensed information by a particular node can be sent only up to couple of meters or tens of meters. And after that what? Finally, it has to be sent to the sink node. So, after that what? After that within that communication range of let us say thirty meters if it is zigbee up to above thirty meters then we need to have another node which again has to relay that information that has been received from this particular node.

This is how we have this multi hop communication taking place between these different nodes in the network. Multi hop, multi hop means what? A particular node has to send something to a remote destination, but it is not within the direct communication range of it. So, what it will do is, it will send to some of it is neighbors. These neighbors will relay the information or the data the sense data that has been received. And send forward and this is this process is going to continue until the data is received at the intended destination nodes or the sink node. So, this is multi hop not single hop. So, source node to the sink node sink node not within the right communication range of the source node. There has to be intermediate nodes acting as relays and this is the whole idea of multi hop communication in sensor networks.

(Refer Slide Time: 14:35)

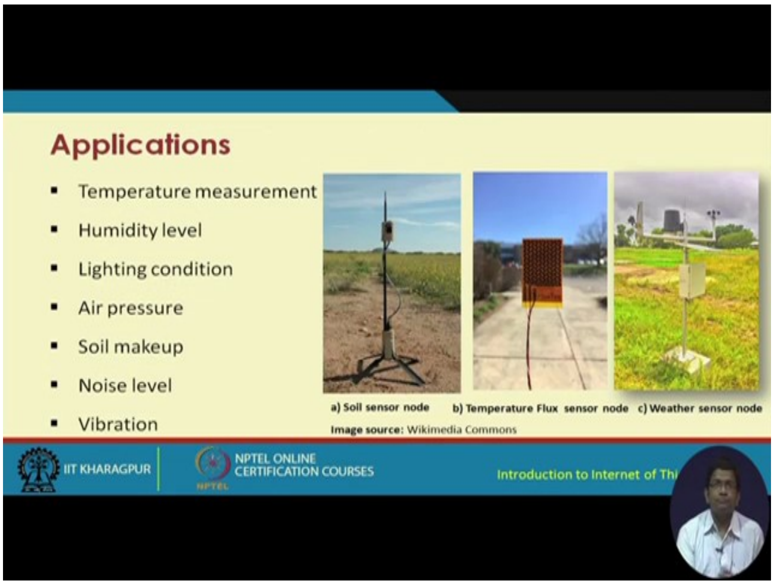


These sensor nodes I should also mention, that these sensor nodes are all not only battery powered. But, they act as mini computing devices. So, they have their own processors and we have already seen that. Processors microcontrollers and so on. They have their own they have their own power unit. They have their own communication unit plus they have their own operating system. One such very popular operating system that is used for sensor nodes is known as the tiny operating system tiny OS.

So, these are the different features and, now let us look at the different constants on the sensor node. So, the sensor nodes are typically small in size, low powered, resource constraint in all different ways, although they are acting as small size computational devices, but they are heavily resource constrained in all different ways that you can think of. So, due to their small size typically in the order of few cubic centimeters or even they can be little bigger also if it is not a mains based sensor.

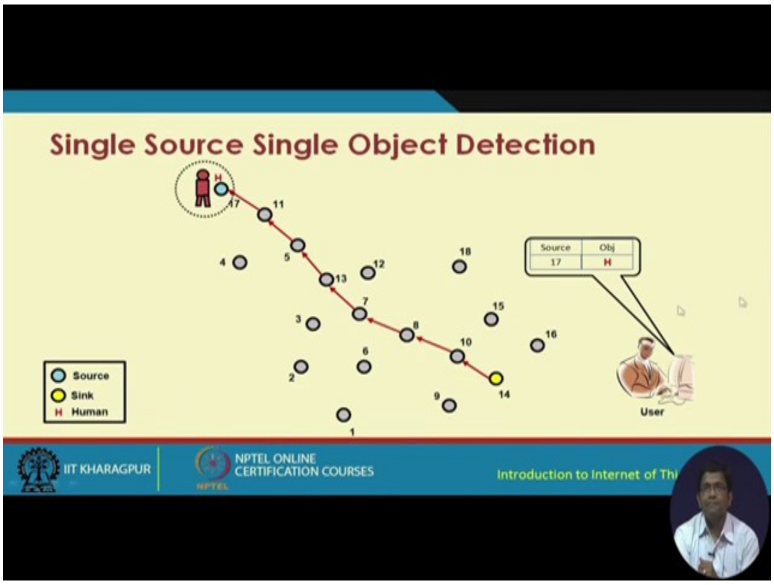
So, because of the small size they must consume extremely low power. They must operate in an unattended manner in a highly dense area, should they should be produced using low cost at low cost, production costs should be less, and they should be easily dispensable. They should be like couple of dollars few hundred rupees and so on. This would be autonomous they should be able to operate on their own and be adaptive to the environment in which they are operating. So, if there is some change in the environment this should be able to you know automatically this would be able to adapt to those changes

(Refer Slide Time: 16:18)



Here a few examples of sensor nodes soil sensor node temperature sensor node weather sensor node and so on, all deployed in real life. And for serving different applications such as temperature measurement, humidity level condition measurement, lighting condition, air pressure, soil makeup, noise level, vibrations and so on.

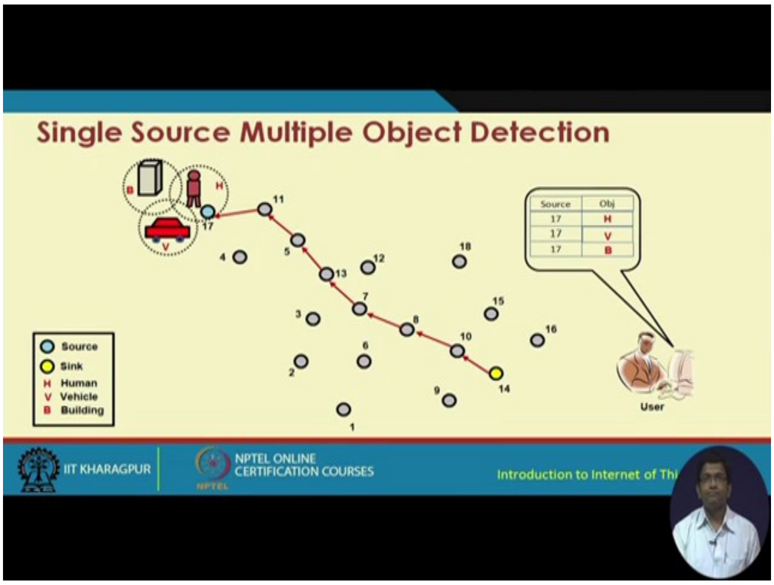
(Refer Slide Time: 16:40)



Now, let us look at few important concepts in sensor network. So, we have seen that in sensor networks we have different sensor nodes that a deployed in a particular region. The sensor nodes they have to communicate via multi hop communication. So, let us say that we have a surveillance kind of application, and where it is required to detect objects. So, as we can see in this particular figure, that the sensor node 17 detects a human object. And that information through this multi hop path is sent to the sink node 14 and there is a monitor a user who is continuously monitoring that, where it can see you know close to which sensor it can see any object, any human object or whatever object it is programmed to sense.

So, as we can see in this particular figure that, node number 17 has seen has sensed a particular object the human object. Now it is going to send the data in this particular direction as we have already seen. But then, why is this arrow shown in the other direction? These arrows are shown in the other direction to signify that, from this sink a query can be sent to all the nodes the query can be sent to all the nodes to see that whether any of them has observed any object around them. So, this is the direction in the other way that is shown that is the whole purpose of showing it in that particular other direction. So, the previous example was for a single source detecting a single object.

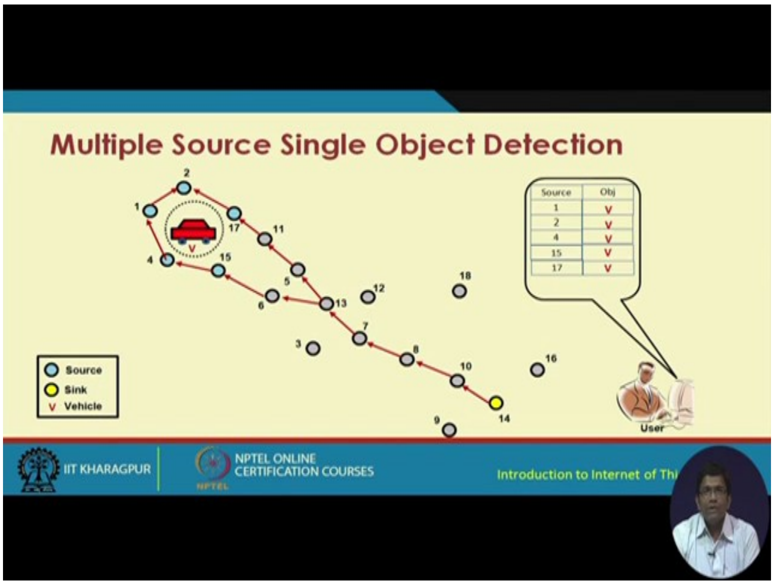
(Refer Slide Time: 18:28)



Now, let us make our life little bit more complicated. So, we have single source detecting multiple objects. So like this. So, earlier there was only human object now we have two more objects. So, we have a vehicle and we also have some other building or something like that. So, we have 3 different objects a human, a vehicle and a building. So now, you as we can see over here, it becomes very difficult for this particular node to recognize that what are the different objects. So, because there are there is not a single object, but three different types of objects and what object. So, object recognition is also very important. So, here in addition to object recognition the complexity is that whether node number 17 will think that, it can see only a single object or 3 different objects. This is something that has to be decided upon. So, you see that by adding few objects only within the periphery of within the vicinity of a single node the life has become So complex.

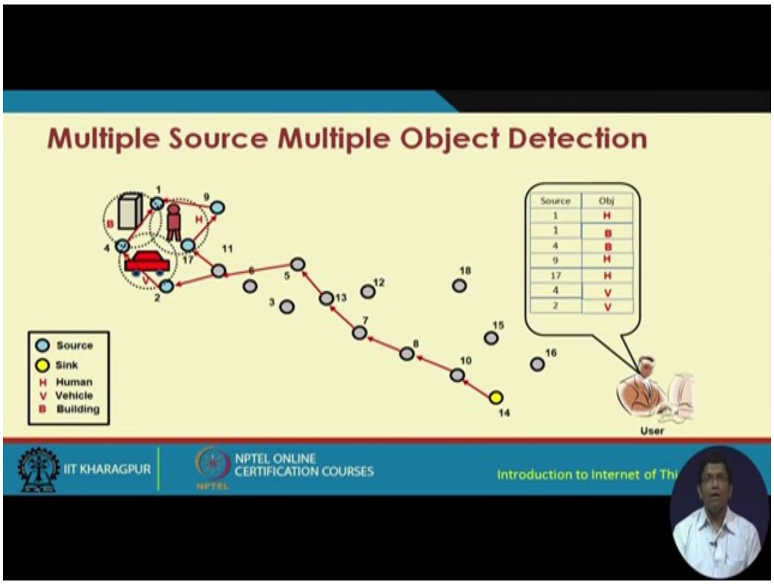
So, so this is the whole idea behind the use of sensor networks for this thing. But we have seen that, by adding few complexities the entire complexity of the entire network increases manifold.

(Refer Slide Time: 19:56)



Now, we see another scenario of multiple source detecting a single object. So, here the single object is a vehicle and, all these blue colored nodes they all act as sources and they sent that sends information to the sink node. Now the sink node and the user that is connected to the sink, the complexity now is that, it will try to understand that whether all these 5 nodes have seen a single object; that means, a car a vehicle or 5 different objects. How will it know? It is not possible. It is difficult to basically a discriminate between these sense data that are received from 5 different nodes, and that is the reason why it is not possible to know that what is the difference. I mean whether it is the same object that is this you know that is all seen by the although all the 5 nodes or 5 different objects.

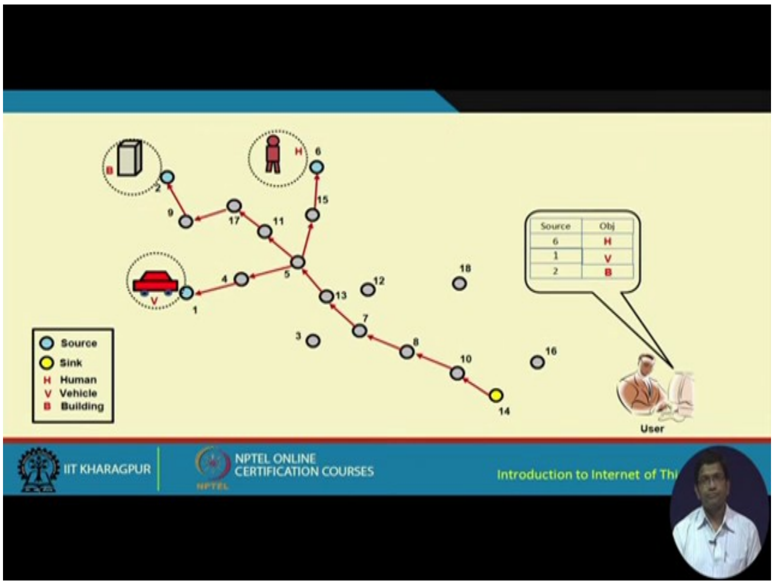
(Refer Slide Time: 21:00)



Another example of multiple sources detecting multiple objects like in this particular figure. And here again you see that complexity is quite increased.

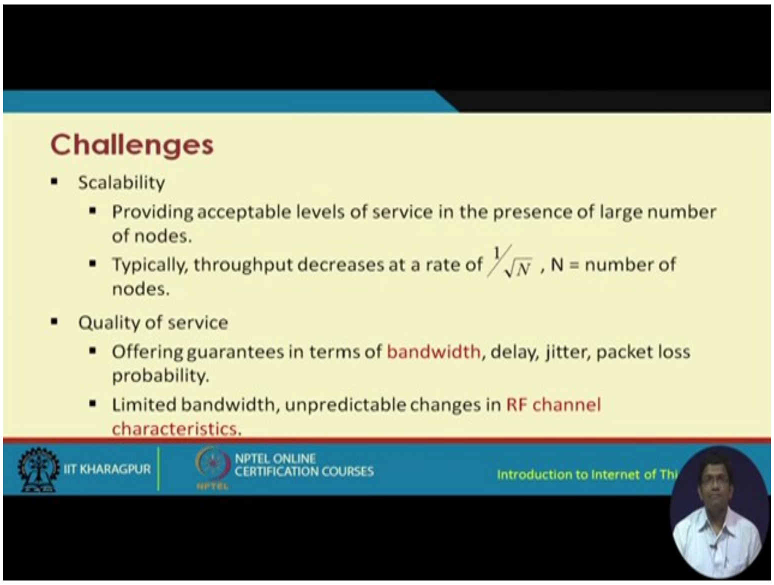
So, these 5 sources whether they have detected 5 different objects or the same object and not only that, but also whether these objects are all different. So, these are the different complexities that are involved in implementing sensor networks. But these are only some of the primitive complexities that we are talking about. There are So many different other sorts of complexities that also have to be worked upon that also have to be implemented when we are talking about using sensor networks to build internet of things.

(Refer Slide Time: 21:48)



This is another scenario and I do not need to explain this further. And as we have seen that this basically you know these scenarios of surveillance basically complicates our life, it is not very simple. And here mind you that in all these 4 5 scenarios that I have just shown you, here we have considered that the nodes are all static and with respect to time. But in reality it is not going to happen, the nodes are going to move around.

(Refer Slide Time: 22:18)

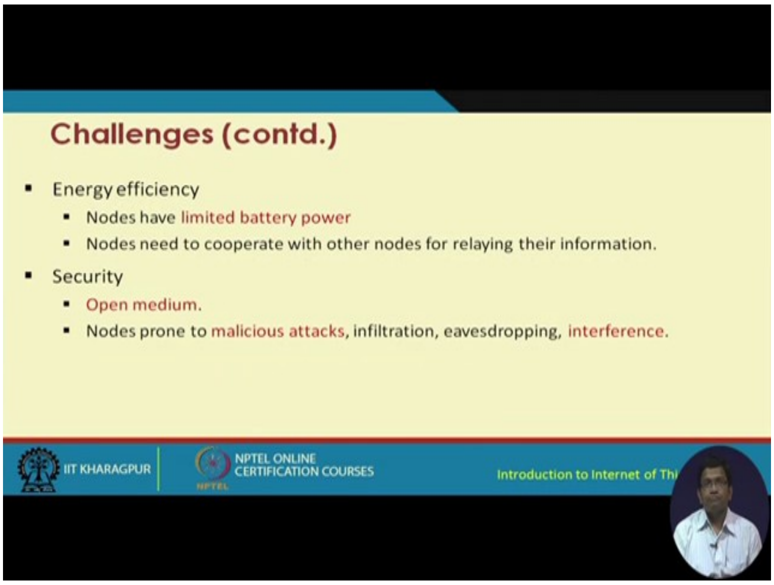


So, what is going to happen? The complexity is going to be even increased further. So, there are different challenges in implementing sensor networks. Scalability is one.

Scalability means that if you are increasing the number of nodes in the network, then how is the throughput going to behave? So, theoretically in the past it has been shown that, if n denotes the number of nodes in the network then the throughput basically decreases at the rate of one over square root of n. And this is as we can understand that from 2 nodes to 4 nodes if we increase the throughput basically goes down drastically. Now from 4 to 8, 8 to 16 and so on and so forth. The throughput decreases quite fast. So, how you are going to handle the issue of scalability in sensor networks? Because, in sensor networks we are inherently talking about networks with large number of nodes. And So, how do we handle the throughput decrease in this particular manner?

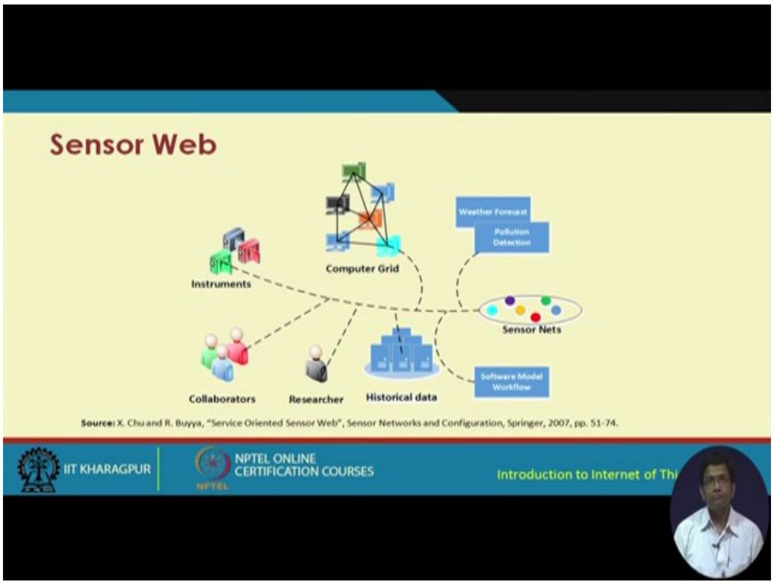
Second issue is quality of service. Quality of service guarantees is required for any network. Sensor networks, IoT using sensor networks, also you know need to have seen you know quality of service guarantees. Quality of service guarantees talks about offering guarantees in terms of the bandwidth, delay, jitter, packet loss probability and so on and so forth. And in a sensor network we are talking about, very limited bandwidth heavily constraint network with heavily constant resources, unpredictable changes in RF channel characteristics and so on.

(Refer Slide Time: 23:51)



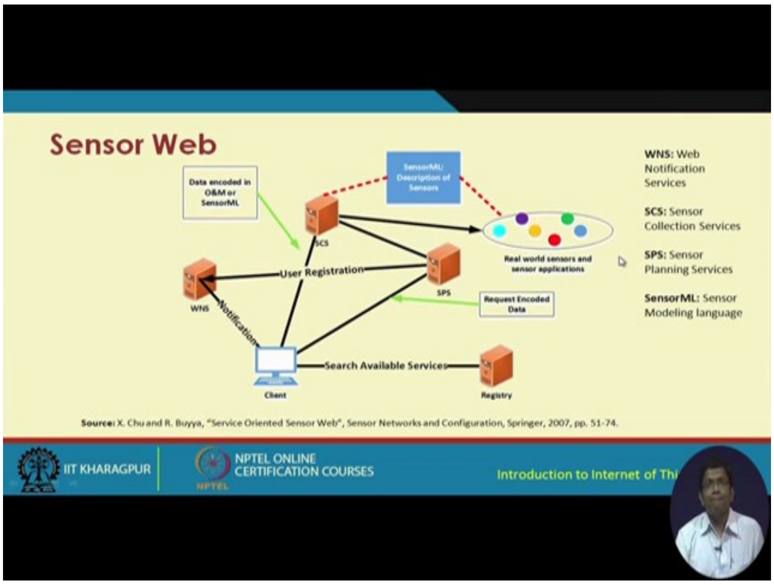
So, in such kind of chaotic environment, how we are going to offer deliver quality of service guarantees? Other challenges include energy efficiency. We are talking about very limited battery power small size batteries, low electrochemical efficiency, limited battery power, how we are going to have these nodes not only function their own things, but also cooperated cooperate with the other nodes the neighbors to relay their information and so on and so forth. Security is also very important. We are talking about an open medium where the nodes are prone to different types of attacks, malicious attacks, infiltration eavesdropping interference and so on.

(Refer Slide Time: 24:25)



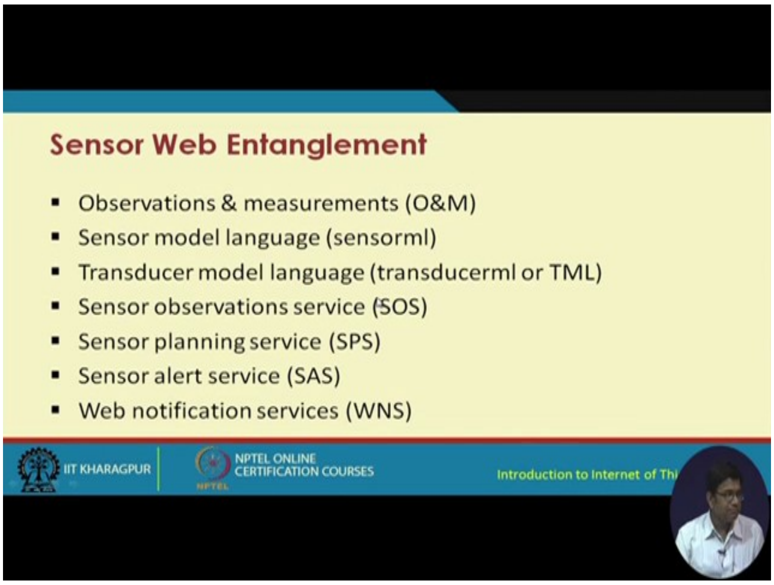
Now let us look at little bit more you know glittering kind of technological concept in sensor network, which is known as the sensor web. In sensor web what we are talking about is not just the sensor networks, but also sensor networks connected to sensor networks. So, what we have are different types of sensor networks like this which are connected 2 different things like computer grid 2 different instruments such as microscope telescope and so on. Scientific instruments; different collaborators through mobile phones etcetera, researchers, different historical data legacy data, which a store in data servers are you know server forms, cloud etcetera. And taking care of issues such as weather forecasts, pollution detection, software model workflow and so on.

(Refer Slide Time: 25:26)



So all these together form what is known as the sensor web. So, in sensor web we have to deal with different types of servers which will take care of web notification services, sensor collection services, planning services, modeling language and so on. Where is the modeling language? We have the sensor modeling language like right here and so on. So, all these WNS sensor collection service running service SensorML.

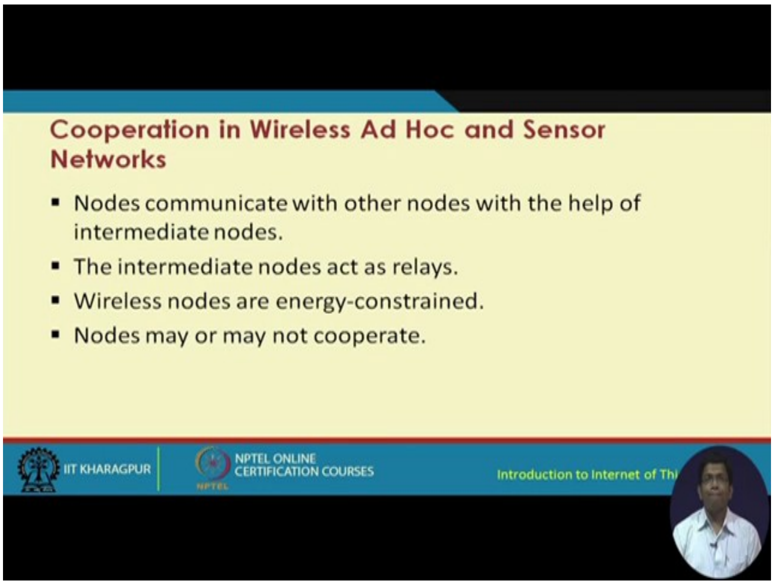
(Refer Slide Time: 26:59)



And so many different types of concepts and components that have to be used.

So in sensor web we have concepts of observations and measurements SensorML, which is sort of like an XML extended XML, a very similar in lines with let us say UML, you know some kind of a modeling language that supports sensor modeling. Then we have the transducer modeling language, transducerml sensor observation service sensor planning service sensor alert service web notifications services. All these put together basically a constitutes the sensor web.

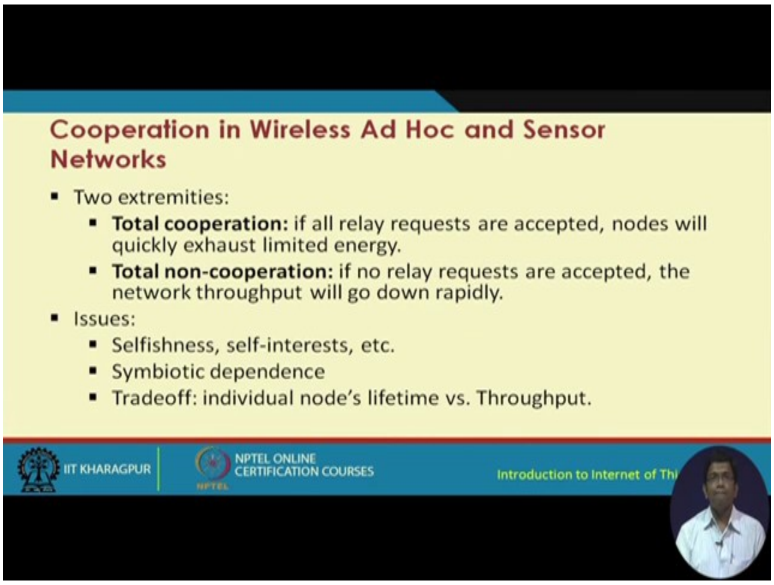
(Refer Slide Time: 26:33)



Now, few other concepts have to be taken care of. One is the concept of cooperation. Cooperation is paramount we are talking about you know a multi hop network, where there are relay nodes in between. So, what happens if these intermediate relay nodes instead of forwarding the packet further, they drop the packet because they will tend to be selfish. They will tend to be selfish because, to forward the packet to relay the packet forward they would have to expend their own little energy. So, why would they do that?

So these nodes are supposed to be cooperative, but, but they may not be as much cooperative because of all these selfish interests you know, resource limitations and all these different other types of considerations. The intermediate nodes act as relays. The wireless nodes are energy constraints the notes may or may not cooperate consequently. Because of all these different constraints, the nodes may not be willing to cooperate with the other nodes for collectively accomplishing the tasks that are supposed to be required to be accomplished in such a social network, socially connected network.

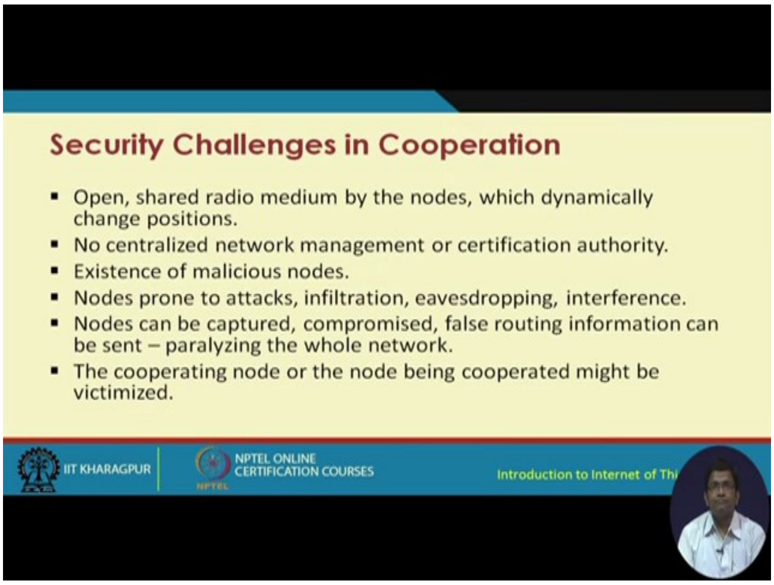
(Refer Slide Time: 27:48)



So taking care of the issue of cooperation, there are 2 extremities that have to be thought about. One is the total case of total is total cooperation. And the other one is the case of total non cooperation. Case of total cooperation where all the relay requests that are received are accepted by the nodes and the nodes will quickly exhaust the limited energy. And the case of total non cooperation if no relay requests are accepted the network throughput will go down rapidly. So, these are the 2 different extremities and, they are corresponding limitations are mentioned over here. So, if none of the relay requests are by are accepted, then what is going to happen? The network throughput will go down rapidly.

So there are issues of selfishness, self interests, symbiotic dependence between these different agents, there have to be worked out. That have to be increased in order to symbiotic dependence has to be increased, not selfishness of course selfishness is a problem self interest selfishness are problems that have to be handled. And symbiotic dependence how it can be promoted? And that also has to be thought of, and corresponding mathematical models have to be developed. And the trade off is between the nodes lifetime versus the throughput.

(Refer Slide Time: 29:03)



There are security I challenges in cooperation. So, first of all we have to get back to our old concept; that means, multi hop network. In a multi hop network sensor node, the intermediate node is cooperating with other nodes.

Now that cooperating node is a good guy. So, that good guy by looking at it there are so many you know there could there could malicious nodes, which might want to intentionally hurt the successful functioning of it and the other similar kinds of nodes. So, what it can do is it can initiate a denial of service attack kind of thing. So, what it will do is it will start you know pumping in lot of false routing information, that and thereby paralyzing the whole network. So, this is basically one of the security challenges in cooperation.

So, with this we come to an end of the first lecture on sensor networks for developing internet of things. And in subsequent lectures we are going to go through the different other concepts in sensor networks we have already seen that there are so many different types of constraints and challenges that have to be overcome in a sensor network, and that is where the sensor networks have to work on to, you know to come up with different solutions that have to be implemented in them to make them work efficiently.

Thank you.

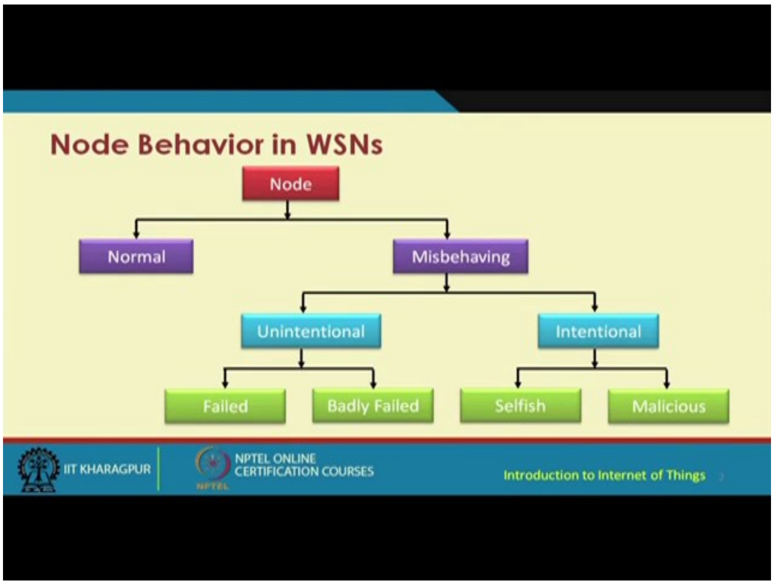
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 15
Sensor Networks – II

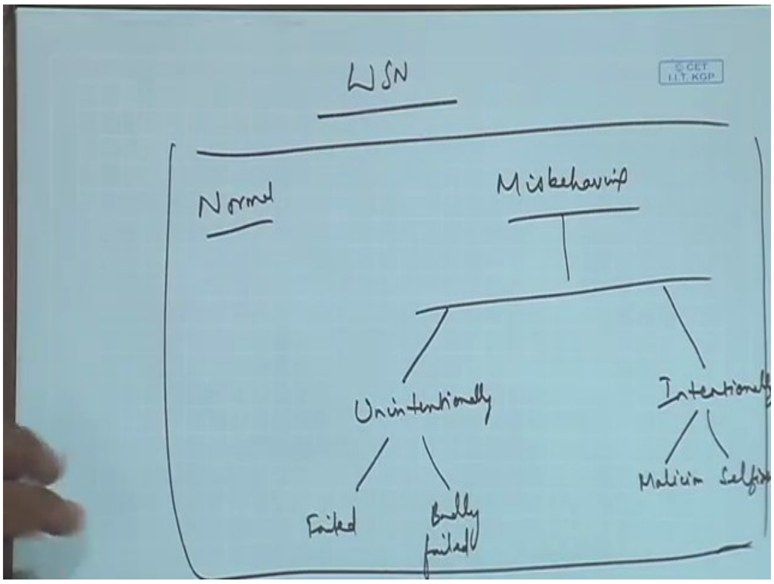
In the previous lecture we have already gone through some of the basic concepts of sensor networks. We have seen that by interconnecting the different nodes in the network, we can have an extended coverage of sensing and, that way we can also have emote real time distance monitoring of what is occurring around this physically deployed nodes in the network. We have also seen that there are different types of sensor networks. Stationary sensor networks, mobile sensor networks. And mobile sensor networks again can be of different types. One is aerial mobile sensor networks; that means, the mobile networks which move you know, sensor networks that move in the space we have terrestrial sensor networks. So, where the nodes they move on the surface of the earth. And we can have underwater sensor networks where the nodes basically move in the underwater area.

So, whatever be the sensor network, whether it is underwater terrestrial or aerial these nodes they basically have to cooperate with one another. In order for the network to function if the nodes do not cooperate they will not be able to function. So, how to promote cooperation? So, before that we need to understand the behavior of the different nodes in the network.

(Refer Slide Time: 01:51)



(Refer Slide Time: 01:58)

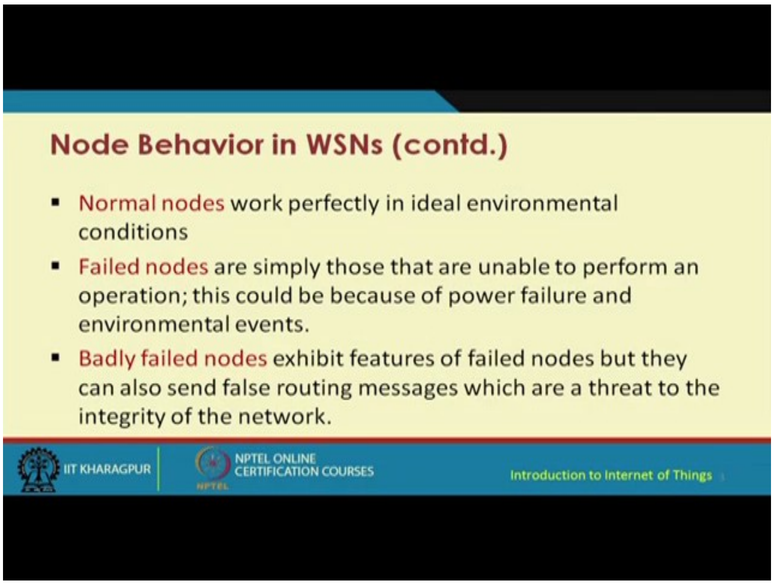


So, when we talk about sensor networks we have, we have nodes that would be behaving as they are supposed to behave. We can have nodes that would be misbehaving. So, we can have normal nodes we can have misbehaving nodes.

So, normal nodes we do not need to worry about they, you know as per the requirement the function the way they are supposed to function. Misbehaving nodes, this misbehavior can be of 2 types. One is that they misbehave unintentionally and the other one is where they misbehave intentionally you know intentionally they misbehave and unintentionally means they do not do not want to misbehave as such, but you know unintentionally they end up on end up misbehaving.

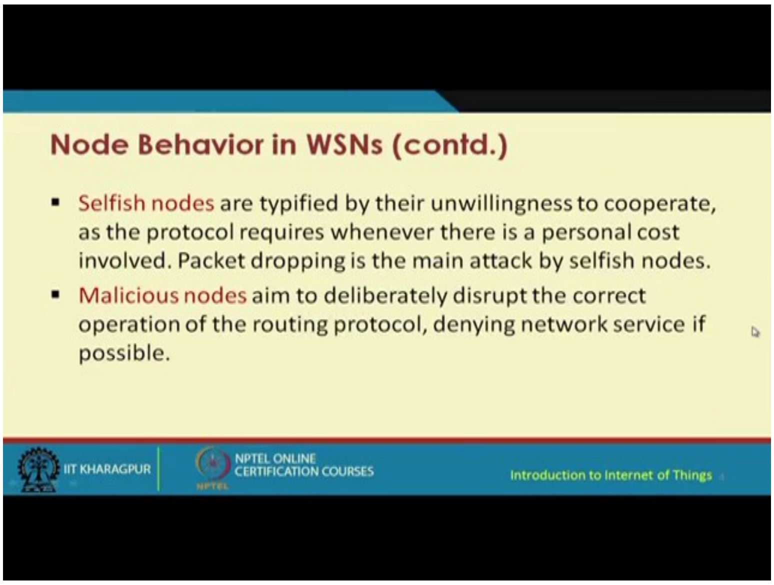
So, in the intentional category we have 2 types. One is the malicious node and the other one is the selfish node. And in the unintentional category, we have the failed nodes and the badly failed nodes. So, these basically forms the taxonomy of behavior of nodes in a sensor network ok.

(Refer Slide Time: 03:53)



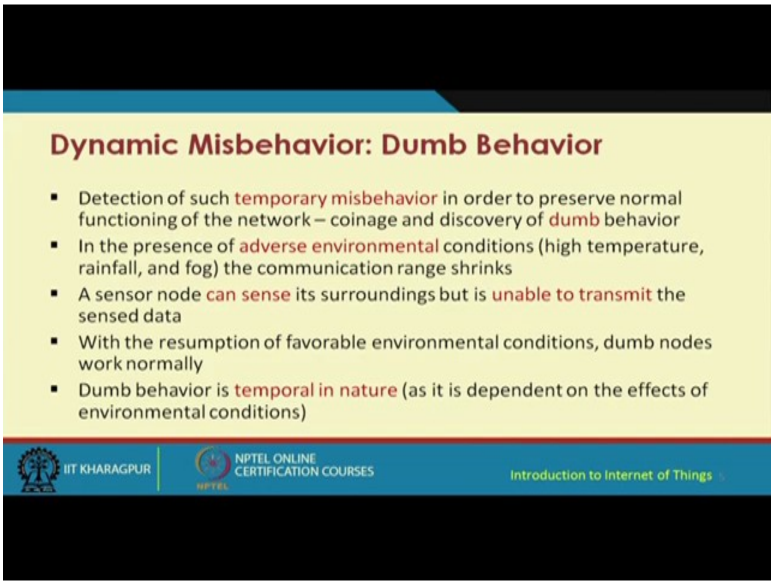
So going ahead we have normal nodes that work perfectly in an ideal environment condition. Failed nodes which are unable to perform the functions that they are supposed to perform maybe due to power failure, or maybe there is some hardware failure, or something of that sort. Badly failed nodes are like the failed nodes, but in addition they sent some false routing messages which basically hurts the integrity or the you know which becomes a threat to the overall integrity of the network. Selfish nodes are basically the ones which are unwilling to cooperate; they do not want to cooperate.

(Refer Slide Time: 04:29)



So, it is intentional misbehavior because, they do not want to cooperate because there is some personal cost that is involved. And packet dropping is one of the consequences of not willing to cooperate. So, if a node which is acting a selfish receives a packet. Instead of reeling it forward which it is supposed to do for successful operation of that particular network, it is going to drop the packet. And this is not desirable. And then we have the malicious nodes which are basically you know, which are like harmful nodes, which are a threat to the network, which want to successful deliberately disrupt the successful operation of the routing protocol or other protocols, and thereby they do not want to deliver the services that they are supposed to deliver.

(Refer Slide Time: 05:36)

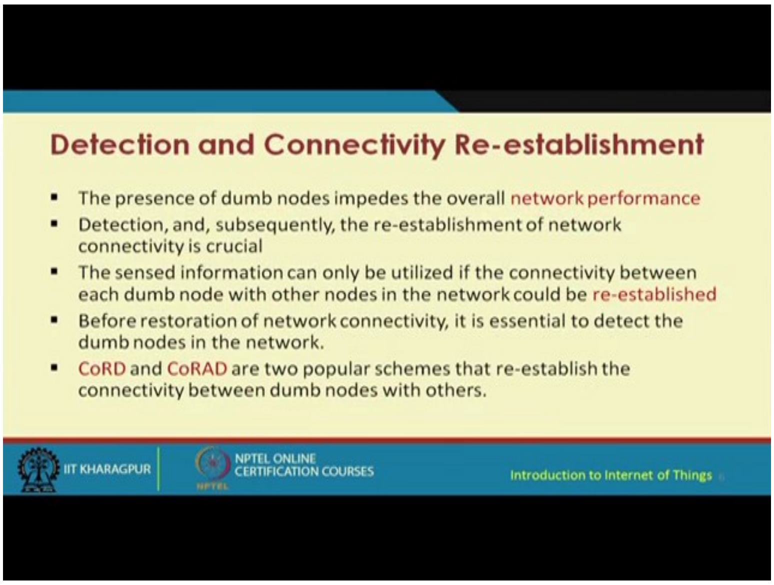


Another type of dumb load which was recently, very recently few years back only, developed or identified not developed, but identified by us in the SWAN lab, is the dumb behavior. And we are the ones who basically detected the existence of this kind of misbehaving node. This is an unintentional misbehavior. So, in this kind of misbehavior, unintentional misbehavior, what happens is these sort of miss behaviors pop up whenever there is some change in the environmental conditions. Maybe there is heavy rainfall, maybe there is heavy snowfall, maybe there is heavy fog and under those circumstances naturally as we know there is you know signal problems that are going to happen. So, a node is going to sense a sensor node is going to sense, but then it is not able to send it forward, it is not able to communicate. Because, of all these weather conditions or environmental conditions. So, that is the reason why the transceiver unit is not able to communicate at all. Or even if the signal strength goes down drastically. So, what happens is that there is no node in this facility.

So, because there is no node in this facility, essentially it is the effect is that it is not able to communicate, it is not able to delay, it is not able to send the sensed information to another node because, there is no such node. The range has shrunk; the range has decreased due to all these weather conditions. And we have coined the term dumb because, these nodes basically behave like sort of you know some sort of you know behavior of dumb persons who can hear, but who cannot speak out, a disability of these kind of differently abled persons, because of which they are not able to. They can they can listen they can see everything, but they are not able to speak out and because of this kind of mimicking behavior with these kind of nodes the sensor nodes we term, these nodes this behavior as the dumb behavior.

Now, this dumb behavior is transient, it is temporary. Temporary means, that it will last only for the duration when the weather condition is bad. Now when the weather condition improves subsequently again the regular communication you know goes on. So, these sort of behavior, unlike the other types of misbehavior are only temporary in nature. And that is why this is known as a dumb behavior. Only dumb behavior unlike other kinds of misbehaviors intentional misbehaviors, these are very temporary in nature, and you know, they occur unintentionally. So, this is very important to understand. Now what is required is to detect this kind of misbehavior and then you know, offer connectivity this reestablishment.

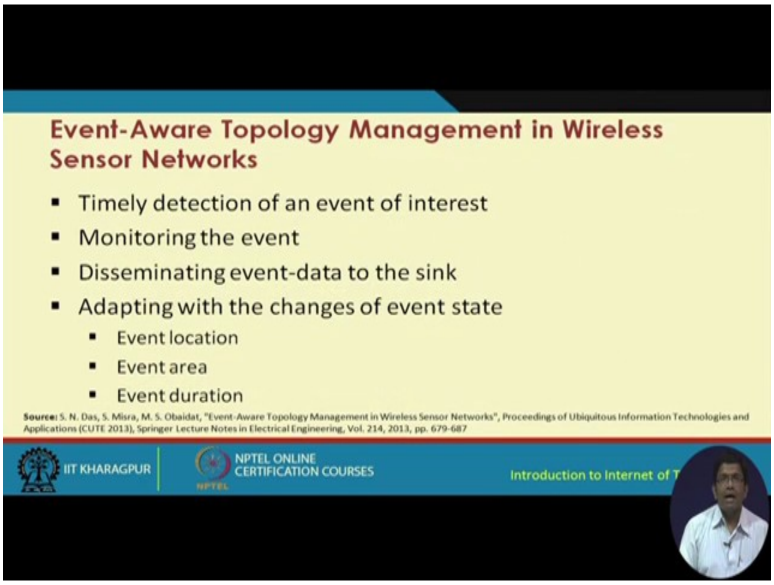
(Refer Slide Time: 09:20)



So, if this kind of see what happens is whenever this kind of behavior occurs in a sensor network. This kind of behavior will not occur typically in other types of networks. Because, sensor networks are typically deployed in hertz in the environmental conditions, in environments where the you know be all these physical things change quite fast quite rapidly and so on. So, since the networks are typical in for deployment in these kind of environments. So, what is required is to detect this kind of misbehavior happening in the network. Because, ultimately what happens, is the node which is not able to communicate it is completely cut off from the other nodes in the network. So, then how will it how in the other nodes know that it is cut off? So, there has to be detected somehow. So, we worked on this particular issue of how to detect this kind of temporarily cut off nodes the dumb nodes and then, how to establish some kind of connectivity, even in the presence of dumb behavior. So, that the normal network functions keep on running until the weather conditions improve.

So, 2 protocols, cord and corad were proposed by us in the SWAN group. And these protocols are available for further.

(Refer Slide Time: 11:02)

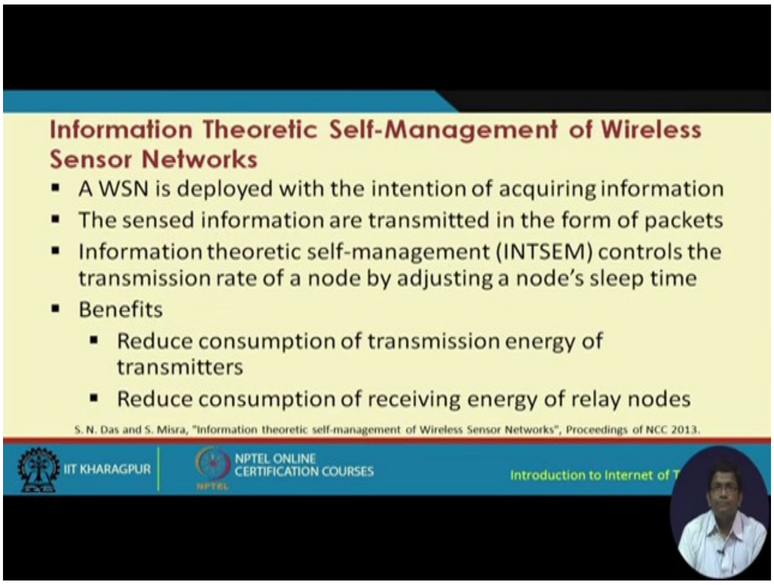


It is available in the internet for further reading. So, if you search with the cord and corad with few other suitable keywords you would be able to get access to these papers. So, these have been published in very prestigious venues like ACM transactions journal of systems and software of elsevier and so on.

Next, event aware topology management in wellness sensor networks, I also want it to give you a little bit of glimpse or flavor of this work. This also has been done by us in the SWAN lab. So, here basically you know we are talking about topology management. So, so topology management is primarily concerned about how to not only establish, but also how to manage the topology over time. How to keep the topology? How to keep the networks, the nodes in the network connected over time. So, that they cannot they can continuously sense and disseminate the data through them to the sink and adapting to the changes of the event state, with respect to event location event area and event duration.

So, this is what this particular work talks about. So, I am not going to, I am just going to give you little bit of idea about these works, but I am not going to go through each of them in detail. The corresponding reference is given for you are already use, if you are interested you know this paper you can please go through.

(Refer Slide Time: 12:45)



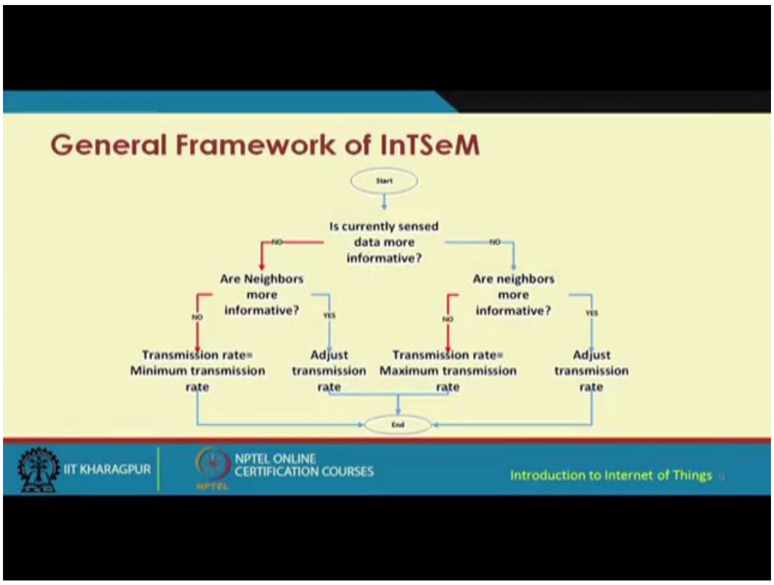
Another paper also done along with my student Shankar Nayayan Das, is this information theoretic self management of wireless sensor network. This is a fine work. Because you know, in sensor networks one of the problems is periodically the nodes this sense what is going on. Typically it is found that with respect to time it might so happen that the information content of this different sensed packets they do not change much. So, why do you want to unnecessarily overload the network by communicating those packets, where the information has not changed much?

So, what is required is at the source, detect how much the currently sensed packet, and the previously sensed one are correlated. And then through this measure, which where we are using advanced information theoretic concepts, we are identifying how much is the correlation between these sensed packets, and then send deciding upon which packet to send forward if they are sufficiently uncorrelated you sent the sensed packet, otherwise you drop it. You do not do anything further. Or queue it for sending it later, or do something else. This is one possibility. Other possibility is that, in a sensor networks typically the nodes are densely deployed.

Now it might so happen that 2 or more different nodes they have sensed data, they have sensed data which are sufficiently correlated. Then the point is that all those 2 or 3 different nodes if they all have similar kind of information content, why do you all want to have those 3 packets to be sent forward to the sync? Because doing so will unnecessarily overload this highly constraint network. So, we have again used tools from information theory, to basically address this particular issue.

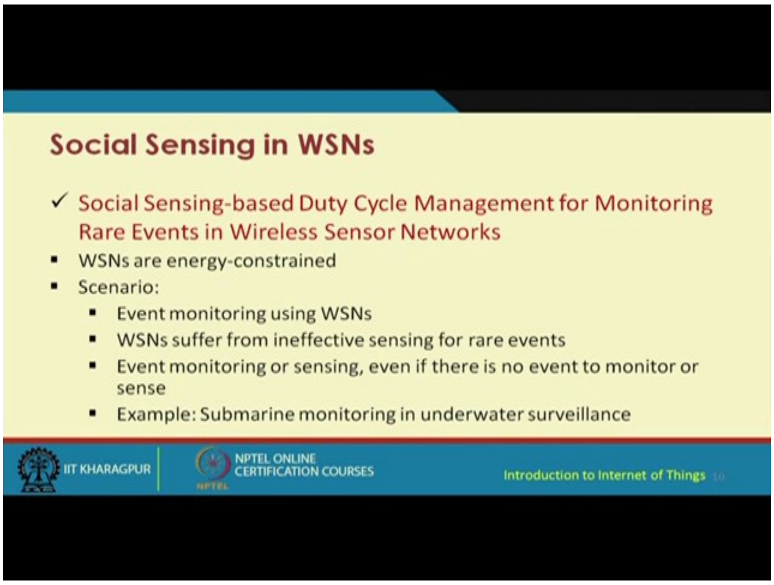
So, these ideas are very fundamental to sensor networks and we have addressed those, and I am trying to give you an exposure to all these different problems, so that you know that if you have to use sensor networks for IoT implementation what are the issues that have to be addressed for it. It is not like buying few IoT devices, few sensors, few different other devices and putting them all together we will have an IoT network. This is a common misconception, implementation deployment of IoT is heavily research intensive, it cannot be done in an ad hoc manner, you have to plan it properly and you have to design the protocols the design the algorithms, find out the different complications that are going to happen, and act accordingly.

(Refer Slide Time: 15:54)



Going ahead we have, so I will skip it is there for you. This is part of the previous information theoretic approach that I mention and finding the correlation between the different packets spatially as well as temporally. So, I am not going to go through it in detail, but it is available for you to go through in this particular slide.

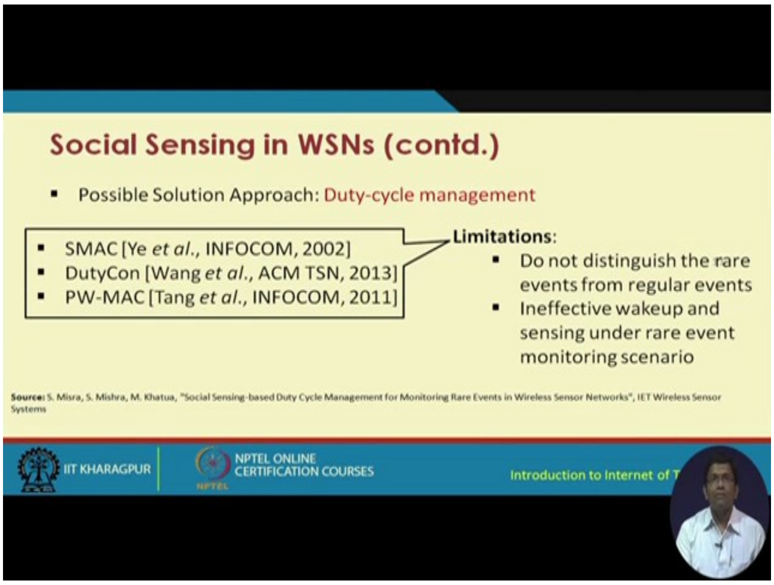
(Refer Slide Time: 16:14)



Another very important thing is social sensing. Social networks like twitter, facebook, etcetera, these are quite popular. At the same time sensor networks are also quite popular, but sensor networks duty cycling is very important because, of these low powered nodes. So, low powered nodes mostly have to be kept in a dormant or a sleep mode, and they have to be woken up periodically. Now when do you wake up, do you wake them up after a certain interval of time? Or is there a better way of waking them up?

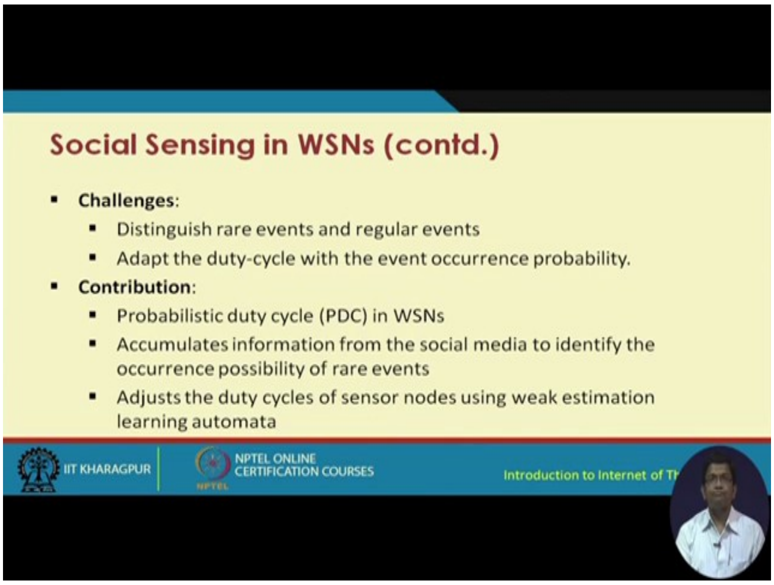
So, we basically studied this issue, and we have seen that if the social sensor networks are hooked up to the sensor networks sorry social networks over the internet then, we can exploit, we can exploit the information flow in these social networks to identify whether the sensing interval can be increased or decreased. May be that based on some you know cracking of the twitter data, there is a straight to the national security. So, the sensor networks that are deployed in the coast, in the water, for naval defense or for aerial defense etcetera, their duty cycle can be increased accordingly. So, can be put in more alert, but for rare events you do not need to improve the duty you know increase the duty cycles so often. You can keep them in a low duty cycle environment.

(Refer Slide Time: 17:58)



So, this is what this third work basically talks about and the source of this literature is also given over here. So, you can if you are interested you may go through this particular. But to understand, how social networks and sensor networks can be integrate together in order to improve the performance of the sensor networks.

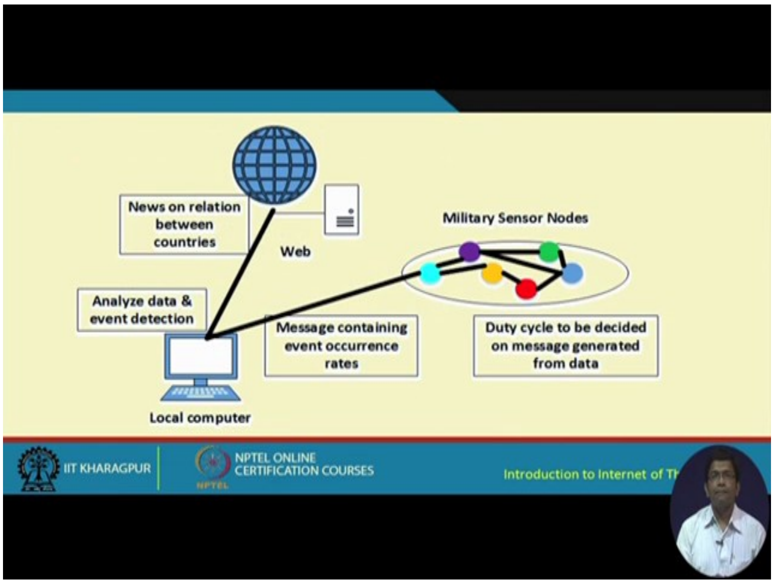
(Refer Slide Time: 18:18)



There are different challenges with social sensing. Distinguishing rare events and regular events, adapting to the duty cycle with the event or occurrence probability and what we have done is probabilistically we determine how the duty cycle is going to be managed.

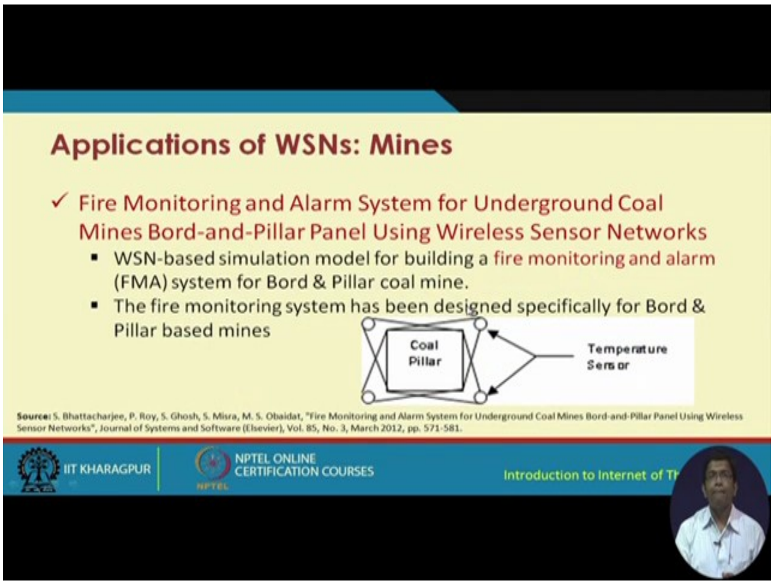
So, we accumulate information from the social media to identify the occurrence possibility of rare events, and adjust the duty cycles of sensor nodes using some learning, machine learning approach.

(Refer Slide Time: 18:52)



Again, so in this particular figure we see that let us say that this is a military sensor network, how this duty cycle is going to be changed over time of this, based on the data that is received from the web from social media.

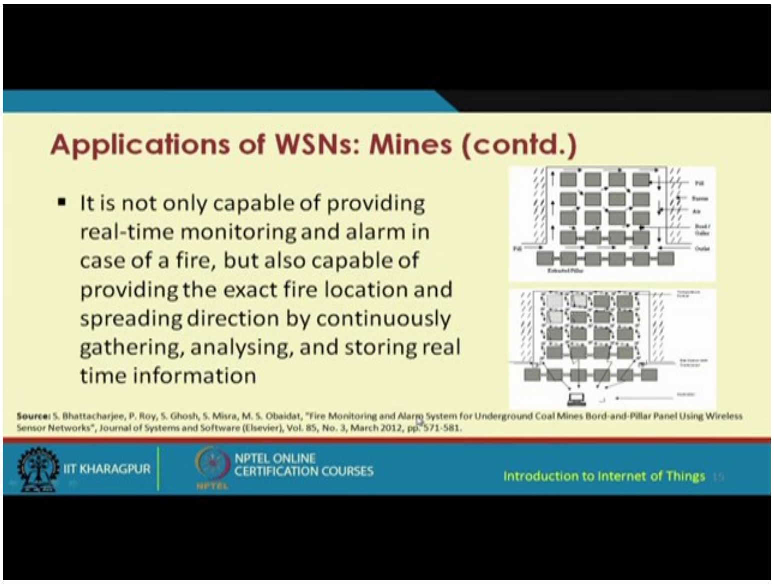
(Refer Slide Time: 19:10)



Sensor networks can be used for a diverse range of applications, for agriculture space applications, mining and health care and so on and so forth.

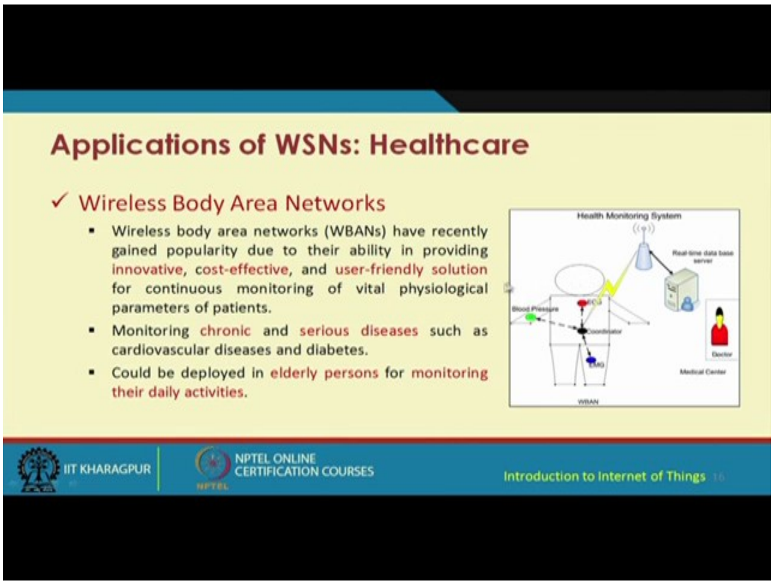
Here is an application of sensor network it for mines. In our country coal mining is very important. And one of the ways of coal mining is basically the bord and pillar coal mining. Bord, bord. Bord and pillar coal mining. So, in the bord and pillar coal mining, what happens is there are some columns these pillars, that are that are basically that is the way the structure of mining is done coal mining is done. Now in modern pillar coal mining So, what we are saying is will be putting different sensors so as to ensure that whenever there is a possibility of fire taking place, it will get automatically detected and it will alert the respective persons, and if indeed fire takes place then, to you know through the actuators to release water pulps in pipes and so on and so forth.

(Refer Slide Time: 20:27)



So, this particular paper whose source is given over here, basically talks about how to do it. So, these are the different columns the pillars and, these are the bord and the gallery. These are the different bords and the gallery and, this is how the sensors are going to replace, the temperature sensor, the gas sensors, and so on. These are all going to be placed and where the actuators are going to replace. These are all shown over here in this particular.

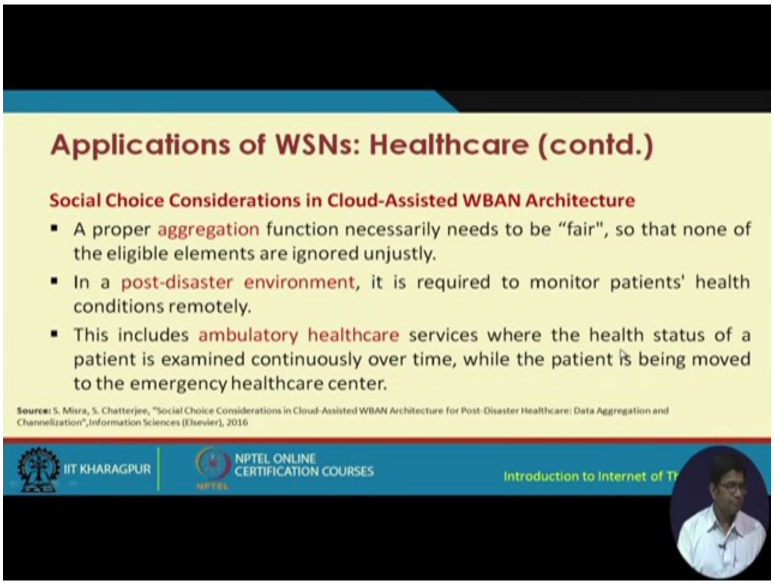
(Refer Slide Time: 20:48)



Now, the other work is healthcare, the other application domain is healthcare. In healthcare what happens is the humans are fitted with different physiological monitoring sensors. Sensors that will monitor physiological conditions with respect to body temperature, blood pressure, you know oxygen saturation in the blood, you know cardio cardiac functionality, a functioning and so on and so forth.

So, when these sensors are all put together on the human body, they can all sense about that physiological functioning of that particular patient, and sends you know send that sensed data to a local unit on the human body, typically mobile phone kind of device, which is technically known as the LPU the local processing unit. So, this becomes the LPU the coordinator. So, all these sensors we will be sending the sensed information to this particular coordinator, and this becomes, this unit because something known as the w ban, or wireless body area network. And from here the data is sent to the you know, through the internet, to the server for doctors to understand remotely the condition of the patient.

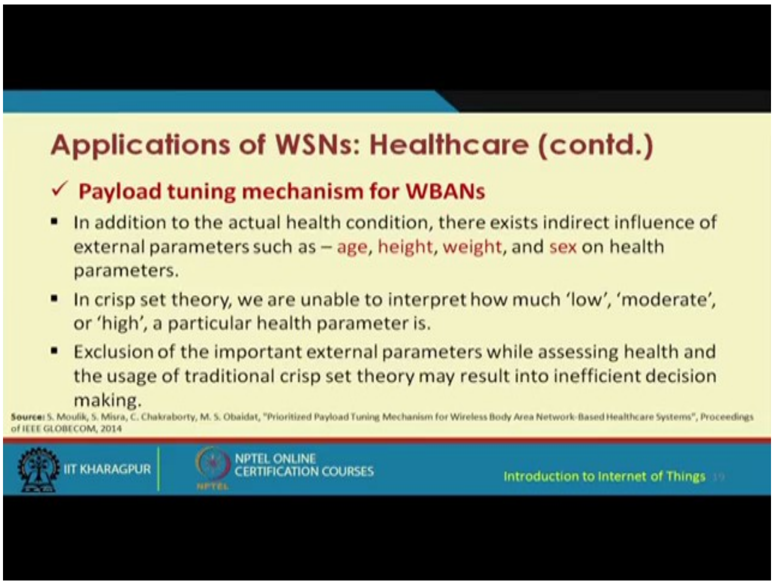
(Refer Slide Time: 22:18)



A very important and an attractive concept, is the concept of cloud assisted sensor network. Specifically in this particular paper we have talked about social choice considerations in cloud assisted wireless body area network architecture, for post disaster healthcare.

So, concept of social choice theory of economics has been used in order to in order to impart fairness to the different nodes in the network, in a cloud assistant w ban scenario. W ban is a sensor network a physiological monitoring sensor network. And all this data in a w ban cloud is going to go to the cloud end. The physiological data are going to go to the cloud end. Now the question is that, how do we ensure fairness among the different nodes in the network? For that we have used the social choice theory for improving it.

(Refer Slide Time: 23:21)

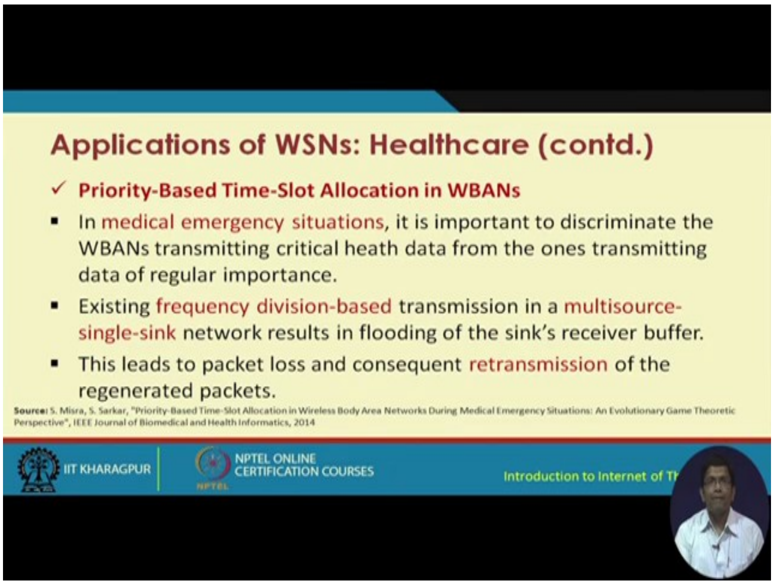


A very important work that was done again in the SWAN lab is the work that is sited over here. Prioritized payload tuning mechanism for wireless body area based healthcare system. This was published in IEEE globe com in 2014.

So, here basically we are using fuzzy logic, in order to improve the tuning of payload in a w ban. So, conditions you know in addition to healthcare conditions, there exist different other external parameters such as age height, weight, gender of the patient and so on. So, all these also have to be taken into consideration.

So, those are you know those can be you know, those can be modeled better with the help of fuzzy logic, fuzzy theory, fuzzy set theory, rather than using crisp set theory. And so, what we had we have done is using the fuzzy based concepts, we have you know taken all these things into consideration and have tried to improve the payload tuning of that particular network.

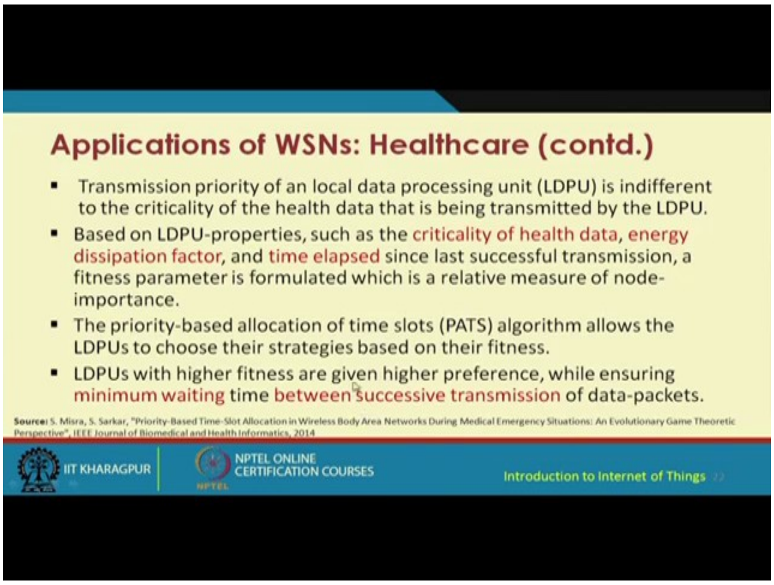
(Refer Slide Time: 24:46)



Another important thing that also has to be taken into consideration when we are talking about healthcare sensor networks is, that particularly during emergencies you know, what happens is let us see that after a post disaster environment, in a post disaster environment. So, so what happens if there are so many casualties? So, many victims and so on and so forth. So, and at the same time we have very limited medical resources be doctors, nurses, paramedics and so on. We have very limited.

So, they all have to be taken care of now if we are using sensor networks. You know deploying different sensors on the human body you know of the patients victims and so on and so forth, then what also has to be done is that, certain patients might require urgent attention, more urgent attention compared to certain other patients. So, that differentiation has to happen. Otherwise what might happen, is some patient who is at the point of maybe collapsing or dying he does not get helped whereas, somebody else who is not so critical get more attention. So, that fairness has to happen, that priority has to be given and this particular paper which was published in the IEEE JB JBHI IEEE journal of biomedical and health informatics basically talks about it.

(Refer Slide Time: 26:06)



So, we have in this particular lecture gone through different flavors of research works, and applications of sensor networks. We have seen that how sensor networks can be used for the broader context of internet of things, deployment of sensor networks to achieve the objectives of internet of things. This is what we have gone through in this particular lecture. We have seen that there a there are lot of applications and we have also seen that there are lots of research issues. Some of the research issues and their flavors is what you have been exposed to in this particular lecture.

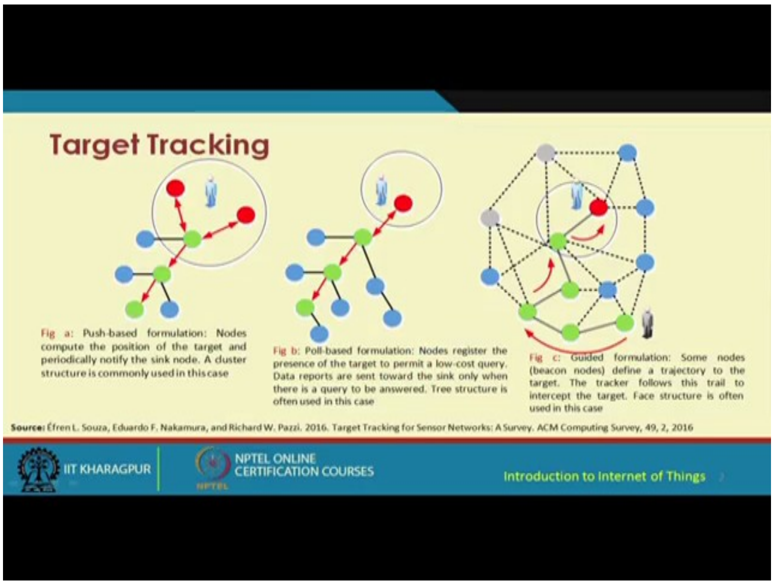
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 16
Sensor Networks- III

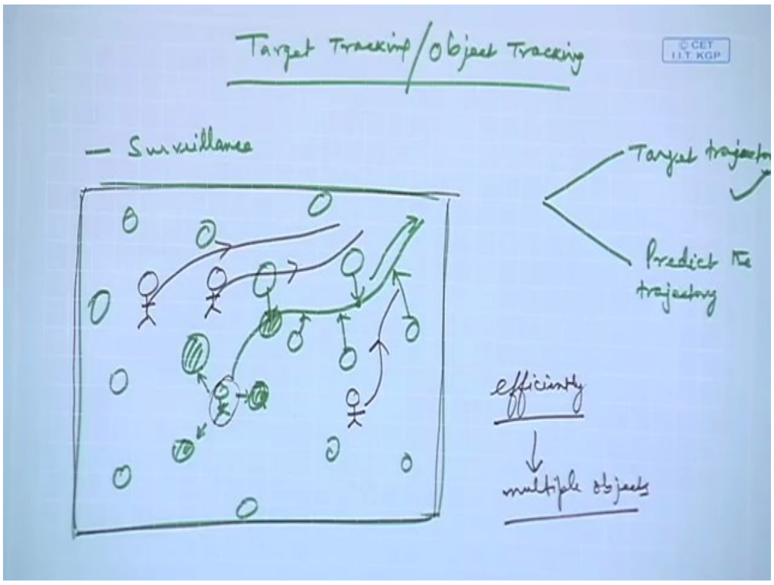
In this lecture, I am going to talk about some of the applications of sensor networks. So, sensor networks as I said in a previous lecture can be used for serving different applications agriculture, healthcare, space and so on and so forth. Many different types of applications are possible. So, we will take up few of the applications where sensor networks can be used and also keeping in mind some of the research works that we have done in our Swen lab at IIT Kharagpur and so that I can give you a little bit of more insight about you know house sensor networks can be used to address different problems of different application domains.

(Refer Slide Time: 01:14)



So, the first thing that I am going to talk about is the problem of target tracking. So, let me explain to you what the problem of target tracking is.

(Refer Slide Time: 01:24)



So, let us say target tracking, this is also known as object tracking. So, what happens is sensor networks are very much useful for surveillance applications, surveillance applications means that we can use different types of sensors, we can use cameras we can use a combination of all of these sensors cameras etcetera. To track a particular object a particular target maybe there is some suspicious activity that is going on maybe in a public place like a railway station or maybe in a crowded place some plaza or some market place or something like that.

So, sensor networks can be used for surveillance application. So, if there is already some sensor infrastructure that is deployed in a particular place. So, these sensors can be used to first of all identify that there is something wrong that is going on. So, you need to have appropriate sensors of course, and thereafter once it is detected that there is some suspicious activity that is going on then to track the trajectory of the target. So, this tracking can be of 2 forms. One is that as and when the target moves we keep on we keep on following the target using these different sensors we keep on sensing, where and how the target is moving.

So, that can be done in real time. The other possibility is that to predict the trajectory of the target. So, predicting the trajectory of the target. So, it can be of 2 types. Now what essentially I in either of these cases what essentially happens is we have different sensor nodes. These sensor nodes are placed all over in the terrain where monitoring has to be done. Now let us say that there is an object maybe a human that has been detected by these sensors these 3 sensors - this one, this one, and this one. So, the problem of trajectory sorry target tracking is that when this target moves the trajectory of that particular target has to be followed by these different sensors on the way. So, this is what this is this particular problem

The second problem is to predict the trajectory. So, prediction means that let us say that this object has been identified here in this particular position by these sensors it moves to the next location the next location is let us say here and then these sensors have detected this particular target like this it keeps on moving etcetera it comes to this particular position and then at this position we have to predict that what is going to be the next particular position or a sequence of positions of the target. So, we have to predict the next position or sequence of positions of this target. So, this is known as the problem of target tracking in sensor networks.

So, going back, we have different types of formulations of the problem of target tracking. One is the push based formulation, which is about that nodes computing the position of the target and periodically notifying the sink node. So, you know if this is a sensor network deployment, then you know this particular target this object has been identified by these sensors have been sensed, by these sensors, and then these sensors when this object moves it is going to compute the position of the target and then periodically at certain intervals of time notify to the sink node in this case, let us say that this is the sink node. So, it will be modified to this particular sink node.

So, sink node is the one which basically gets all the data from the other nodes the source nodes and the intermediate relay nodes. So, this is the sink node leadership. Now the other formulation is known as the poll based formulation which is shown in the second figure over here. So, in this particular formulation what we have is nodes registering the presence of the target to permit a low cost query. So, in other words the nodes are going to send out are going to poll all the other nodes to see if there is any object that is there in their locality; that means, within their sensing range. So, this is the poll based. So, it is going to periodically it is going to polled.

So, every node is going to be polled periodically. And the third is where there is a tracker that is used. So, tracker basically follows the trail of the target and intercepts the target.

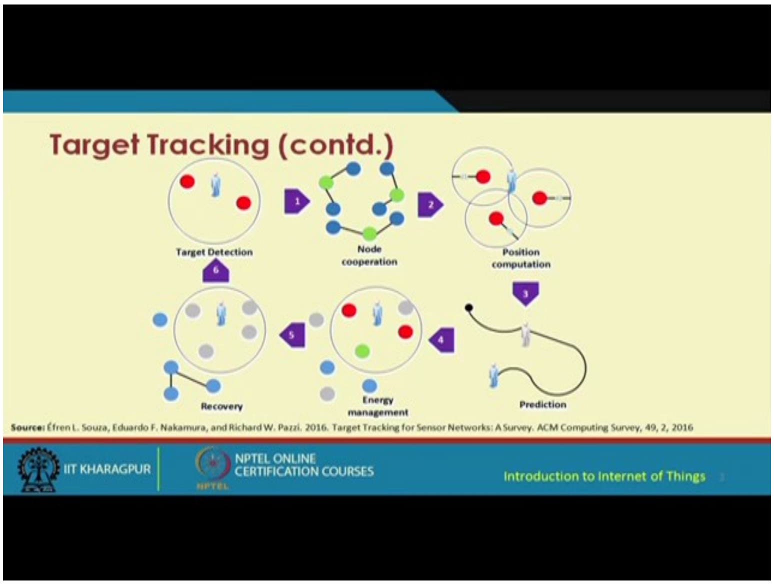
So, this is known as a guided formulation. So, we have 3 distinct types of formulation of the problem of target tracking in sensor networks. The next point that I would also like to highlight is that targeting is actually very important for sensor networks target tracking applications like surveillance etcetera are very attractive. And that is why there has been lot of research on target tracking or object tracking in sensor networks lot of research in our research group also we have done a lot of work on target tracking.

And so if you are interested you know you can visit my website and can get access to these papers research papers, but without getting into the research details let me also highlight another particular aspect.

So, let us say that we have going back we have a terrain like this. So, in this particular terrain in the previous example, I had considered that there is a single target or single object this human like this. There could be other objects as well and this is quite natural or this is quite typical in most of these applications because normally you are not going to track a single object normally it is going to be like there are multiple objects.

So, tracking multiple objects is it even more difficult problem, then single object tracking multi object tracking is even more a difficult problem than multi objective and that is quite obvious, I do not need to really elaborate am about why it is. So, so this multi object tracking one way is that individually you keep on tracking all the other objects as well, but that is not efficient. So, the problem is that how to efficiently how to track multiple objects in a terrain. So, now, let us move to the second slide where we have to understand how this target tracking basically functions.

(Refer Slide Time: 10:05)

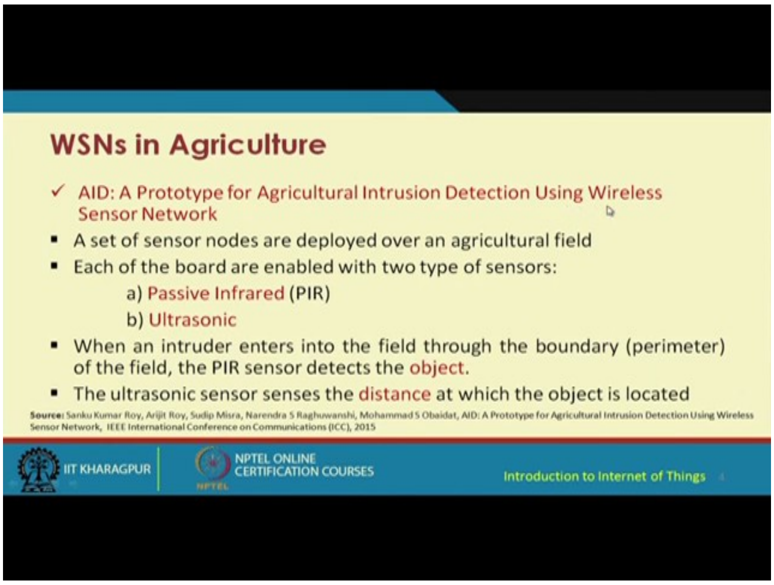


So, first let us say that you know we have different sensor nodes. This sensor nodes they have an object in their position in a close to them in their sensing range. Now what has to happen is the different nodes have to do lot of cooperation, for different purposes maybe for aggregating the data maybe for relaying the information that has been received about the tracking from other nodes, who have actually detected the presence of the target or who are following the target and so on and so forth. So, like this lot of different types of cooperation has to happen.

And then what happens is the position the exact position of the target has to be computed and this can be done using different ways, the position computation can be done in different ways for example, using the concept of trilateration using the concept of trilateration. If we know the positions of these 3 different sensor nodes we can easily compute the position of this particular object which is within the sensing range of these 3. Then after that there has to be some prediction that has to happen. So, prediction is about that if the object is at a particular location at this part at a certain instant of time, then at the later instant of time after delta t time, let us say where the object is going to be. So, let us say that the object is going to be over here.

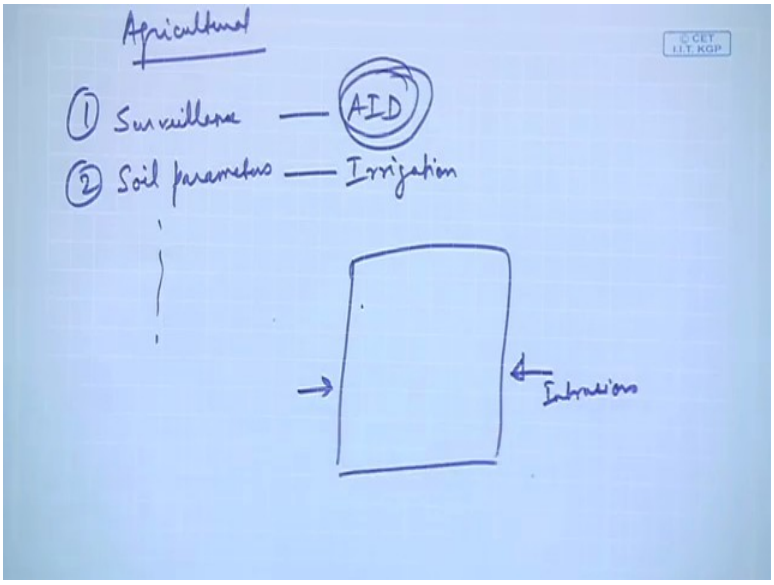
So, this particular position has to be predicted and thereafter issues such as energy management etcetera have to be taken care of because it should not happen that large number of sensors basically are activated and they all start sensing. So, what is the minimum number of sensors that are required in order to efficiently track the target first of all identify the position of the target and then track it. So, activating those sensor nodes, and those few sensor nodes and basically putting the other nodes to the sleep mode which is basically a low resource consuming low energy consuming mode of the sensor nodes.

(Refer Slide Time: 13:12)



So, this is another energy management problem that also has to be addressed alongside the problem of target tracking. So, I told you about the problem of target tracking like this sensor networks can be used for various other applications as well it has indeed been used in our research group apart from different other applications, we have particularly focused on the use of sensor networks in agriculture. So, in agriculture we have basically focused on number one, surveillance of agricultural field.

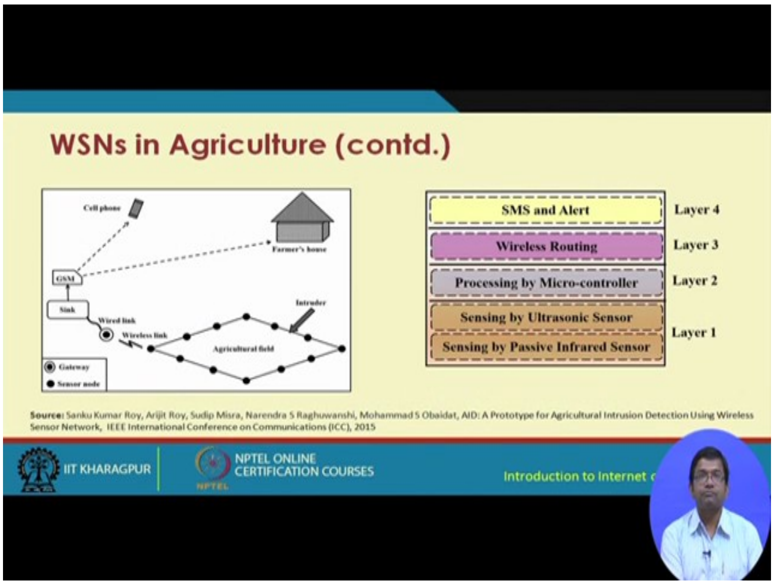
(Refer Slide Time: 13:41)



So, this is basically agriculture agricultural applications, we have also done some work on the use of sensor networks in the agricultural field for monitoring the soil parameters the soil parameters. So, for example, moisture content water level content and many other parameters for example, the mineral content of the soil phosphorus nitrogen and so on. So, these can also be sensed. So, soil moisture water level etc they can be used they can be sensed and that information can be used for irrigating irrigation of the field. So, if the soil moisture of the particular field has gone down we can irrigate the field and so on. So, like this actually there are different types of applications in surveillance we have worked on monitoring if a particular agricultural field is protected from intrusions, from intrusions from let us say cattle like you know cows goats etcetera because normally you know this is a very typical problem in a country like India where we have different cattles and different animals getting into the field damaging the crops and so on.

So, this kind of surveillance of the field is also very much required. So, so this kind of intrusions have to be detected and this can be done with the help of this technology the system that we have developed which is known as the aid. So, aid is basically a prototype for agricultural intrusion detection using wireless sensor networks, we are using 2 types of sensors the passive in infrared sensor the PIR sensor and the ultrasonic sensor. So, when an intruder basically enters the field through the boundary of the field the PIR sensor detects the object; that means, the intruder and the ultrasonic sensor basically senses the distance at which the object is located.

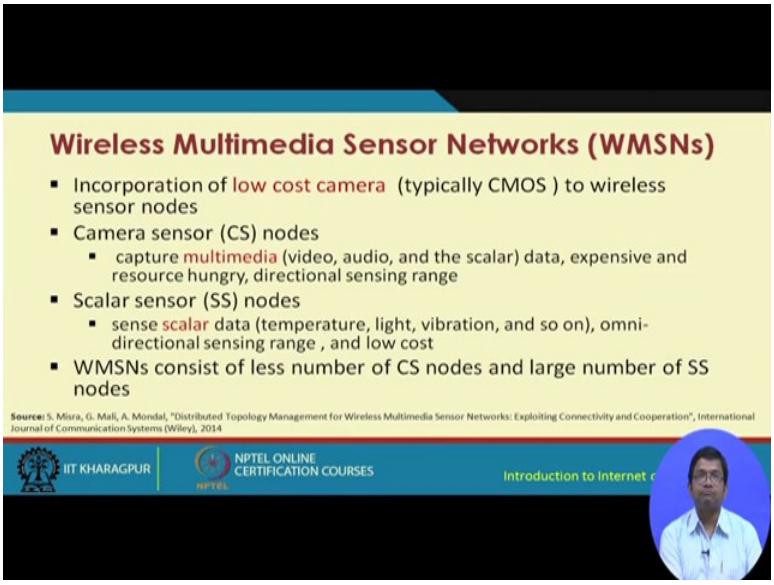
(Refer Slide Time: 16:23)



So, this is why these 2 different sensors are used there is sensor whether it has the entered or not and the ultrasonic sensor about how far the object is from that particular sensor. So, this is the schematic diagram. So, this is the agricultural field and an intruder getting in these different sensors are deployed in the perimeter or the boundary and the sensors will detect whether there is any intrusion that is going on or not and if it is going on then the farmer is going to be notified through cell phone or through other means at his home or wherever he is this is the layered architecture of this particular system that we have developed. So, first 2 layers are sensing using PIR sensor and the ultrasonic sensor.

And then processing by the microcontroller and then routing and finally, the application level SMS and alert messages will be sent to the farmer or any other stakeholder of that particular field.

(Refer Slide Time: 17:18)



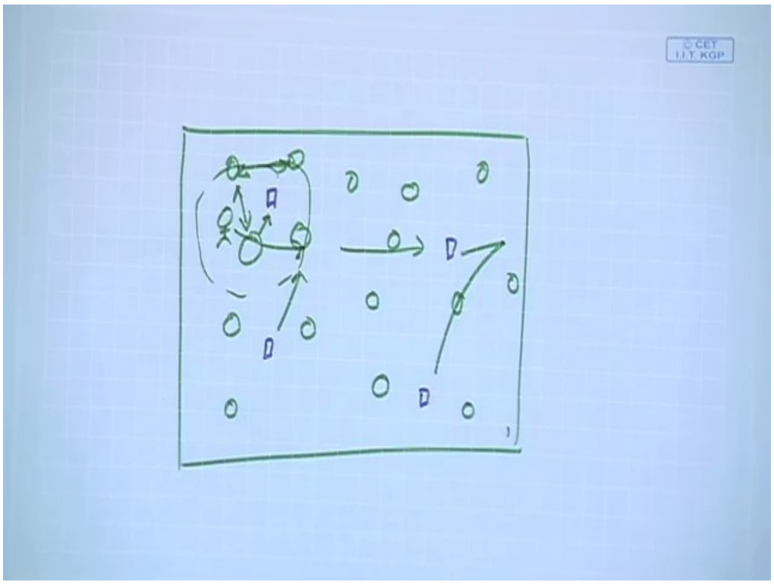
So, this is one application that we study the second definitely, the first is basically target tracking second is agriculture and in agriculture what we have just gone through is detecting intrusions in agricultural field, we could as I told you also that we could use sensors different types of sensors to measure to monitor the soil conditions with respect to moisture content water level content and so on and so forth. And correspondingly if let us say the soil parameters have gone down or is below a certain desired level then the field is going to be irrigated. Now let us look at something known as the multimedia sensor networks, multimedia sensor networks is very interesting in the media sensor networks.

We use multimedia devices apart from the regular sensors, these regular sensors like temperature sensor humidity sensor soil moisture sensor etcetera. These in multimedia sensor network technology in the community is known as scalar sensors, these sensors are known as scalar sensors. And in addition we have the camera sensors the camera sensors basically include like steel cameras in the small sized steel cameras or video cameras, which can be integrated along with these scalars scalar sensors to get a complete picture of what is going on in a particular area of interest.

So, typically what would happen is, we would be very much interested to get a complete picture and for getting complete picture ideally we should have cameras everywhere which would take still images and so on, but that basically is not only expensive having too many cameras deploying too many cameras in a field is not only expensive, but also that is not a very good solution from a network point of view, because if we have too many images of big size being taken then these big images big sized images are going to float all over in the network. And that is going to be not a very good solution for a resource constrained more specifically a bandwidth constrained environment like a sensor network.

So, the whole idea is can we use large number of these inexpensive cheap low cost sensor scalar sensors and have a fewer camera sensors, and together we can we have a better surveillance. So, how it is going to happen I will show you.

(Refer Slide Time: 20:09)



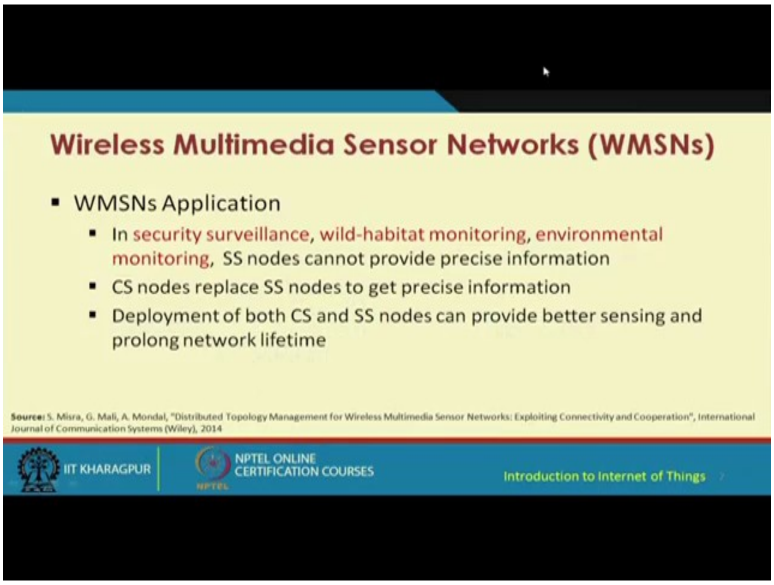
So, let us say that we have some terrain of interest. So, here we can have these different scale sensors all over which can be something like temperature sensor, humidity sensor, soil moisture sensor or whatever depending on the application that we are targeting and within this we would be using.

So, these are the green colored circles basically denote the scalar sensors and then we would be using only very few cameras. So, these cameras are expensive. So, we cannot use too many of them and also from a network perspective, as I said before we cannot use too many cameras. So, what is going to happen first these cameras these scalar cam sorry.

Ah these scalar sensors they are going to detect whether there is something going on or not, and thereafter if indeed there is something some suspicious activity or something going on and is detected by these scalar sensors through their collaborative sensing, then these sensors are going to activate the camera and this camera is then going to servile.

What exactly precisely is going on? Similarly the other cameras could also be activated depending on the position of the particular object, and how it is moving in the particular field. So, this is how the camera and scalar sensors putting together can work collaboratively you know wireless multimedia sensor network.

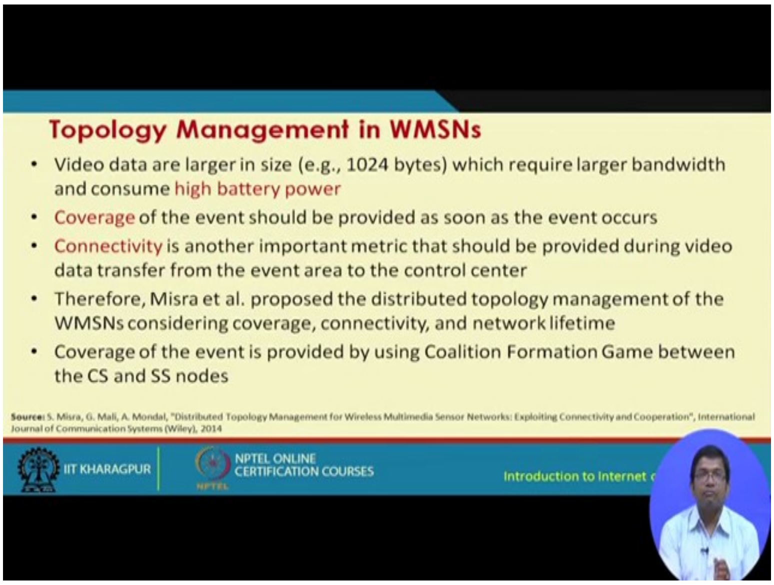
(Refer Slide Time: 21:59)



So, there are different applications of multimedia sensor networks surveillance is something that I was talking about right.

Now, but we can also have wild habitat monitoring like you know wild habitat monitoring means, like you can have these multimedia sensor networks to track precisely and monitor, how the different wild animals in their natural habitat are moving how what activities they are doing whether they are healthy or not and so on and So, forth environmental monitoring likewise and so on. So, like this actually there are different types of applications of multimedia sensor networks.

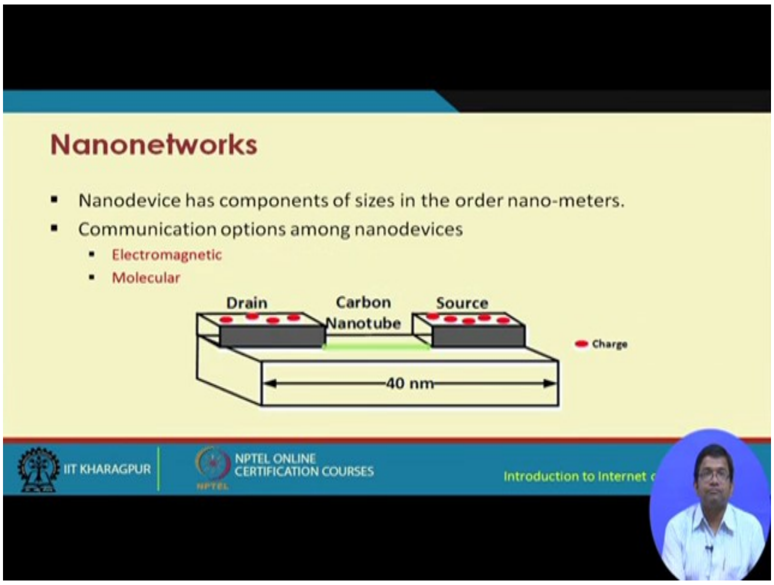
(Refer Slide Time: 22:42)



Topology management is another very interesting problem. In topology management what happens is that in the presence of these different sensors and in our particular case we are talking about multimedia sensors. In the presence of these multimedia sensor networks and these different sensors.

How the topology is going to be maintained over time, how these sensors are going to connect with one another over time, whether they are you know whether with respect to coverage means that with different sensors whether the entire region of interest is covered by at least one sensor or not. So, with respect to coverage and connectivity means that from every sensor whether there is connectivity to the sink node or not, so with respect to coverage and connectivity, whether at different instants of time the network is has a healthy topology. So, this is what is taking care of in the problem of topology management. And this is this is one paper that is there for you as a source which you can go through to understand the problem of topology management in sensor networks.

(Refer Slide Time: 24:07)

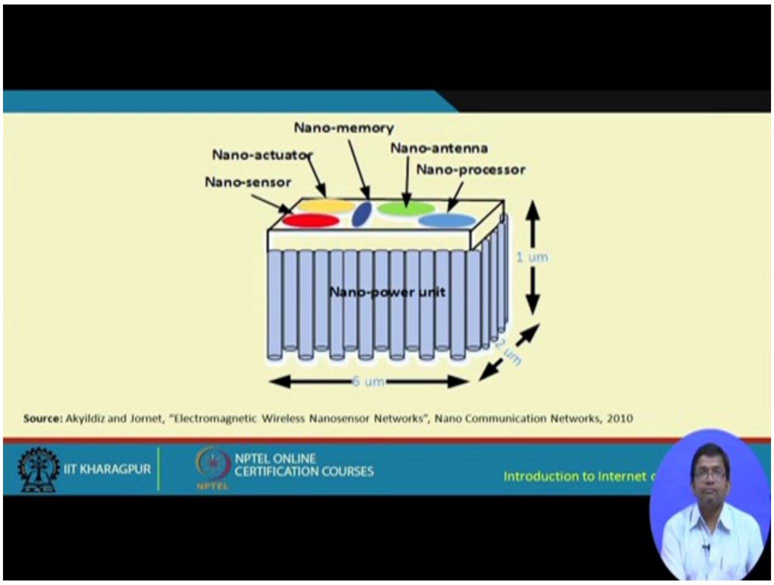


Another application and a technology that has evolved over time is nanonetworks. You must have already heard about lot of interest in nanostructures, nanomaterials, nanodevices and so on. And in including nanosensors, but you may not have heard about nanonetworks.

So, narrow networks more specifically nanosensor networks can be of 2 types. One is the electromagnetic nanosensor networks the other one is the bio nanosensor networks. So, the electromagnetic nanosensor networks basically as the name suggests the communication is through electromagnetic means and the other one is by nanosensor networks where basically it is biomolecules that help in communication in the human body or any human or you know any other natural being. So, nanodevices are used for as nodes in a nanonetwork on a nanosensor network. And every nanodevice has different components like one of which is the nanosensor, nanoactuator nanopower device and so on and so forth. So, this is how the communication takes place and between the source and source device and the sink there is going to be over the nanomedium such as carbon nanotubes there is going to be flow of charges that is going to take place and as you can see over here this is in the scale of few nanometers only. So, as you can understand one issue over here is to first design or fabricate nanosensors. Similarly it is also required to design and fabricate other nanodevices like nanoactuators nanopower sources and so on. And then the other problem is how we can put the nanosensors nanoactuators nanopower devices.

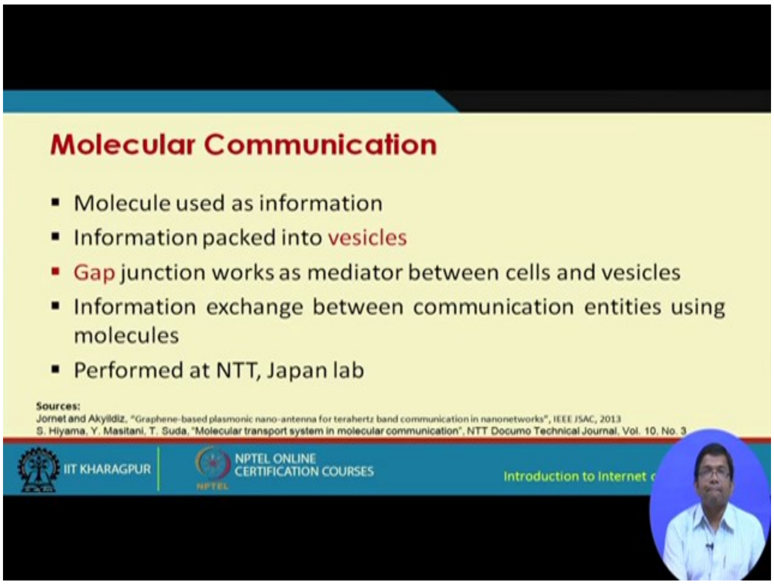
And the like together as a single device then nanonode and this nanonode also has a nanocommunication unit and this communication unit of one nanonode would help to connect with another nanonode with a similar kind of receiving device, and this communication in nanoelectromagnetic networks takes place in the terahertz band so this is typically this communication takes place in the period spent in nanonetworks.

(Refer Slide Time: 27:06)



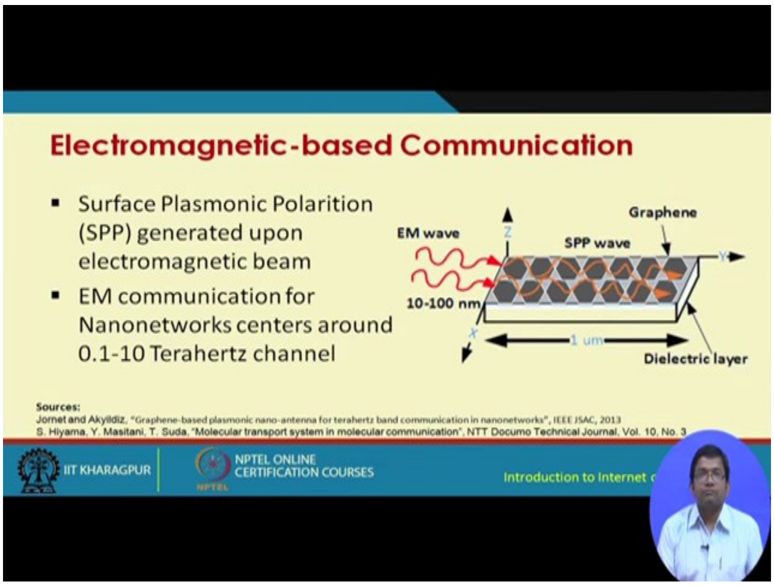
So, this is what I was telling you. This is a schematic of how a nanonode looks like. So, we have this nanopower unit, we have this nanosensors actuators nanomemory nanoprocessor nanoantennas for communication and so on and these corresponding dimensions are also mentioned over here. So, this is like 1 micrometer 2 micrometer 6 micrometers and so on. So, this is a very small kind of you know extremely small scale nanoscale node, which has to be fabricated not using conventional sensor node design mechanisms, but using a very sophisticated mechanism that is that takes help of nanofabrication units nanofab fabrication facilities.

(Refer Slide Time: 28:02)



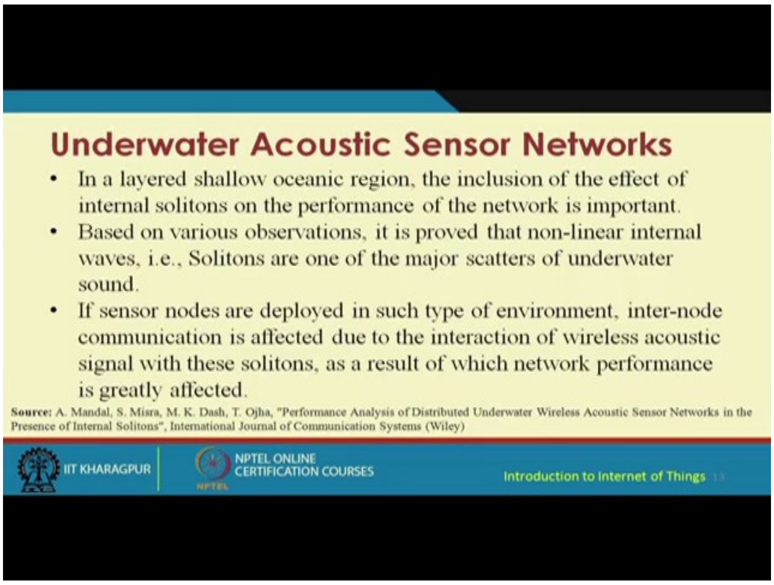
So, earlier I was talking about this nanoelectromagnetic communication. I also mentioned that bio nanonetworks are possible where the communication takes place through molecular exchange. So, information in this kind of a bio nanonetworks is basically packed into something known as the vesicles. And the gap junction works as a mediator between the cells and the vesicles and the information is exchanged between the communication entities using the molecules.

(Refer Slide Time: 28:37)



So, in the electromagnetic communication, something like this happens you know it is basically electromagnetic waves that basically are passed through some kind of nanomaterial like a grapheme or something like that and the information is transferred from one device to another device.

(Refer Slide Time: 29:11)

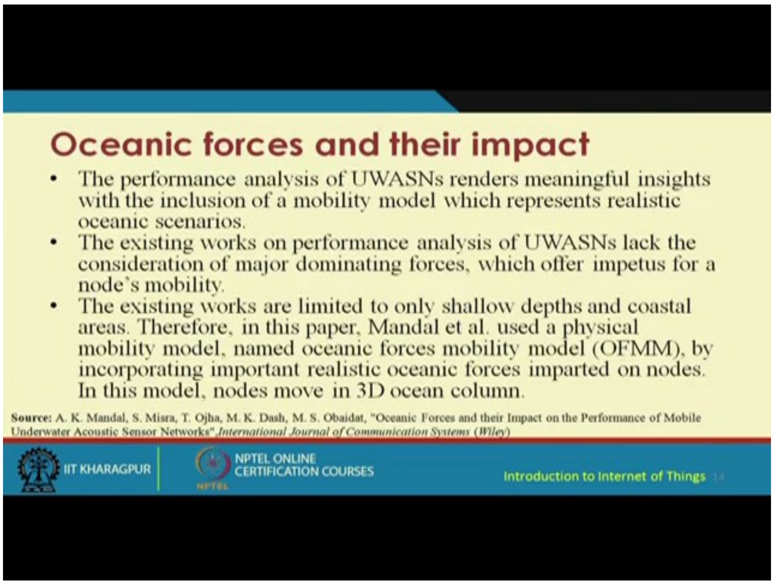


So, great magnetic communication for nanonetwork centers around the 0.1 to 10 terahertz general band. Then we have underwater acoustic sensor networks where basically it is about submerging conceptually submerging the sensor nodes that we are familiar with. So, far in the underwater domain submerging them let us say in the ocean and then having them sense and communicate to retrieve the information from under the surface of water. So, this conceptually is very simple and is similar to what happens in the terrestrial sensor network domain.

However in practice achieving and underwater sensor network fabricating a underwater sensor node and then connecting those nodes to communicate underwater to sense and communicate underwater is a hugely challenging task and there are so many different challenges that have to be taken into account. The first thing is the mobility the mobility because of waves and currents underwater the nodes wants to deploy them at a particular point, they are not going to maintain their position subsequently they are going to move all around.

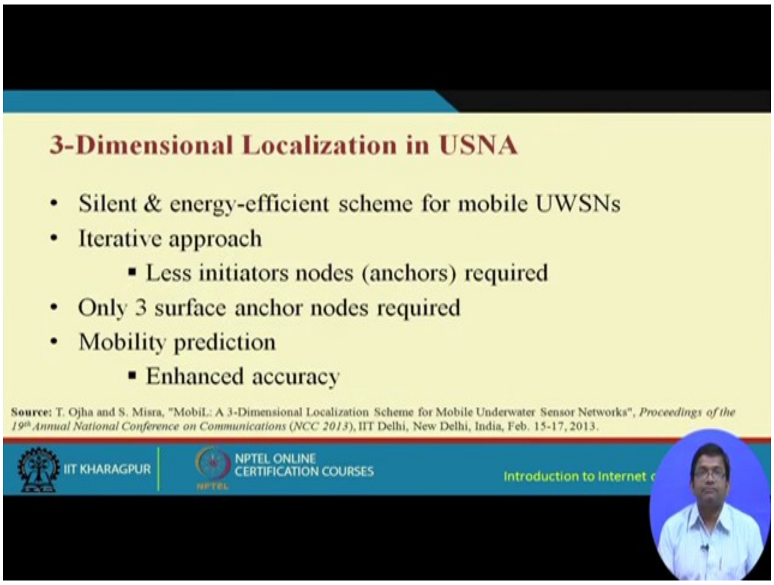
So, how do you maintain the topology of the network in the first place second thing is that with respect to communication when these different waves are hitting these different nodes, then they are also affecting the communication channel the channel are is also going to be affected. So, in such kind of noisy environment how the communication is going to take place also. In addition we have the medium which is typically like saline in nature where there is lot of temperature very in the ocean column where there is lot of pressure variation in that ocean column. So, all these also affect the communication channel and the performance of communication in such environments.

(Refer Slide Time: 31:28)



So, different oceanic forces also have impact on these networks, and that is the reason trying to simulate trying to simulate an underwater sensor network and it is environment is not very easy. So, one of the important concerns about simulation is that how the nodes in an underwater sensor network are going to move.

(Refer Slide Time: 33:09)

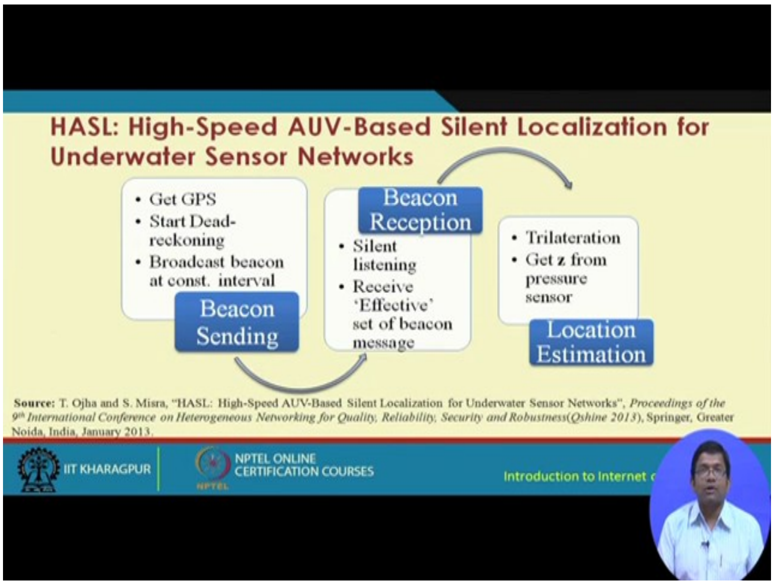


So, for that there is a mobility model that has been proposed, and this is known as the there are different mobility models one of which is the meandering current mobility model. So, this meandering current mobility model was proposed in a paper that was published in infocom conference several years back. And thereafter we have proposed in our group a mobility model which is known as the of mm oceanic forces model mobility model. And the characteristic of this particular of mm mobility model is that we have taken into account the realistic forces that are going to hit a particular node in a in an oceanic environment, whereas, the meandering current mobility model that do not take all these different forces.

That we have considered and this is how we have come up with this OFMM mobility model and this can be used to simulate the behavior of underwater sensor networks.

Localization is another problem localization problem is concerned about that how to localize the different nodes in the network and as I said that underwater environments highly dynamic highly chaotic, and localizing the position of the different nodes is highly challenging as well. And there are again lot of works that have been conducted on this particular problem. So, it is important to predict how the different nodes are going to move at different points of time accurately. So, accurately finding out that at a particular instant of time in the future where this node is going to be is a challenging problem of localization in underwater sensor networks.

(Refer Slide Time: 33:58)

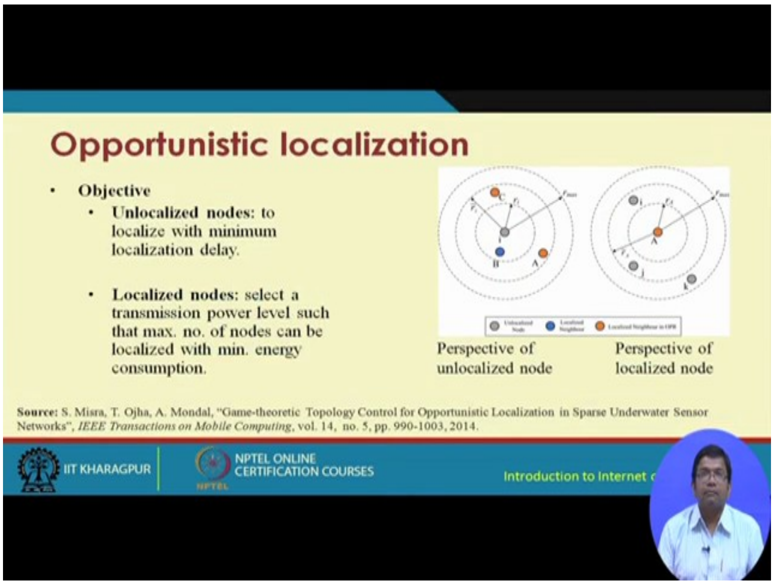


Protocols such as HASL which use beacon sending beacon reception and location estimation information to basically localize the nodes. So, these are these start with first getting some GPS coordinate from maybe a surface sink, and then start processes like dead recording and broadcast becoming sorry broadcasting beacons and so on, receiving the beacons getting an estimate of location estimation through processes such as trilateration and so on. And this has been explained in detail in this particular paper that is referenced over here at the bottom of the slide.

So, dead reckoning I was mentioning to you about dead reckoning digitally is I mean it is a technique of localization that is typically used in oceanic environments where it is hard to find specific references. So, in dead reckoning what is done is based on the distance from a particular target or a particular node whose position is known. It is estimated how another node how much far another node is located and at what angle.

So, based on this distance and angular information the position of the target at different instance of time in a marine environment is basically computed.

(Refer Slide Time: 35:35)

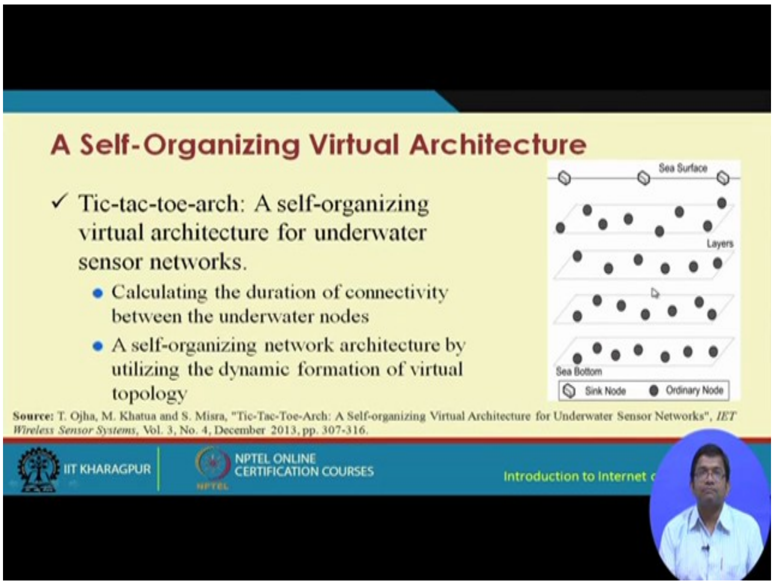


This is a proposal you know, this is a paper I triple e transactions on mobile computing it appeared. And here basically you know we are talking about how to efficiently localize with the help of advanced techniques such as game theory and so on.

So, here we have considered 2 types of nodes that are localized nodes and the localized nodes the problem is about based on the location information from the localized nodes how to get the location information of the unlocalized nodes. And for this what we do is we vary the communication range the transmission range of the of the of the nodes and by varying it the problem is to maximize the number of varying or increasing the increasing the transmission range, the problem is to maximize the number of nodes other nodes which can be put within that corresponding range the transmission range of a particular node. So, this is what is shown over here pictorially as you can see this particular node, you know it has an initial communication range like this the transmission range which can be increased further like these other circles.

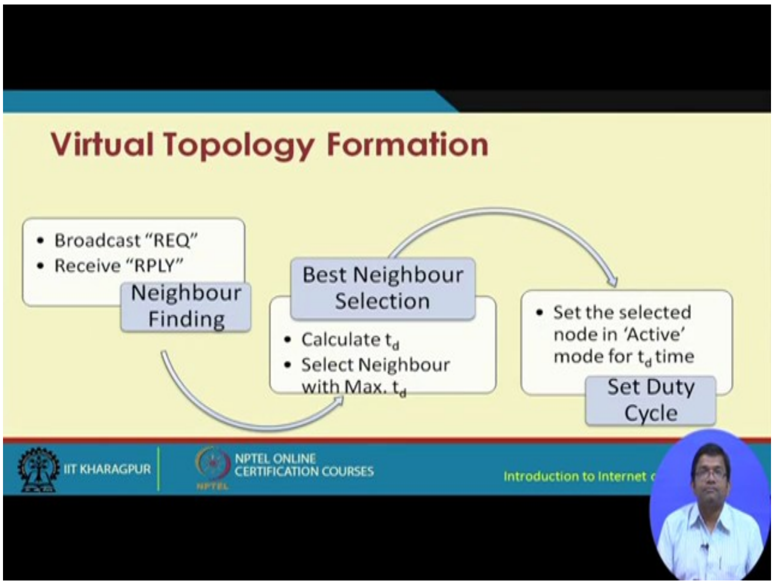
So, these are the 3 different ranges that are shown of the communication range or the transmission range of this particular node likewise for the other nodes also it is shown like this.

(Refer Slide Time: 37:09)



And the other problem is to maintain the topology maintain the architecture in underwater sensor networks for this there is this architecture, the tic tac toe architecture which is a self organizing virtual architecture has been proposed by us, in the iet wireless sensor systems journal and here. Basically what we do I am not going into the details of it because it is not required; I just wanted to give you a flavor of this particular problem because this is indeed very important and fundamental in the underwater sensor network community. So, it is required to calculate the duration of connectivity between the different the water nodes, and what we have done is we have to post this tic tac toe architecture, which is a self organizing network architecture by utilizing the dynamic formation of virtual topology.

(Refer Slide Time: 38:01)



So, here there are 3 steps neighbor finding neighbor selection and duty cycle and duty cycle management. So, duty cycle management means that based on the computation of how much the nodes are separated from each other the other nodes and their corresponding duty cycles are set or reset accordingly.

So, with this we come to an end of this particular lecture and what I have tried to do in this lecture, is to give you a feel of the different applications of sensor networks and the different research challenges in order to address those specific applications. And so we have also gone through some of the high level ideas about how to address what are the different solution approaches to address those problems.

Thank you.

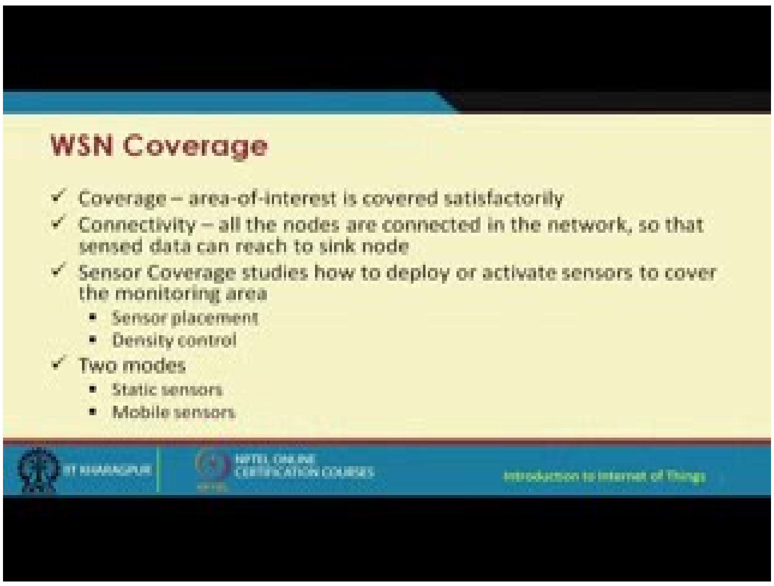
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 17
Sensor Networks- IV

In this lecture, we will try to understand a very important concept, which is the coverage the concept of coverage in sensor networks. Coverage is a very important problem because what is required is using sensors or sensor networks. We have to deploy the sensors or more specifically the sensor nodes in a particular terrain in such a way that no point or no none of the areas in that particular terrain left unsensed in that region. So, we have to deploy the sensors in such a way that none of the points in the terrain of interest which has to be that means, which has to be sensed which has to be surveilled, it should not happen that there is such a point which is not within the sensing range of if any sensor node.

So, this is basically known as the point coverage like this there are different other types of coverage called area coverage then we have barrier coverage and different other types of coverage which have been researched upon in the literature. So, we will try to understand this concept first.

(Refer Slide Time: 01:44)

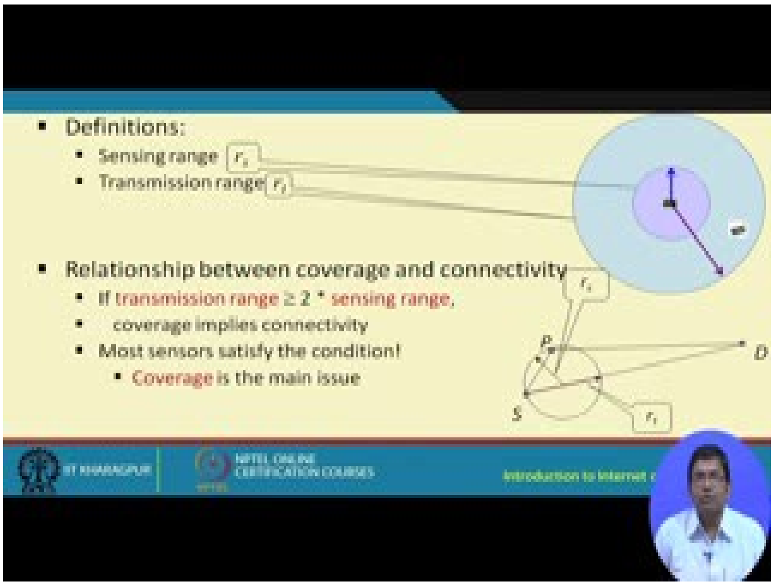


So, we have an area-of-interest and what is required is to ensure that that particular area of interest is covered fully covered is fully covered by at least one sensor. So, there has to each and every point in that particular area has to be within the sensing range of at least one sensor. So, there is an elite terminology which is called the connectivity and connectivity of the nodes is basically to ensure that all nodes that means, each and every node in the network from that point to the sink node there is some path that is available to transmit the sensed information. So, we have to ensure in the connectivity problem, we have to ensure that all the nodes are connected in the network. So that the sense data can be reach the sink node.

Sensor coverage basically studies how to deploy or activate sensors to cover the monitoring area. So, there are two variants of this particular problem, one is called the sensor placement problem and the other one is the density control. So, basically we have to ensure that how we are going to deploy the sensor nodes in a particular region of interest, so that the problem of coverage is addressed. So, how do we place the sensor nodes. And the second problem is that minimally how do we place, so that you know appropriate or desirable density is maintained in that particular area.

So, there are two modes of sensors one is the static sensor the other one is mobile sensor. The problem of coverage with static sensors basically is different from the problem of coverage with mobile sensors whereas, in static sensors we are primarily concerned about how to deploy the sensor, so that each and every point in the area is covered. In mobile sensors, we have to ensure that with respect to not only space as in static sensor, but also with respect to time that means spatio temporally that region of interest is covered with respect to space and time and that is in harder problem to solve.

(Refer Slide Time: 04:14)

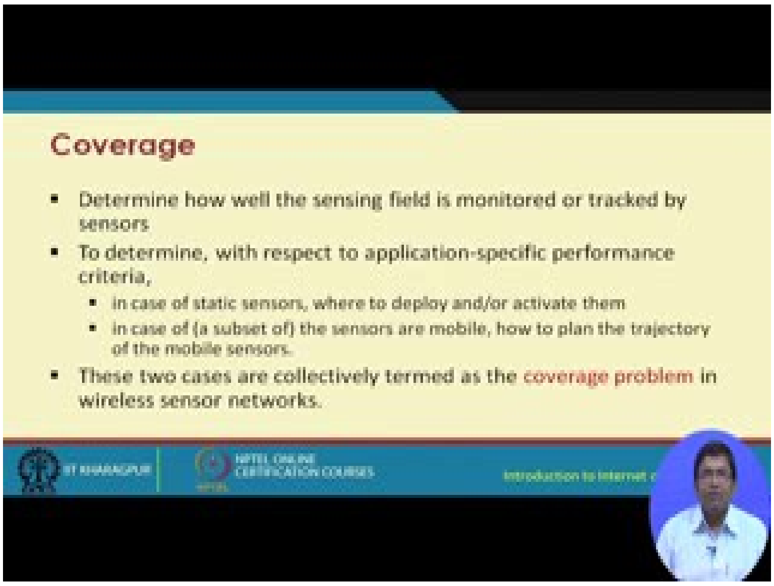


Now, let us try to understand few concepts. The first is the concept of sensing range and transmission range. So, when we have a node like this, it can sense up to a certain radius around it. So, it is typically like few meters or so. So, for a particular sensor node the sensing radius is the sphere around it, till which this particular node can sense. So, this is the sphere we are talking about or into D it is a circle. Now, there is this elite concept of transmission range, which is bit different. So, this transmission range or the communication range is concerned about how far this particular node can communicate. So, these are concentric circles and typically the sensing range is lesser than the communication range as shown in this particular figure.

But in literature on coverage, you will often find that the sensing range and the communication range are equated, they are considered to be equal. So, there is a relationship between the coverage and connectivity. If the transmission range is greater than or equal to twice the sensing range, it has been shown by researchers that the problem of coverage implies the problem of connectivity. In other words, we simply have to take care of coverage, and if we have ensured that coverage has been taken care of in a particular area then automatically connectivity is also taken care of.

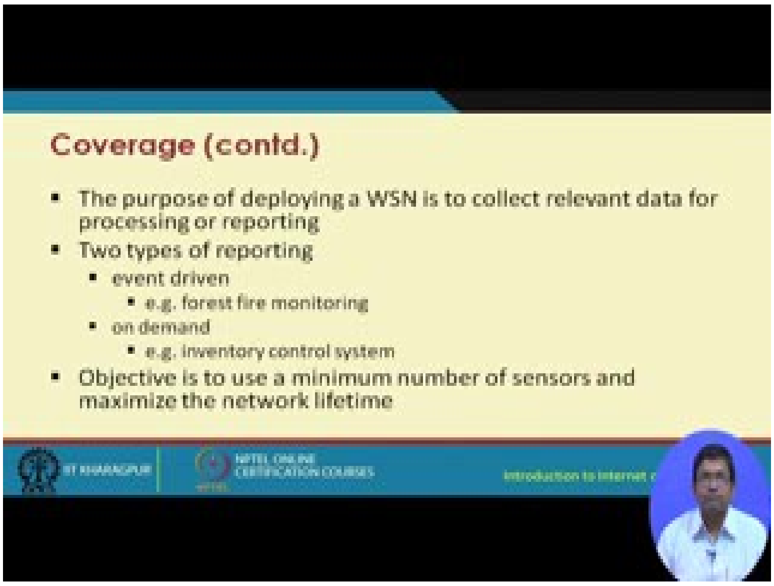
So, for ensuring coverage as well as connectivity, we have to ensure that for the particular sensor node, that we are considering. The transmission range is at least twice the sensing range. And typically for most of the available sensor nodes in the market most of the you know so this particular condition is taken care of. So, typically the the the transmission range or the communication range is quite much much bigger than the sensing range and that is why coverage becomes the main issue to be addressed.

(Refer Slide Time: 07:02)



So, the problem of coverage once again ensures that how well the sensing field is monitored or tracked by the different sensors. And to determine that with respect to certain application specific performance criteria in the case of static sensors where to deploy and or activate them; and in case of mobile sensors how to plan the trajectory of the sensors. So, these two cases are collectively termed as the coverage problem in wireless sensor networks. So, we have the coverage problem for static sensor networks concerned mostly about how to place the sensors or if they are already placed how to activate them, when and how to activate them, so this is the problem of coverage for static sensors the problem of coverage. For mobile sensors is basically, how to plan the trajectory of these mobile sensors, so that the region of interest is covered spatio temporaly.

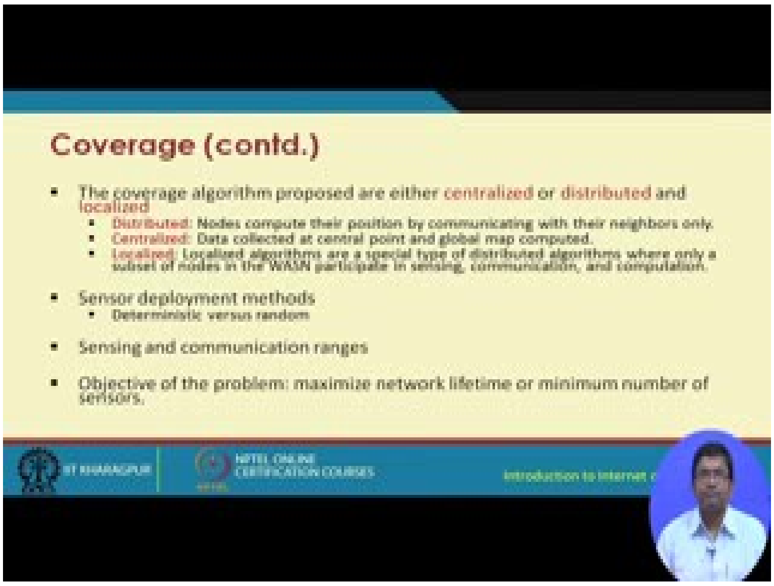
(Refer Slide Time: 08:02)



So, the purpose of deploying a sensor network is to collect relevant data for processing or reporting. And there are two types of reporting one is event driven, the other one is on demand. Event driven applications include like forest fire monitoring building fire monitoring and so on. So, whenever there is some kind of event. So, event means like fire taking place that is an event so then that particular event is reported. And on demand is basically that for example, if there is some information that is required then that you know some query is going to be sent for example, in inventory control systems. So, query is sent whenever there is some information that is required. So, the objective is to use a minimum number of sensors and maximize the network lifetime. And network lifetime is basically in plane and simple terms, it is about how long the network is going to survive how long the network is going to survive.

So, actually in the literature there are different definitions of network lifetime. So, one definition basically says that the time until which the first sensor node in the network dies. There is another definition which says, that the time until which the last sensor node in the network dies that means, it would runs out of battery power or it you know it stops functioning. And there are different other definitions as well, which are somewhere in between. So, the time until which let us say P percentage of sensors die in a particular network is the network lifetime.

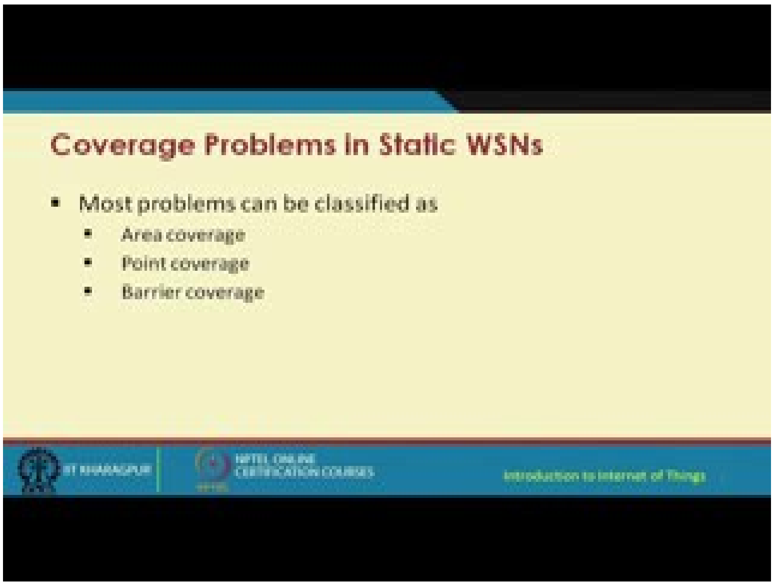
(Refer Slide Time: 09:50)



So, basically the objective is to use a minimum number of sensors and maximize the network lifetime. So, this coverage problem is such that it can be addressed either using centralized algorithms or using distributed algorithms or using localized algorithms. In distributed version of the problem the nodes basically compute their position by communicating with their neighbors only. Every node basically computes their position by communicating only with their neighbors. In the decentralized version the data are collected at the central point and global map is computed and in the localized version here. Basically, it is sort of like a distributed algorithm where only a subset of the nodes in the sensor network participate in sensing communication and computation. So, it says sort of like a variant of the distributed algorithm localized algorithm.

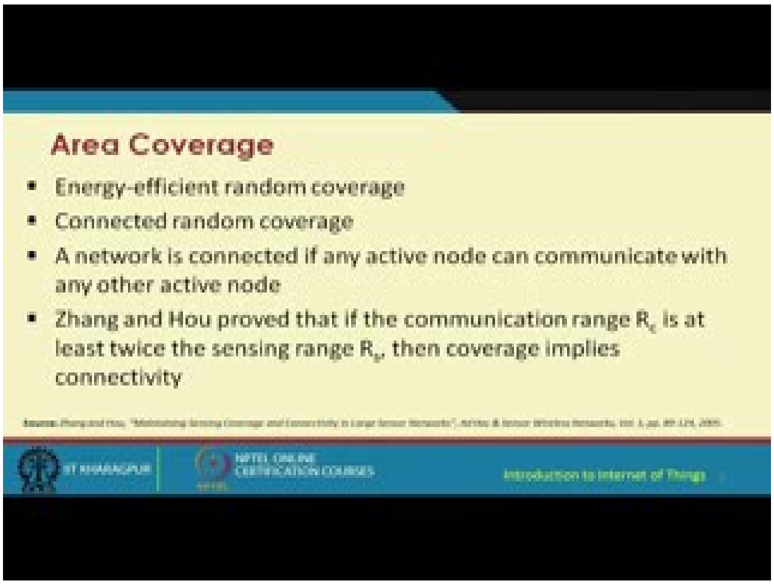
So, the different ways in which the sensors can be deployed for the purpose is basically either using deterministic means like you know, you preplan everything in a particular area. You know that xyz coordinates where each of these individual sensor nodes are going to be deployed and that is PD determined P calculated and the other one is basically random where using some random means like airborne means or whatever the sensors are thrown into that particular area.

(Refer Slide Time: 11:26)



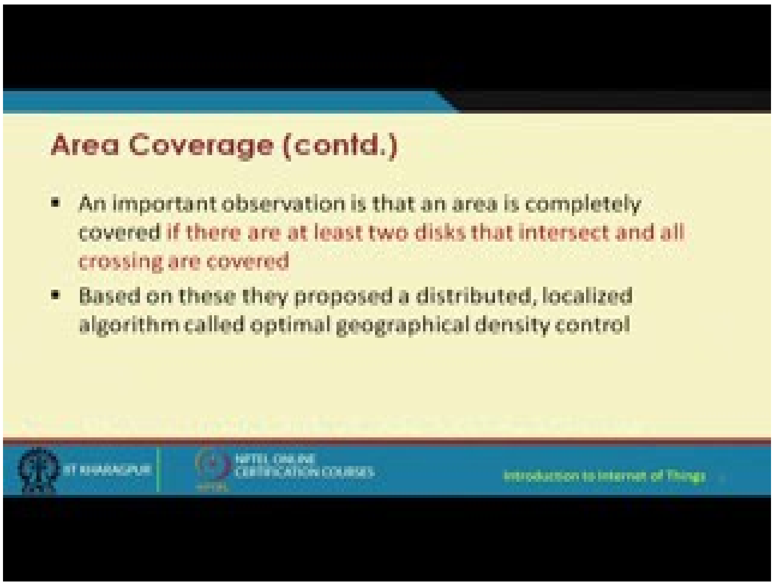
So, there are two types of ranges one is the sensing range and the other one is the communication range and the objective of the problem is to maximize the network lifetime or minimize the number of sensors. There are basically mostly three types of coverage that are quite common one is the area coverage the second is the point coverage and the third is the barrier coverage.

(Refer Slide Time: 11:40)



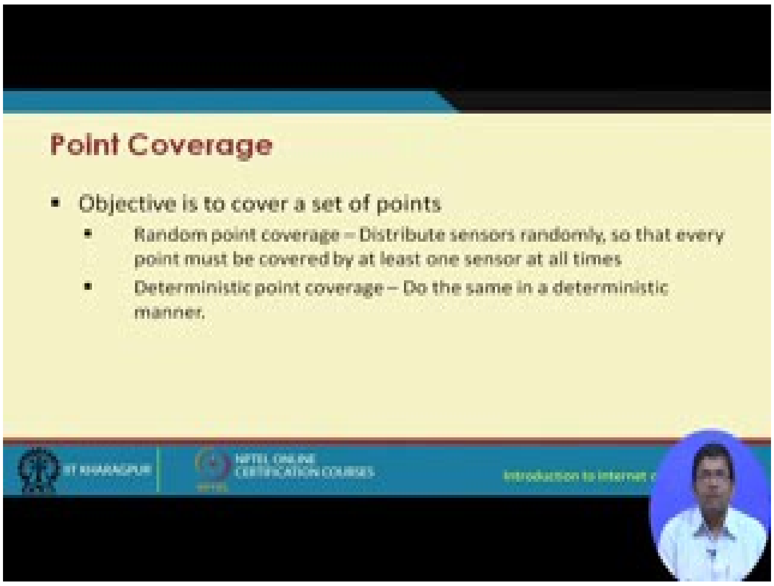
So, area coverage out of these three is the most common form of coverage in area coverage what has to be done is, we have to ensure that each and every point in a particular area is within the sensing range of at least one sensor node and that is that area covered. So, likewise actually that entire area is it consists of infinite number of points. So, we have to ensure that those infinite number of points each and every point in a particular area is within the sensing range of at least one sensor node. And on area coverage lot of work has been done by Zhang and Hou, who proved that, if the communication range is R_c and the sensing range is R_s then if the condition R_c greater than equal to twice of R_s holds then coverage implies connectivity. And this is something that I told at the outset as well of this lecture.

(Refer Slide Time: 12:35)



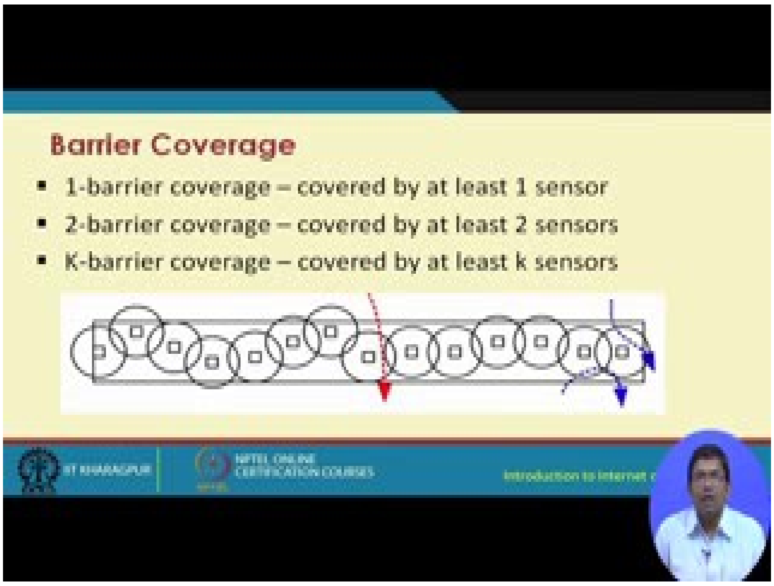
So, this is what has to be done. So, what basically has to be done is we have to ensure that two disks intersecting at crossings will be determent. And then, we have to ensure that likewise there are you know all these crossings that are formed out of the intersection of the different circles are covered. And this is what the algorithm one of the algorithms that was proposed by Zhang and Hou the OGDC algorithm that, we going to talk about shortly basically does and you know so without going into the details of it me also explain the concept of point coverage.

(Refer Slide Time: 13:03)



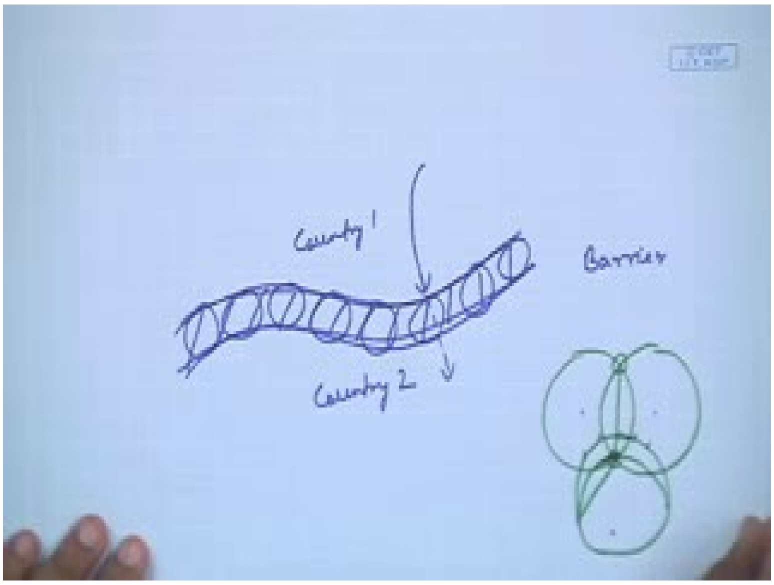
So, in point coverage, what we are doing is we are ensuring that if there is a set of points in a particular area to ensure that, those set of points are covered. Those set of points are covered in that particular area with minimal number of sensor nodes. So, it comes in two flavors one is the random point coverage and the other one is the deterministic point coverage in random point coverage it is required to distribute the sensors randomly. So, that every point must be covered by at least one sensor at all times and in deterministic point coverage we have to do essentially the same thing in a deterministic manner.

(Refer Slide Time: 13:53)



Then we have the barrier coverage in barrier coverage we have three variants one is the one barrier coverage the second is the two barrier coverage and the third is the K barrier coverage. So, here we have to ensure that a particular barrier is covered. So, let me just explain to you this particular concept.

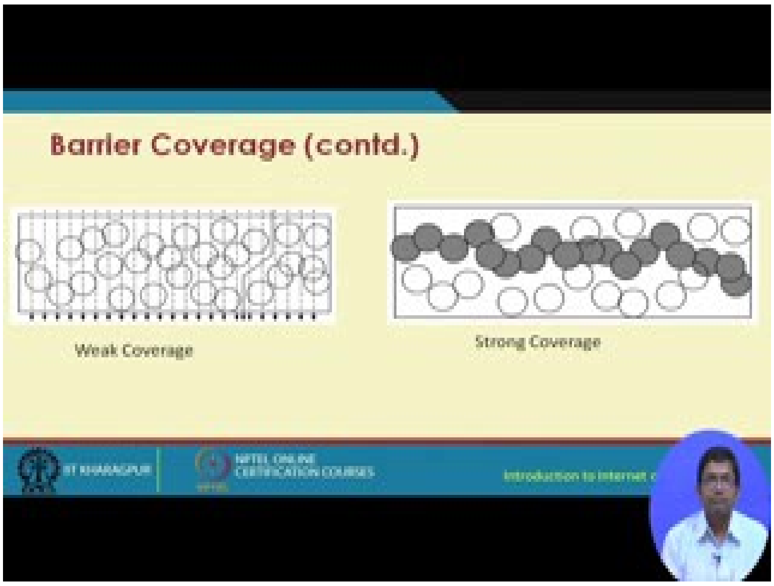
(Refer Slide Time: 14:23)



Let us say that we have two countries. Let us say that, we have two countries. And we have this is country 1 and this is country 2. So, this let us assume is the border between these two countries. So, the barrier coverage problem says that how we are going to place the sensor nodes and at what interval we are going to place them so that this particular barrier is covered. Covered means what that let us say that if there is some intruder that gets into from country 1, it tries to get into country 2, then it will get detected by at least one sensor node. So, this is the barrier coverage problem.

So, one barrier coverage ensures that at least one sensor node detects the intruder in what I just explained before. Two-barrier coverage ensures that, you know at least 2 sensors detect such an intrusion and k-barrier coverage ensures that at least k number of sensors k can be anything greater than 2, k number of sensors basically detect this particular intrusion.

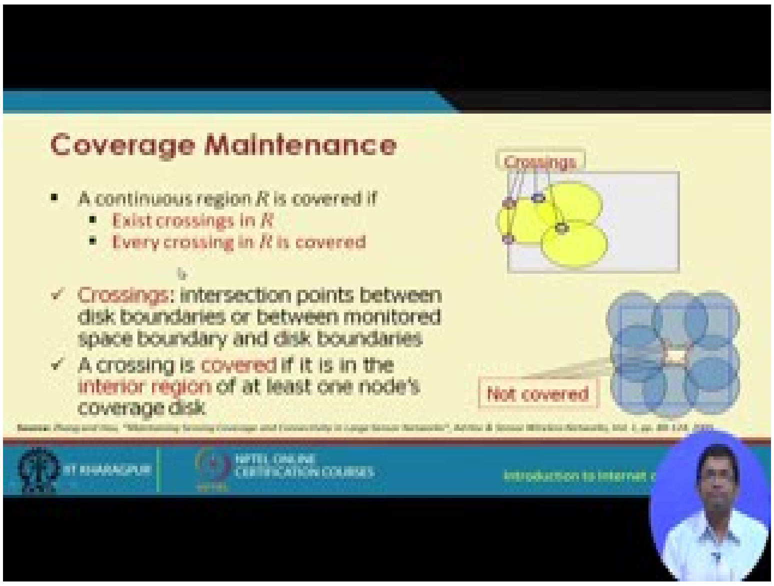
(Refer Slide Time: 16:02)



So, we have different types of barrier coverage the left hand figure shows thus case of weak coverage and the right hand side figure shows the case of strong coverage. So, as you can see over here in this scenario we have weak coverage because, you know one can find paths by which one can you know avoid getting sensed avoid getting sensed. On the other hand, if you look at over here, there is no such paths that can be found without getting detected without the intruder getting detected by one of these sensor nodes.

So, in this particular figure, what we see is that these empty circles basically denoting the nodes which are there, but and not active and these shaded circles denoting the nodes which are active. So, I hope that this point is clear over here. So, we have weak coverage and we have strong coverage. So, as you can see over here. So, a path like this by an intruder can avoid getting detected by add at least one sensor node; however, no such path can found out over here. So, this is the case of strong coverage and this is the case of weak coverage.

(Refer Slide Time: 17:42)

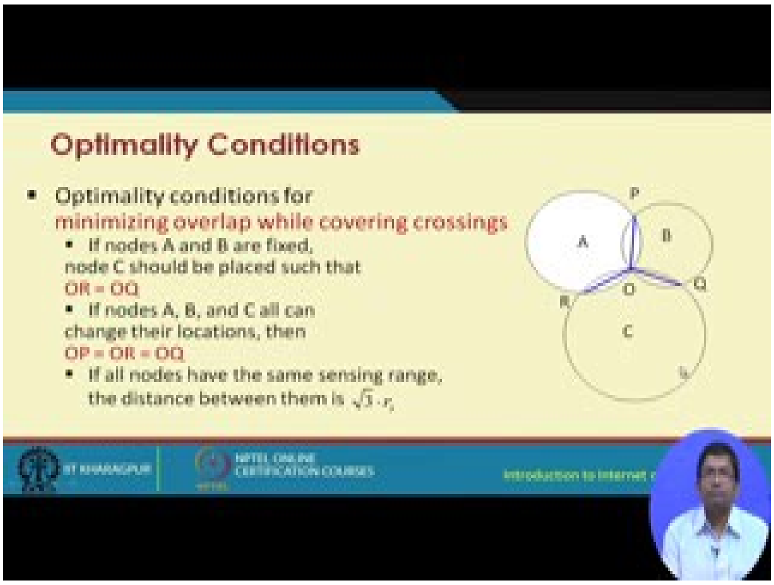


So, what is required is to continuously ensure that the coverage criterion is mate at all points of time and we have to activate the nodes in that manner. Maybe if it is a random deployment there could be some redundant nodes and it there is no point of two nodes doing the same thing at the same time, so maybe you put one node to the slip state the other one could be active and then this cycle can be changed over time. So, a region like this has to be covered. So, in this particular region, we have these different sensors we have these different sensors. So, we have to ensure that each and every point is covered.

So, how do we do that, we keep on placing this sensor nodes. And let us say that this is the sensing range of this node. This is the sensing range of the second node and this is the sensing range of the third node. So, these points that are shown over here are termed as the crossings these points and these points. What is the difference over here, these points are crossings between two circles, two or more circles, whereas these points are crossing between a circle and the boundary.

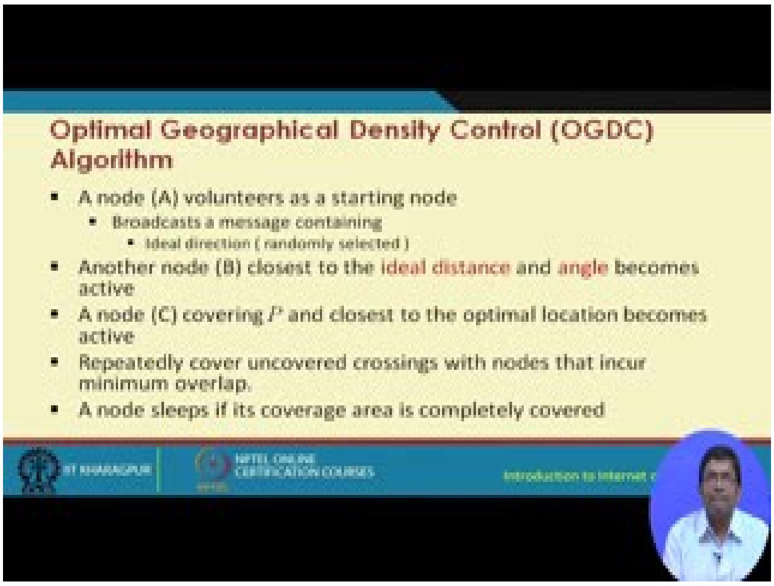
So, we have 1, 2, 3 and 4, 4-crossings. So, a continuous region R is covered if there exists crossings in R and every crossing in R is covered. So, we have to ensure that there are crossing in this particular region and we do see that there a crossings in this region and then we have to ensure that every crossing like this crossing, this crossing, this crossing each and every crossing again has to be covered. Like this crossing in this particular figure is not covered, this crossing is not covered, whereas this particular crossing which was formed out of these two circles is covered by this circle. So, this crossing is covered, whereas this crossing this crossing or these crossing these are not covered. So, this is what has to be ensured and this is shown in a different way in this particular diagram.

(Refer Slide Time: 20:14)



So, now let us look at a little bit of geometry. So, you know we have to come up with some optimality conditions. Optimality conditions for minimizing the overlap while covering the crossings and that way we have to ensure that minimum number of sensor nodes are utilized in order to cover covered the crossings. So, if nodes A and B are fixed like in this particular figure. So, if nodes A and B are fixed, we have to place a nodes C we have to place a node C in such a way that OR = OQ. So, A, B we have to place C in such a way that OR = OQ. If nodes A, B and C all can change their locations then and that is quite possible. So, if nodes A, B and C all can change their locations then we can even have OP = OR = OQ. So, OP = OR = OQ that can be very well done and if all nodes have the same sensing range that means, the circles have the same radius.

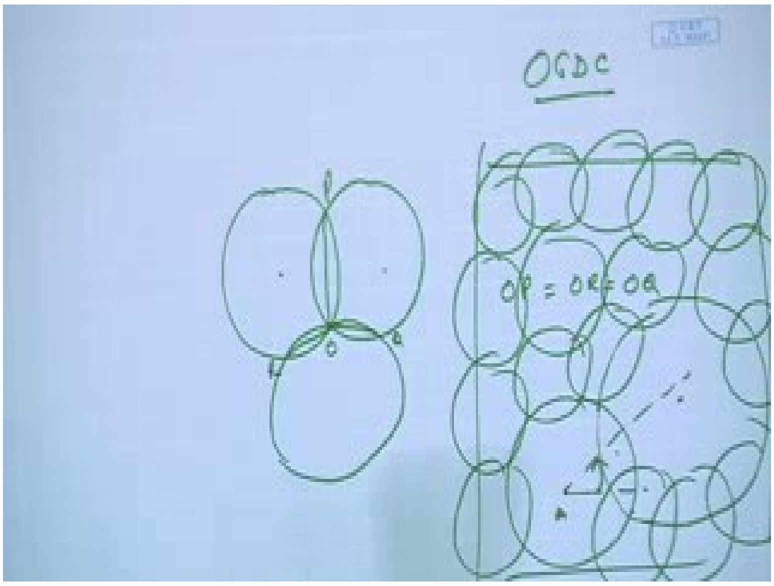
(Refer Slide Time: 21:49)



Then the distance between them is square root of three times R_s the sensing range. So, a node in the OGDC algorithm what happened is first a node volunteers as a starting node and it starts broadcasting a message containing the ideal direction which is randomly selected. If another node B which is closest to the ideal distance and angle becomes active a node C covering P and closest to the optimal location becomes active and repeatedly, it is required to cover the crossings uncovered crossings with notes that incur minimum overlap.

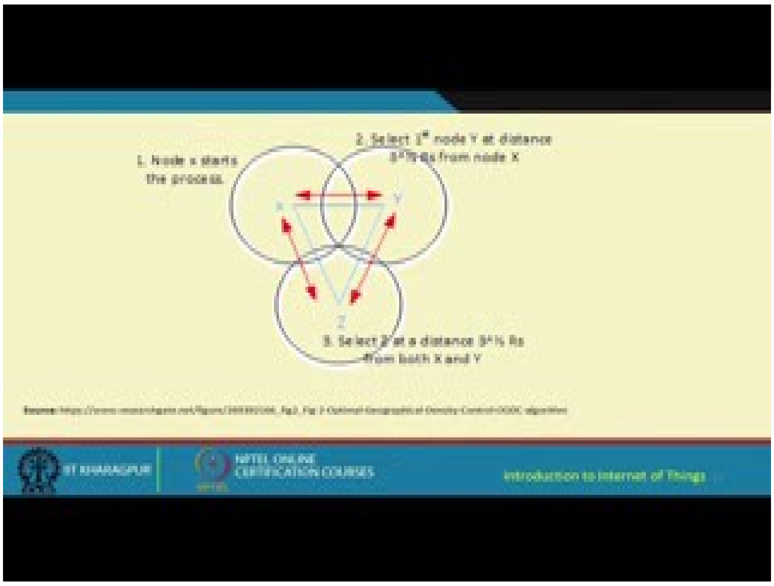
So, a node sleeps if its coverage area is completely covered. So, let me show you this particular concept it to really. So, what we have one node we have another node both have the same radius. So, and these are the crossings this is one crossing and this is another crossing. So, the point that was made earlier was that we have to place this another node in such a way sorry this is not correct. So, we have to place it in this way not this in such a way that this is again let me do it once again.

(Refer Slide Time: 23:26)



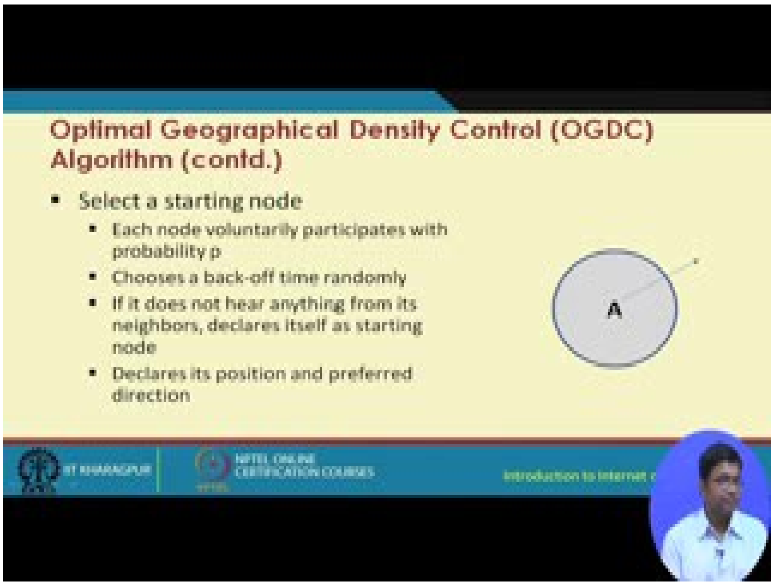
So, let us say that we have two different nodes and we have to place third node in such a way that this one, this one and this one at the same. So, in this diagram actually it is not very precise. So, we have to do it in such a way OP, OR, OQ. So, OP equal to OR equal to OQ. So, what happens is that one node what it will do it will at a particular angle it will start broadcasting a message. Then another node which is in this particular direction and in this angle that means in this particular direction and it is closest to this particular node that node has to be placed in this manner. And like this if you consider this whole area you keep on doing the same thing and ensure that the crossings are also covered. So, what is going to happen like this you know. So, what we are going to get is all the crossings getting covered like this with a minimum number of sensor nodes. So, this is how the OGDC algorithm works.

(Refer Slide Time: 25:06)



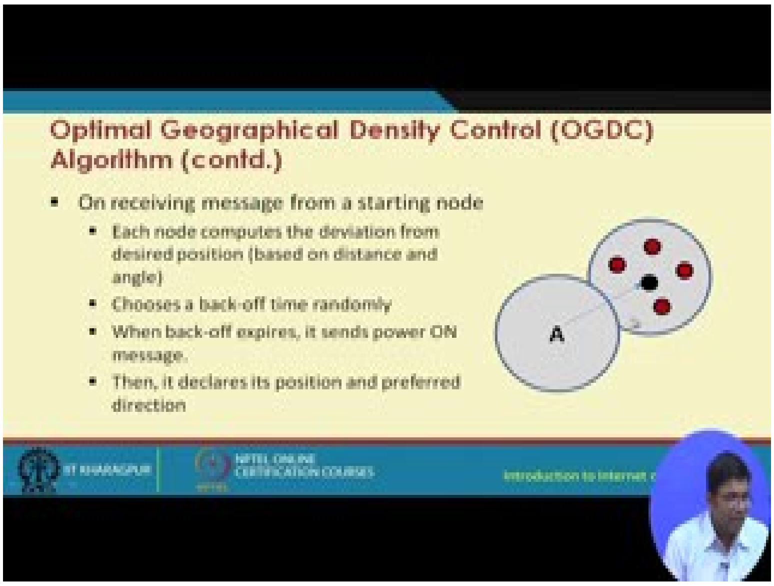
So, node x starts the process it selects the first node Y at a distance some distance from this particular node. So, this distance is what square root of three times R_s square root of 3 times R_s it will choose this node then this node Z is selected at a distance square root of 3 times R_s from both X and Y. So, from both X and Y this has to be put square root of R_s distance square root of 3 times R_s distance. So, this is square root of 3 times R_s this is square root of 3 times R_s and this is square root of 3 times R_s.

(Refer Slide Time: 25:57)



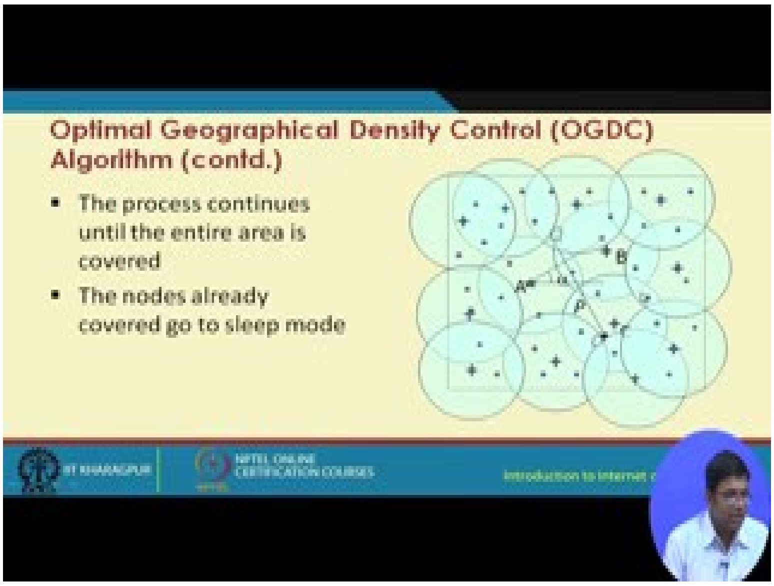
So, let us go through this algorithm once again each node voluntarily participates with probability P in this case this node A participates with probability P. It chooses a back of time randomly. If it does not hear anything from its neighbors, it declares itself as a starting node, it declares its position and preferred direction. So, in this case it declares its current position and the direction alpha.

(Refer Slide Time: 26:26)



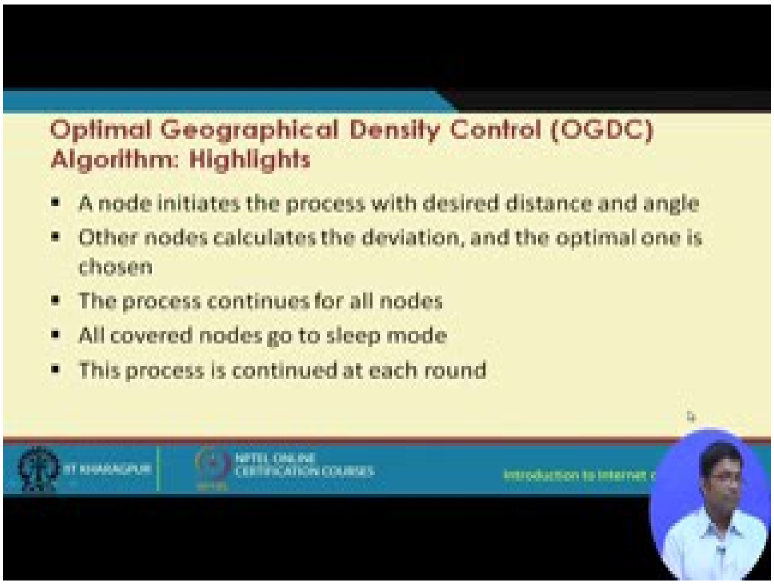
On receiving messages from the starting node, each node computes the deviation from the desired position. It chooses a back off time randomly when the back off time expires it sense the power on message then it declares its position and the preferred direction. The process continues until the entire area is covered as in this particular figure.

(Refer Slide Time: 26:44)



So, this node it started at a particular angle closest to it, another node is chosen this particular node basically will be selected, these crossings are formed another node C is chosen. So, square root of 3 times R_s square root of 3 times R_s square root of 3 times R_s and then we have further crossings. So, you keep on placing the other nodes so that all the crossings are covered.

(Refer Slide Time: 27:20)



So, some highlights again. A node initiates the process with the desired distance and angle other nodes calculate the deviation and the optimal one is chosen the process continues for all nodes and all cover nodes go to the sleep mode, this process is continued for each round.

So, with this we come to an end of the lecture on coverage and coverage is one of the very important issues in sensor networks, because it ensures that each and every point in the region of interest is covered or a set of points is covered. And if it is each and every point is covered that is that area coverage problem and if it is a set of points that have to be covered then it is a point coverage problem. And it is this area coverage problem that is the most common and most popular form of coverage problem that is addressed in the literature, lot of research works have been gone into it.

Similarly, there is the third type of coverage which is the barrier coverage. Here again you know this is also very important because sensor networks are often used for unmans surveillance in you know bordering areas between two countries and that is where you know this particular rectangular strip or a strip of region between two countries has to be monitored using sensors. So, the coverage while ensuring that minimum number of sensor nodes are used at and has to be placed in that particular border is a very important problem and is known as the problem of barrier coverage. And we have finally, discussed the OGDC algorithm which is one of the important area coverage algorithms that have been proposed and it is quite popularly used in the sensor networks community.

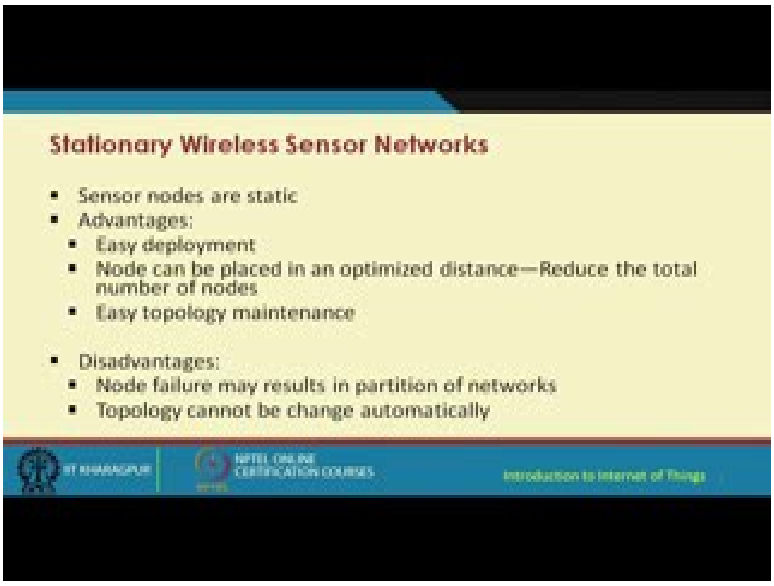
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 18
Sensor Networks- V

So finally, we come to the last lecture of the series on sensor networks. So, here basically I would like to highlight some of the concepts of mobility. So, more specifically I would like to explain the concept of mobile sensor networks.

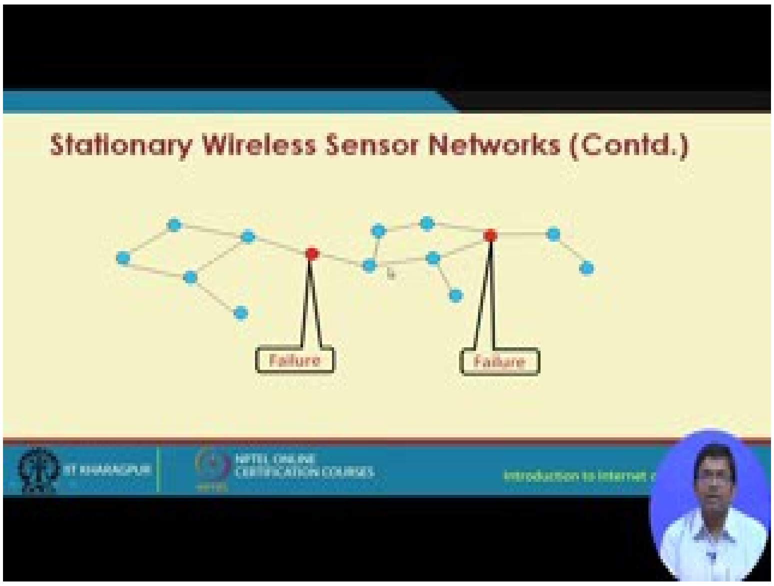
(Refer Slide Time: 00:39)



So, let us first look at the static variant sometimes it is also known as the stationary sensor network. So, here basically as the name suggests the nodes are stationary or static. So, they do not move; once deployed they will maintain their positions at later instants of time as well. So, the advantage is basically it is easier to deploy sensor nodes in a stationary sensor network, the nodes can be placed in an optimized manner, then it there maintenance of the topology is easier and so on and so forth.

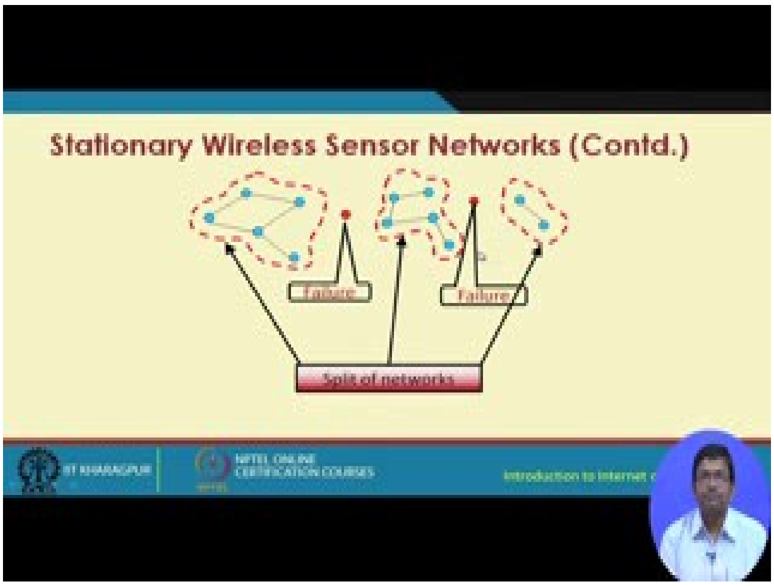
The disadvantage is that if there is a failure in the static sensor network then it is likely that that point of failure can partition the network into two or more fragments, two or more partitions. So, it is quite likely that there can happen. And particularly if it is a critical node, so in that node failing means that you know it is likely to partition the network. So, one part of the network will not be able to talk with another part of the network. And topology cannot be changed automatically is also another disadvantage of a stationary sensor network.

(Refer Slide Time: 01:54)



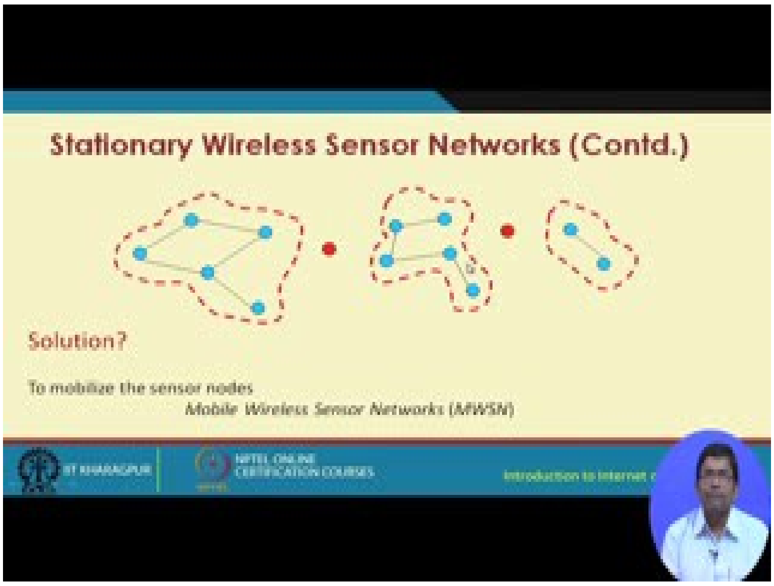
So, let us consider a state stationary sensor network as shown in this particular slide. So, we have these red colored nodes as points of failure because if this particular node dies for one reason or other for example, the hardware in it has failed it has stopped functioning or maybe that you know the battery that was powering that particular node it is exhausted.

(Refer Slide Time: 02:50)



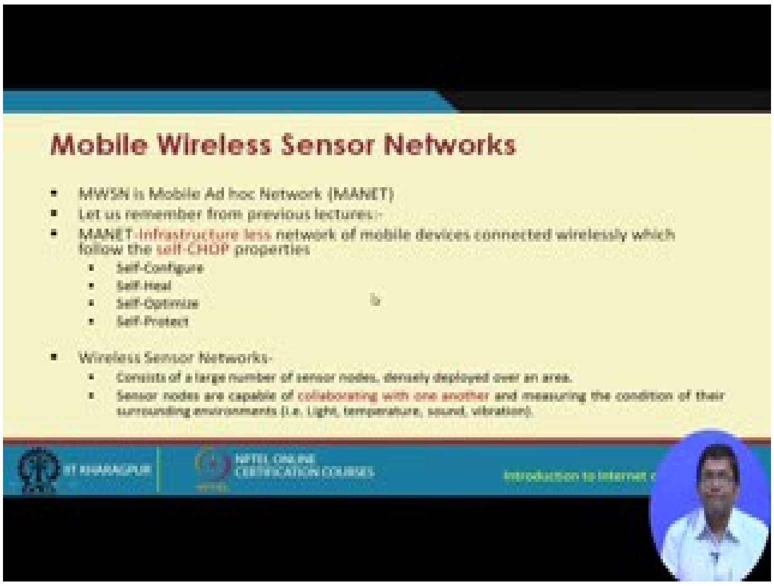
So, what is going to happen? As a consequence these nodes are positioned in such a way that these network partitions will be created. So, three network partitions would be created if these two nodes fail. So, as a consequence what is going to happen is that we would have three partitions or three split ups of the network due to these points of failure.

(Refer Slide Time: 03:08)



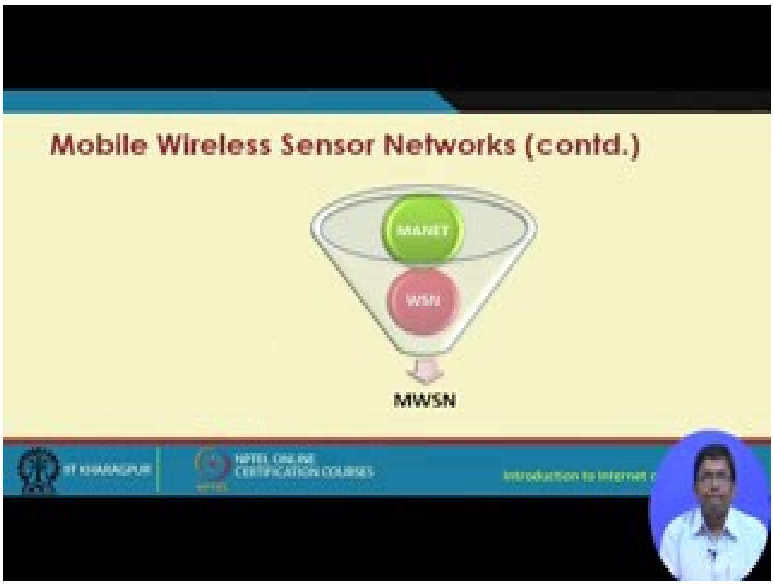
So, what is the solution? So, one way to address this is to have some node maybe some external node, external to this particular network or among these if we can have one of these nodes mobile nodes which can move. Then what it can do is one of these nodes let us say this particular node can come and take the position of these red colored node and this network will be joined these partitions will be joined. Likewise maybe this node can come over here and likewise these two partitions can be joined. So, these three partitions can be joined if some of these nodes one of these nodes is mobile.

(Refer Slide Time: 03:58)



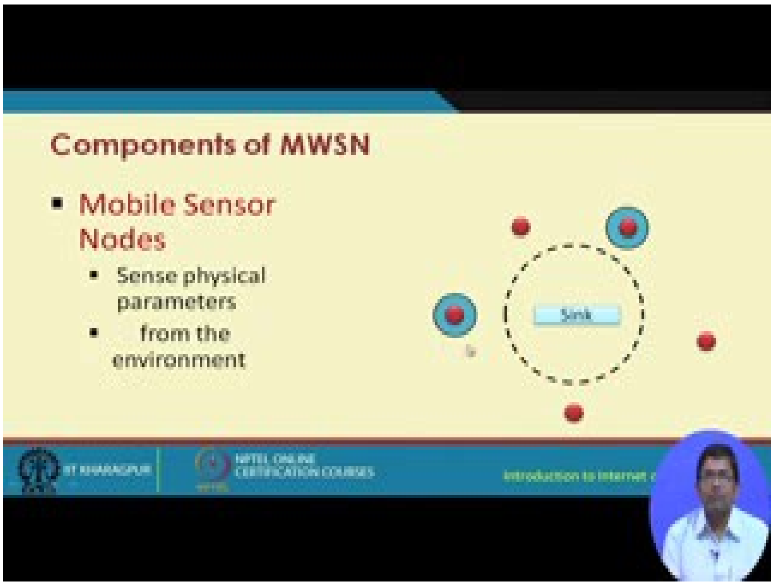
So, we have a mobile wireless sensor network which is basically a sensor network, a stationary sensor network conceptually integrated with a mobile ad hoc network. So, this is not physically integrated conceptually. So, take the features of mobile ad hoc networks, take the few features of stationary sensor networks put them together and then you get the mobile wireless sensor networks. And as we know that MANETs mobile ad hoc networks are infrastructure less and infrastructure less. So, basically what happens is the topology basically becomes dynamic dynamically changing topologies that basically invites following properties like self configuring, self healing, self optimizing, self protecting and so on. So, these have to be there these are infrastructure less networks these do not have any centralized entity which will control the network management functions. So, this self job properties basically are going to take effect.

(Refer Slide Time: 05:10)



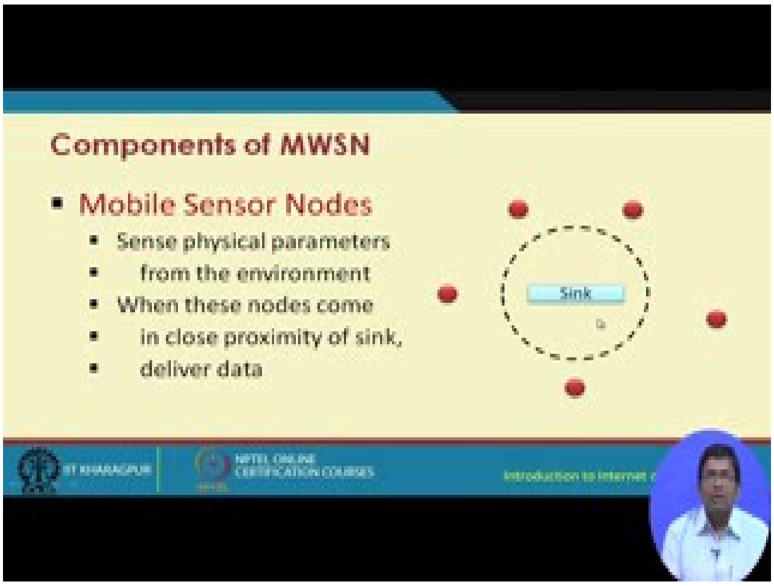
So, this is what I was telling you little while back. So, mobile wireless sensor networks are basically a conceptual integration of MANETs with wireless sensor networks.

(Refer Slide Time: 05:25)



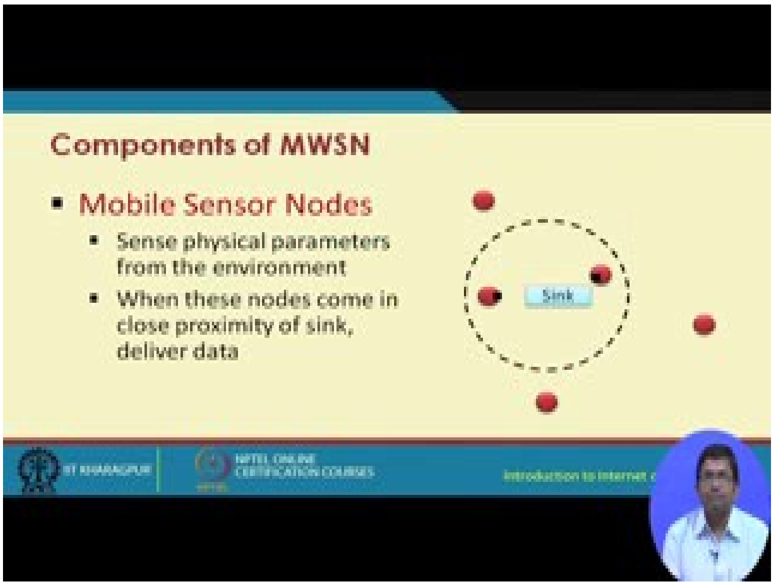
So, components of a mobile wireless sensor network one is the mobile sensor node the nodes themselves could be mobile. So, these nodes we have a sink, these nodes can move all around the sink. So, the sensor nodes, these mobile sensor nodes they would be sensing some physical parameters from the environment like the way it is shown over here. So, this node this red color node is sensing some physical parameter around the environment.

(Refer Slide Time: 05:55)



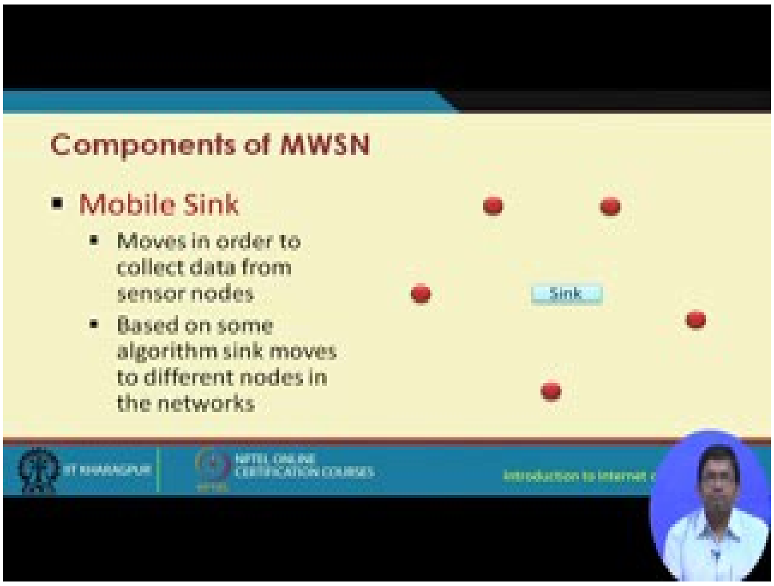
So, they sense the physical parameters from the environment, when these nodes come in close proximity of the sink they would deliver the data as shown

(Refer Slide Time: 06:05)



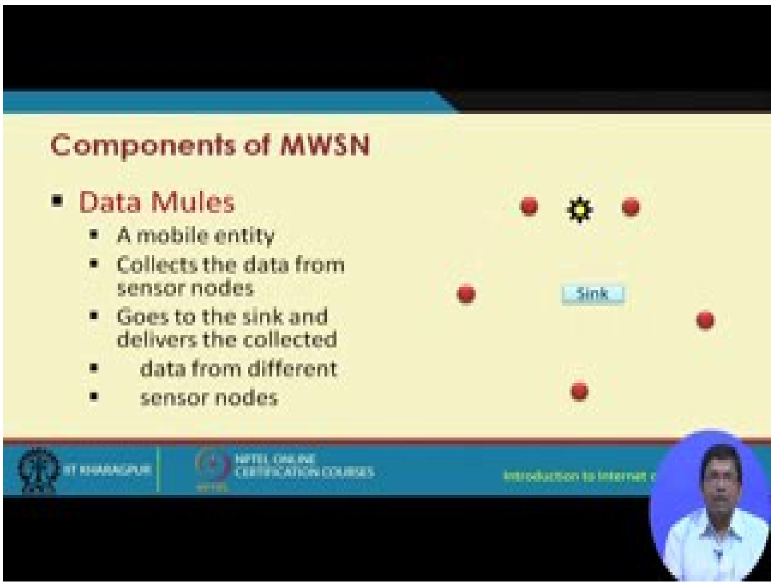
So, in this particular figure as we can see what happens is these two nodes they have come within the communication range of the sink node, and once they come into the communication range of the sink node they would deliver the sense data. So, maybe they have sense that data somewhere outside this range then they have moved and then they dump that data once they come into the proximity of the sink node.

(Refer Slide Time: 06:41)



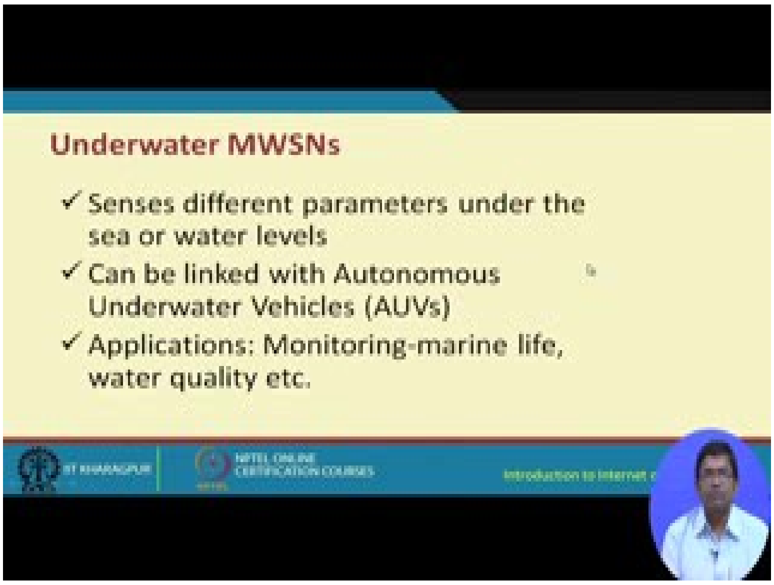
Then we have the mobile sink, which moves in order to collect data from the sensor nodes the sink itself this. So, these sensor nodes in the earlier situation in the earlier example we had considered that the sensor nodes can move; here actually in this particular figure we show that the sensor nodes are all stationary, the sink node can move and can collect data from each of these sensor nodes.

(Refer Slide Time: 07:12)



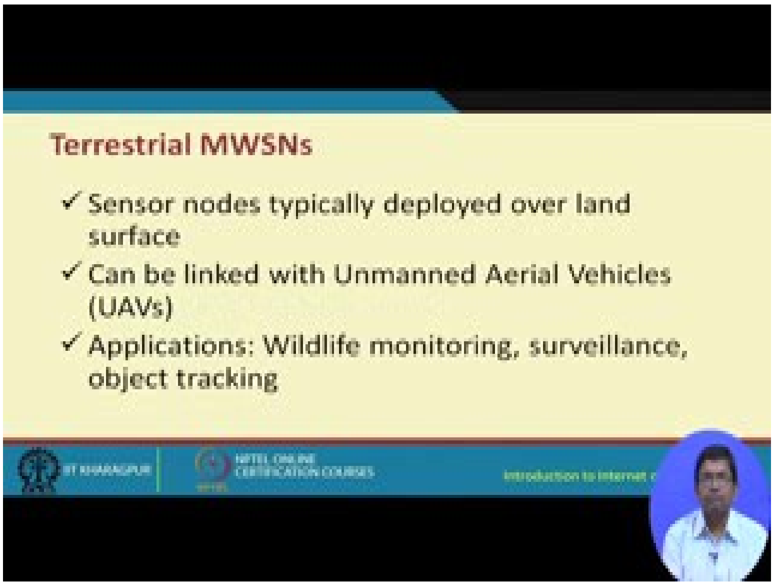
Then we can have data mules future mobile. And these are like external entities which collects the data from the sensor nodes goes to the sink and delivers the collected data from the different sensor nodes. So, this mule can go in close proximity to each of these red colored nodes. And thereafter once it has you know finished collecting the data from these red colored nodes it will come in the close proximity of the sink node and will deliver the message to the messages all these messages to the sink node.

(Refer Slide Time: 07:47)



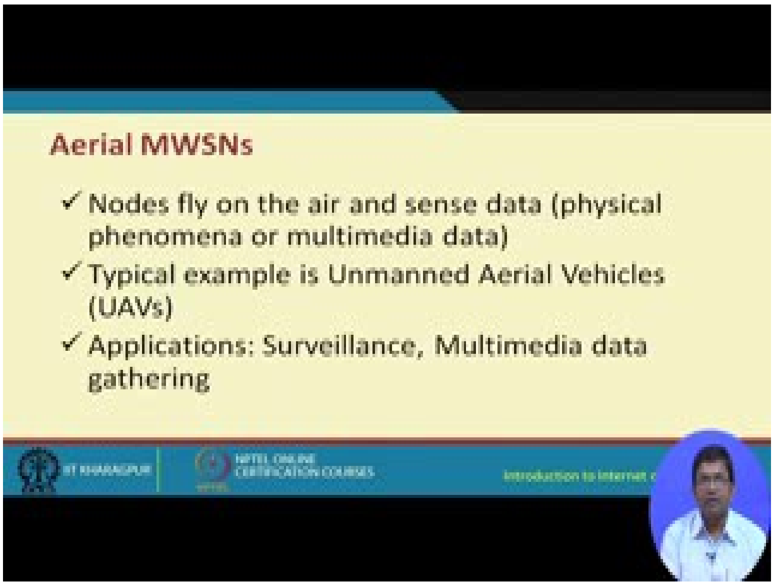
Now this mobile sensor network it can be used either in the terrestrial environment maybe by fitting sensors to robotic devices or can be used in the aerial environment, flying sensor networks. For example, the sensors the nodes themselves they fly or it can be an underwater sensor network that means that the sensors are fitted to underwater mobile devices like autonomous underwater vehicles, rovers and so on. So, the examples could be to monitor the marine life or water quality. So, we have use of underwater mobile sensor networks which can autonomously automatically sense and remotely send the sensed parameters of different things such as the sea level, water level you know water quality marine life and so on and so forth.

(Refer Slide Time: 08:53)



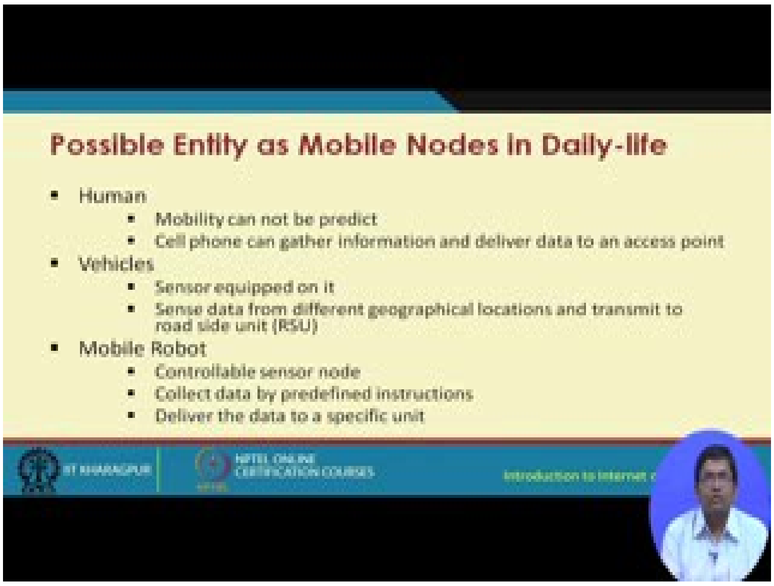
Terrestrial wireless mobile sensor networks sensor nodes typically deployed over land which can be linked with AUVs; that means, the autonomous unmanned aerial vehicles and the applications would be wife wildlife monitoring, surveillance, object tracking and so on.

(Refer Slide Time: 09:11)



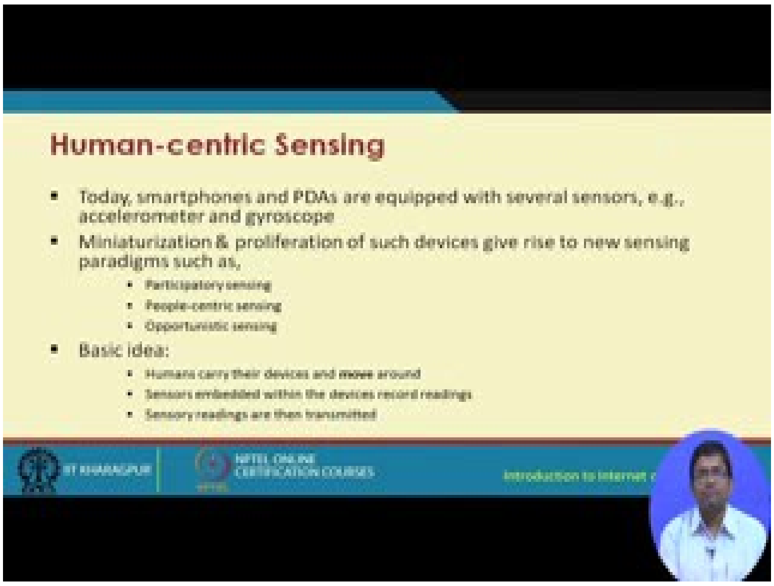
And the aerial version I told you where the nodes they fly. So, when they fly they sense and they form a network through which the data are sent to the surface station. So, the typical examples is unmanned aerial vehicles fitted with sensors; applications include surveillance, multimedia data gathering and so on.

(Refer Slide Time: 09:32)



So, what can be mobile, what can be mobile in a mobile sensor network? We can have different types of examples of mobile entities from daily life one is the humans, humans can be mobile and the mobility of humans are unpredictable. For example, if somebody is walking with the cell phone on and then we want to gather the information of the cell phone then it is unpredictable to you know so it is unpredictable how the human being is going to move and consequently it is unpredictable to predict the mobility of the cell phone. For vehicles, for example, sensors are typically used in cars and different modern day vehicles so that becomes vehicular sensor network where these vehicles are fitted with different sensors the sensed data from the different geographical locations and transmit to the roadside unit. And then we have the mobile robots which are controllable sensor nodes that collect data by predefined instructions and deliver the data to a specific unit.

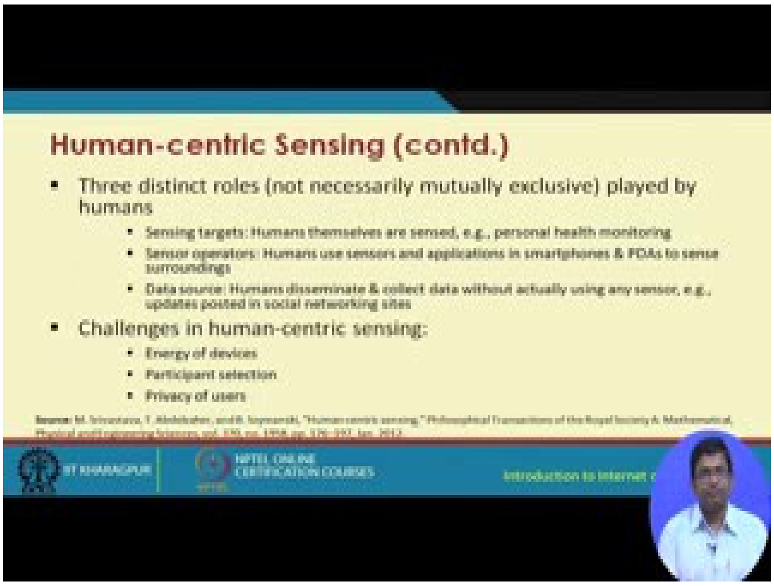
(Refer Slide Time: 10:50)



Human-centric sensing is possible because of the use of smartphones and PDAs which nowadays are equipped with several sensors typically even up to like several sensors there are lot of smartphones. So, these sensors could be like accelerometer sensor, gyroscope sensor and so on which are commonly available in the modern day smartphones and PDAs. So, miniaturization and proliferation of such devices give rise to new sensing paradigm such as participatory sensing, people centric sensing and opportunistic sensing. Participatory sensing in participatory sensing a crowd, a group of people each having their smartphones equipped with sensors turn on their respective sensors in their mobile phones and then consequently what is going to happen is we are going to form a human-centric sensor network a human centric mobile sensor network.

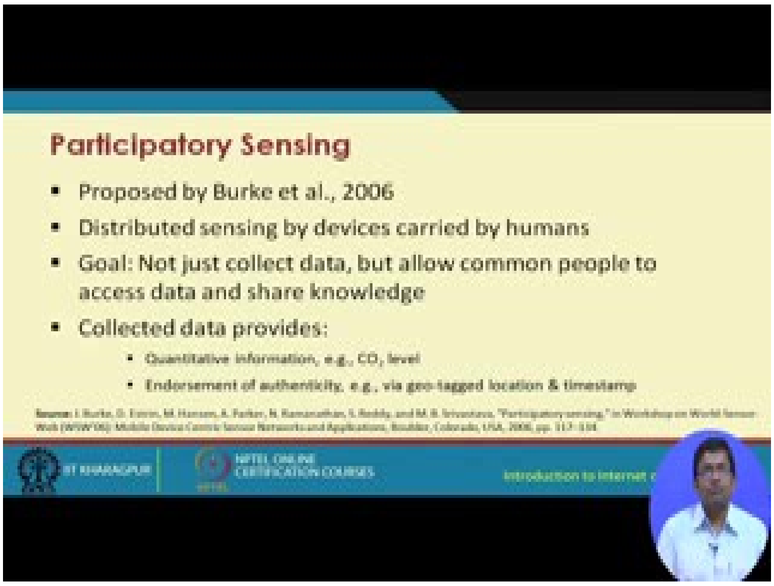
Then we have the people-centric sensing very similar to the example that I just told you. So, basically you know the previous example I had talked about using peoples people moving. So, a every you know people they can also sense you know we have eyes, ears etcetera. So, through which we can also sense the people can also sense so that becomes people-centric sensing. And then we have opportunistic sensing which basically is that peripheral a particular node moves in that to a different location then opportunistically it is going to sense and then opportunistically it is going to deliver the message if another node comes in proximity.

(Refer Slide Time: 12:35)



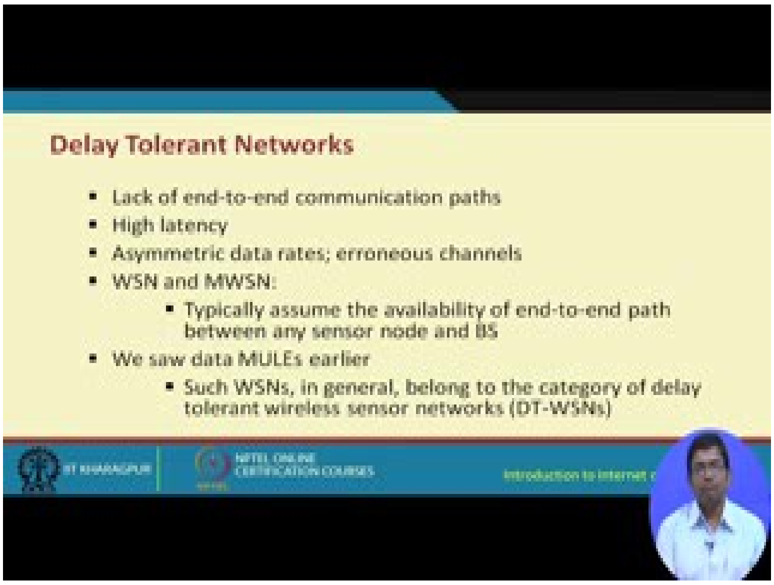
So, the basic idea is that humans carry their devices and move around sensors embedded with the devices, record the readings and the sensory readings are then transmitted. There are three distinct roles played by humans, one is the sensing of the targets, second is the sensing of the operators and third is the acting as a data source.

(Refer Slide Time: 12:58)



Now, for human centric sensing there are different challenges, challenges with respect to the energy of the devices, then participants selection, privacy of users and so on. So, I already explain to you the concept of participatory sensing which was proposed by Burke et al., in 2006 as you can see that it is not a very long or you know old concept. And here basically we are talking about distributed sensing by devices carried by humans and the goal is not just to collect the data, but allow common people to access the data and share the knowledge.

(Refer Slide Time: 13:25)



Delay tolerant networks basically you know from one point to another the sense data will take lot of time to get delivered compared to the regular time. So, with this we come to an end of this series of lectures on sensor networks. We have seen that sensor networks are very much attractive and more importantly sensor network I would think personally to be the most effective most important tool for building internet of things and we have covered the different aspects of sensor networks in detail. There is a separate NPTEL course which is on wireless ad hoc and sensor networks where we discuss about the details of sensor networks in depth.

So, we come to an end of all these lectures on sensor networks for internet of things.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 19
UAV Networks

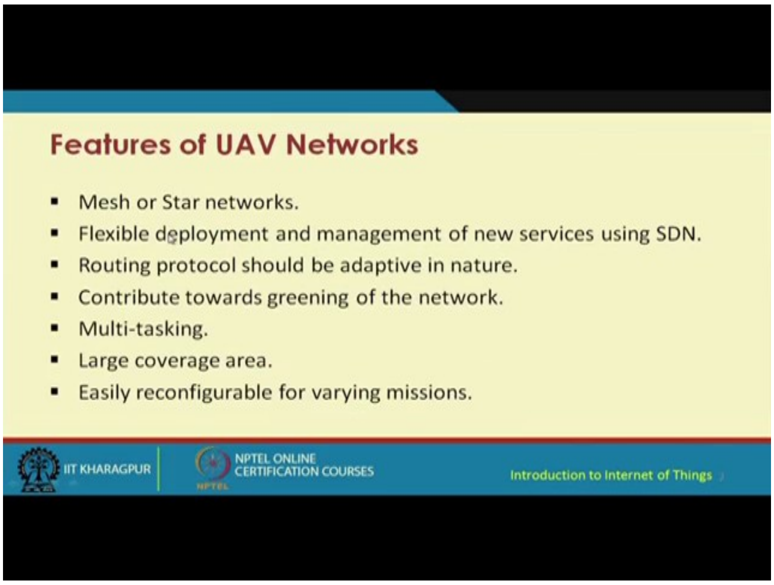
So far in the previous lectures we talked about networks, which are going to operate on the ground typically. But it is also possible for networks to be formed out of flying objects. So, we have flying networks. So, these flying objects could be different things like the these could be aeroplanes, helicopters, you know several helicopters, inter network together or few small, small planes which could be inter network together or nowadays we have these UAVs or drones more popular are the quad copters. These quad copters could be acting as these flying objects. And if we have a several such quad copters flying together we can inter network them we can network them together, So that they can communicate between themselves and they can go about accomplishing some missions.

And this particular, this particularly is very much attractive for different types of applications civilian applications, and particularly for military applications this is very, very important. For example, is form of UAVs, a network of UAVs could be going and accomplishing some task across the border maybe, performing some recognize a survey between 2 countries, border bordering 2 countries right.

So, in the borders the swarm of UAVs can go and it can surveyed. Similarly, if there is some kind of a disaster. Post disaster you know taking stock of the situation a swarm of UAVs can go take stock of the situations maybe through their cameras or whatever and come back. So, they have to interconnect they have to talk to each other and then send that sensed, sensed or you know collected information to the ground station. This is done using something known as the UAV network.

So, in plain and basic terms, UAV network is a network of UAVs. So, quad copters for example, or drones more generally can be internetwork together to form UAV networks. So, there are different features of UAV networks.

(Refer Slide Time: 02:42)



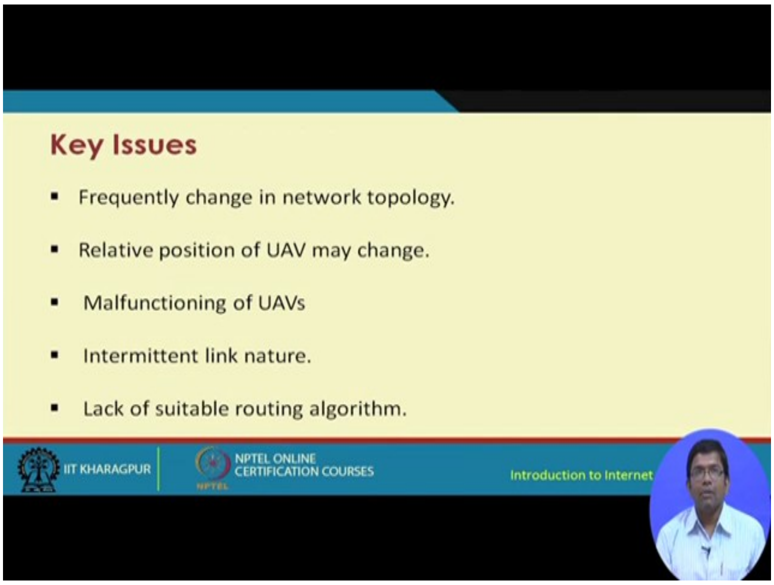
So, first thing is the topology. So, we are talking about a network which is highly dynamic, the topology is fast changing very fast changing, compared to this you know the terrestrial networks, compared to the terrestrial or ground networks. Because these are flying objects and they fly at very high speeds, the topology itself will be changing very fast. And the network itself will be moving together. And consequently the dynamic, dynamism in the topology is going to be very much.

So, there are 2 types of popular topologies that are used to have to model UAV networks. One is known as the star topology. I will show you what is the meaning of star topology. And then we can have a mesh topology which is, attractive in the sense that you know mesh basically mesh kind of topology for any network ensures reliability and fault tolerance. So, mesh networks are very very attractive and, but at the same time star topology is more common and are easily deployable. Then the second feature is the flexible deployment and management of new services using SDN.

So, now a day's people are talking about using SDN to manage UAV networks for deploying flexibly deploying and managing different services. The routing protocols should be adaptive in nature, should contribute towards greening of the network. And, multi tasking, multi tasking is a very important feature. So, these nodes you know, so these flying nodes these quad copters for example, in a UAV network they could be doing different things together, they have to do different things together. And that is a very important feature of UAV network.

Then another very important feature of UAV network is that, you can cover you can offer connectivity over a larger area. So, you can have larger coverage of connectivity or sensing coverage also can be expanded with the help of UAV networks, because these are fast moving flying networks comprising of different flying nodes. So, this could be easily configure reconfigurable for varying missions. So, depending on the mission these networks can be you know programmed or predefined or reconfigured or preconfigured in different ways.

(Refer Slide Time: 05:23)

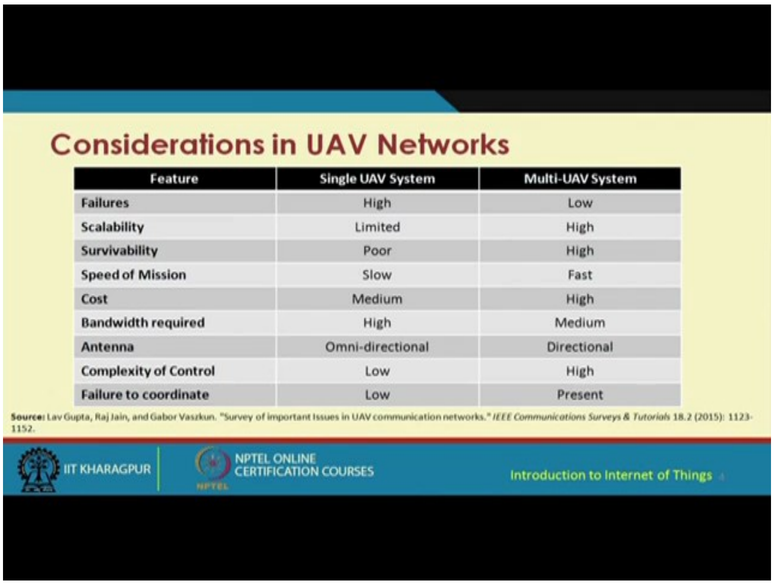


So, the key issues here are that we are dealing with a different type of network, where the topology is going to frequently change, very frequently change. Then the relative position of the UAVs may also change very frequently because within a group these nodes are going to change their positions pretty fast. So, we have a network where not only the network is moving very fast, could be moving very fast, but also these nodes in that particular network they could also be changing their positions pretty fast.

Then the third feature is malfunctioning. If there is some malfunctioning in the network, if there is some malfunctioning in the network maybe a particular node you know the hardware has failed it does not fly any further. Then these networks are developed in such a way that they can still continue to function, they can still continue to function in the presence of malfunctioning. They will reform the network the topology is going to be reformed, the topology is going to be changed and they are going to function. And the next one is intermittent link nature. Which means that because this topology is changing, because the internal node positioning is going to change dynamically over time, the links are going to be also changed you know, so 2 nodes they might be linked up at one instant of time. Then with one of these nodes another link might be set up in another in a instant of time and so on.

So, intermittent link connectivity, intermittent connectivity sometimes these links might be you know these nodes might be able to communicate over a particular link at a few other instance they may not be able to communicate over the links and so on. So, intermittent link connectivity and, lack of suitable routing algorithm is another feature. So, basically you know what happens is because it is a highly dynamic different kind of network that routing algorithms like AODV DSR etcetera, that are available for ground ad hoc networks or ground terrestrial sensor networks are not usable per se in these kind of networks which are highly dynamic, much more highly dynamic than even manets mobile ad hoc networks.

(Refer Slide Time: 07:46)

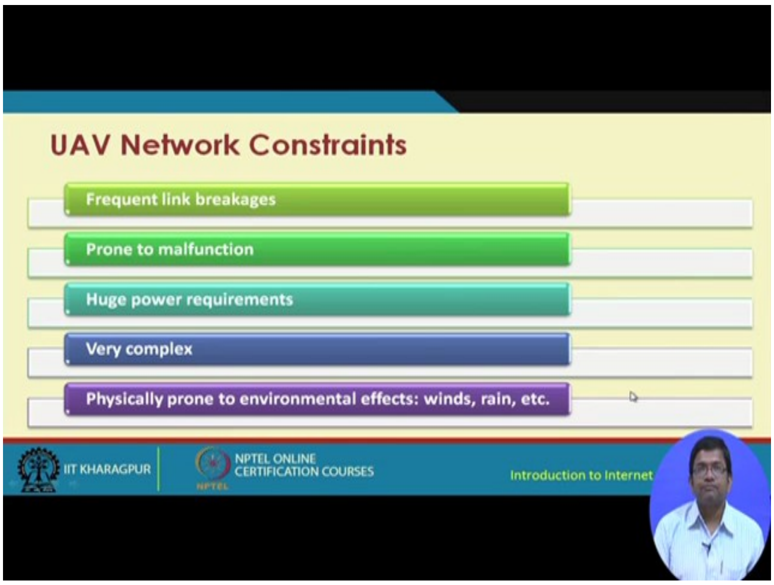


Here are some of the considerations in UAV network. We have a single UAV system and we have a multi UAV system. Failures single UAV system the chances are high. In a multi UAV system the chances of failure are low. Failure of the system as a whole, we are talking about failure of the system as a whole, and this is quite obvious. The scalability is limited in a single UAV system, in a multi UAV system, you know, it is highly scalable. Because, if you, if you increase the few nodes you know the node the basically the network can be expanded further. Then we have the speed of mission. In a single UAV system the speed is slow, but in a multi UAV system the speed of mission is fast.

Survivability is poor in a single UAV system; survivability in a multi UAV system is higher. The cost in a single UAV system the cost is medium cost because, you are dealing with a single UAV and in a multi UAV system the cost is medium because, you are dealing with, sorry the cost is high because you are dealing with a multiple UAVs. In terms of the bandwidth requirement the bandwidth requirement over here is high whereas, when a multi UAV system the bandwidth requirement is medium. In a in the case of antennas, the antennas over here are omni directional whereas, in multi UAV system the antennas are directional. In terms of the complexity of control, it is low in a single UAV system, but high in multi UAV system.

In terms of the failure to coordinate low in a single UAV system and in a multi UAV system it is present.

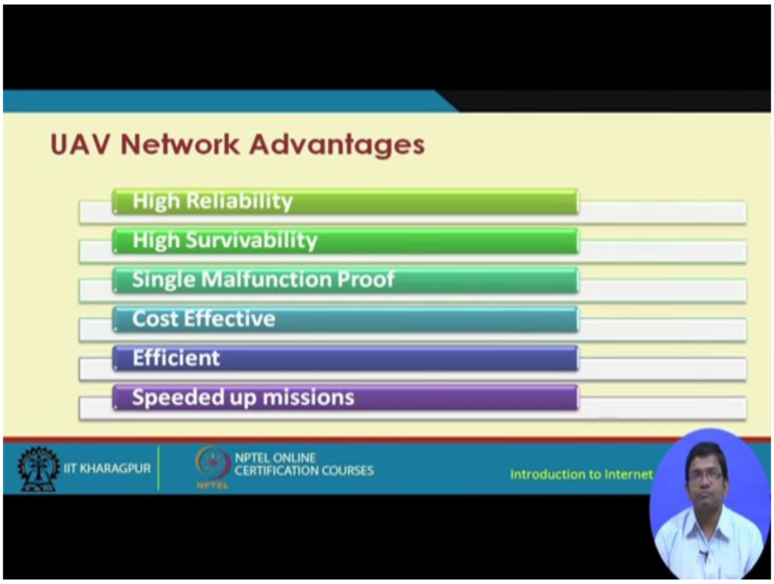
(Refer Slide Time: 09:33)



So, there are different constraints on these UAV networks we have frequent link breakages due to the high degrees of dynamism that I just mentioned. These networks are prone to malfunctioning due to one or more nodes failing, and this is quite possible in these flying networks. Then we have huge power requirements because you know these nodes are like you know high powered you know these nodes they have to fly and they have to again carry some payload, and then they have to communicate.

So, all these basically increase the power requirements per node. These networks that are formed are quite complex very complex networks because of these all these dynamisms and the complexity of changing topology, mode position, link breakages and makages and so on. Then then physically these nodes are physically prone to environmental effects with respect to wins, rain etcetera. Because they operate in such kind of environment, where they are they are they are susceptible to environmental effects.

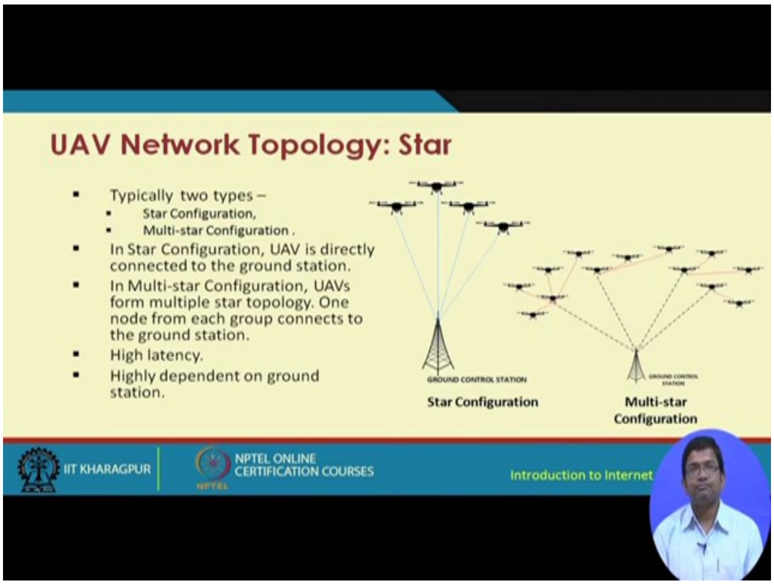
(Refer Slide Time: 10:45)



The advantages of UAV networks include high reliability. Because you know, instead of a single UAV if we are talking about several UAVs that improve in that improves the reliability of the system, high survivability is another important feature. Single mal function proof you know, if single node malfunctions you know UAV network are not going to get affected where is the single UAV systems are going to get affected. Cost effectiveness you know, In fact, you know unlike what would normally be believed you know, these networks UAV networks are cost effective. Cost effective because you know, so what happens essentially is I mean although initially you we are going to buy couple of these UAVs not one, but they can you know accomplish a mission much more efficiently compared to a single UAVs.

So, that way basically the cost is you know the efficiency with respect to cost is improved in a UAV network. Efficiency overall of the network improves in a UAV network system, and the missions can be speeded up you know. So, the time that it takes for accomplishing a particular mission that gets speeded up in UAV networks.

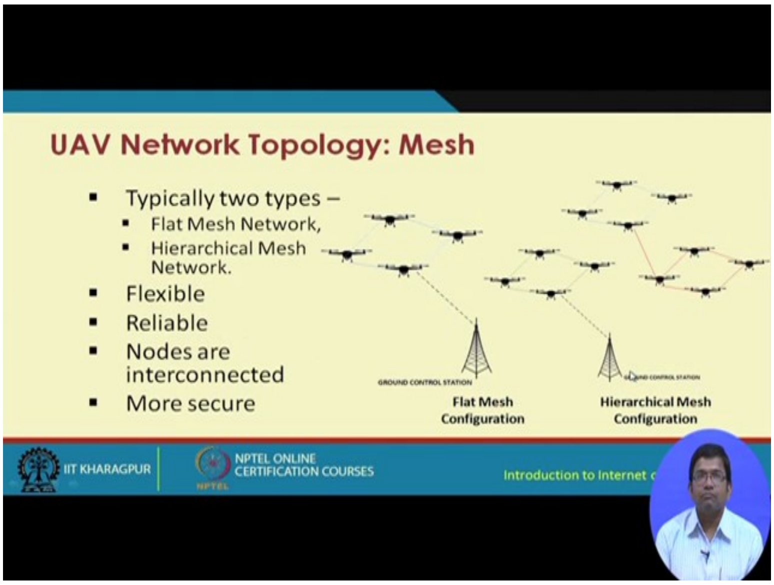
(Refer Slide Time: 12:02)



So, if you recall that initially we were discussing about the different topologies of UAV networks. So, we will start with the star topology. So, there are 2 types of topologies in star one is the basic star, and where we have this ground station. And these different UAVs basically connected directly to this ground station to form a star topology.

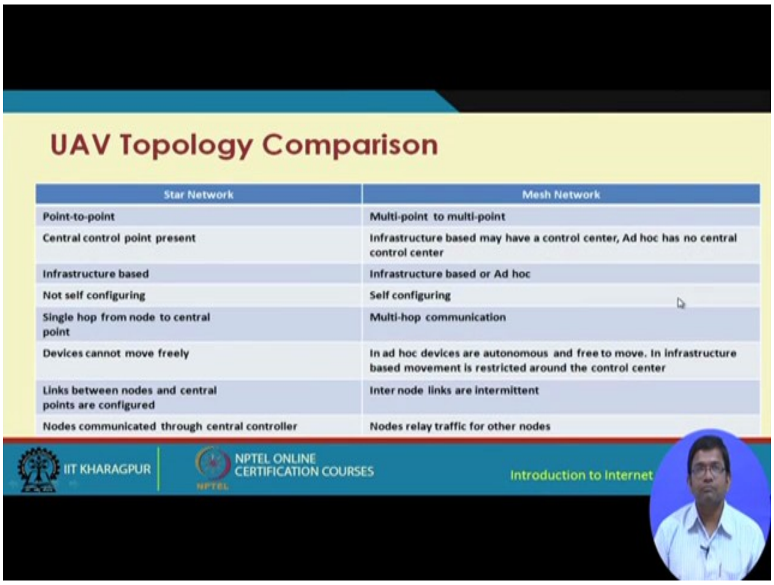
Then we have the multi star topology where, basically you know this particular unit is repeated and, so we have 1 star 2 stars 3 stars and 4 star 4 star topology you know 4 stars all connected to you know 4, 4 of these starts call connected to the ground station.

(Refer Slide Time: 12:46)



In a mesh topology, a mesh kind of topology is formed. And one of these nodes in this mesh is going to connect to the ground station like this. So, we have this unit of the mesh and this is repeated and this kind of architecture this kind of topology is; obviously, quite scalable.

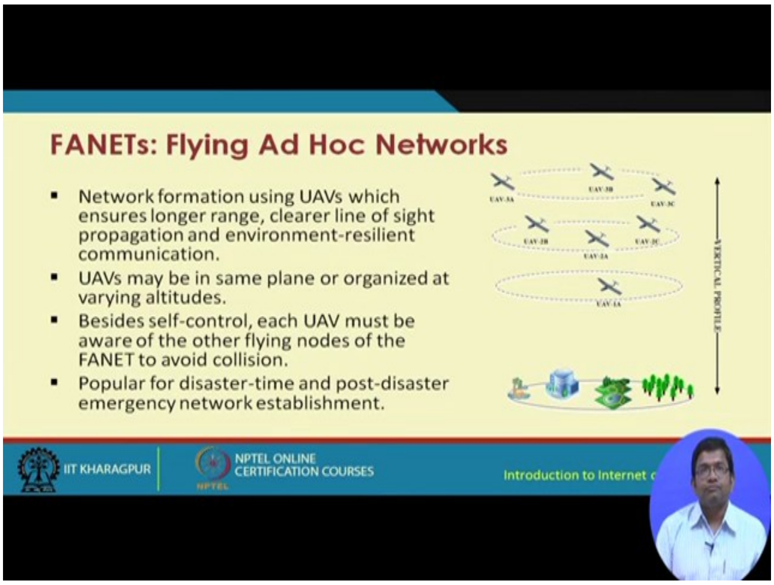
(Refer Slide Time: 13:10)



So, when we compare the star topology and the mesh topology star topology is point to point communication, in the mesh topology we have multi point to multi point communication. Then we have the central control point present in a star topology whereas, it is infrastructure based may have a control center and ad hoc has no central control center. So, basically you know if it is infrastructure based it may have a control center whereas, if it is a adopt based then there is no control center in the mesh network.

It is infrastructure based in the star network whereas; it is infrastructure based or ad hoc in the mesh network. Likewise actually there are other properties that differentiate the star topology with the mesh topology. I am not going to go through them further, but it is given to you in this particular table for you to go through.

(Refer Slide Time: 14:10)



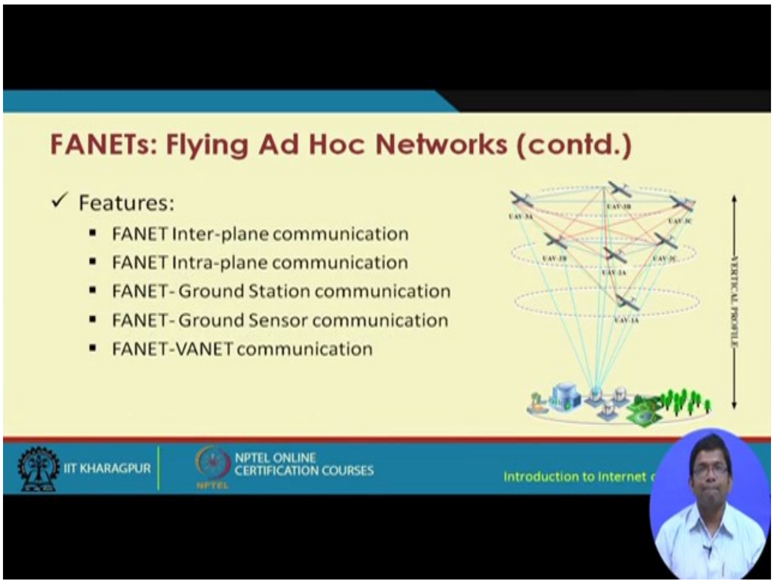
So, essentially what we are talking about is something like a flying network. So, ad hoc networks on the ground we have already we know how they work. So, there is no centralized coordinator, there is no network manager, the nodes they come together they self organize self configure and then they start working. Now imagine that that ground ad hoc network is brought up to, to fly.

So, then what we have is a flying ad hoc network. And this flying ad hoc network is known in short as fanets on the contrary, the ground based ad hoc networks are known as mobile ad hoc networks. So, we have this network formation done using UAVs which ensure longer range, clearer line of sight propagation and environment resilient communication. And these UAVs maybe in some plane or are organized at different altitudes like shown over here.

So, like these 3 UAVs are in the same plane, these 3 UAVs are in another plane and these this UAV is another plane. So, as we can see that they are they are in 3 different planes with 3 different altitudes, but these UAVs in a single plane they are they are in that same plane. So, besides self control each UAV must be aware of the other flying nodes of the flying ad hoc network to avoid collision because if that information is not known then it might. So, happen that you know there might be chances of physical collision between the different nodes of the same network.

So, this sort of network topology flying ad hoc networks is popular for applications such as disaster monitoring, post disaster monitoring, emergency network establishment and so on.

(Refer Slide Time: 16:12)

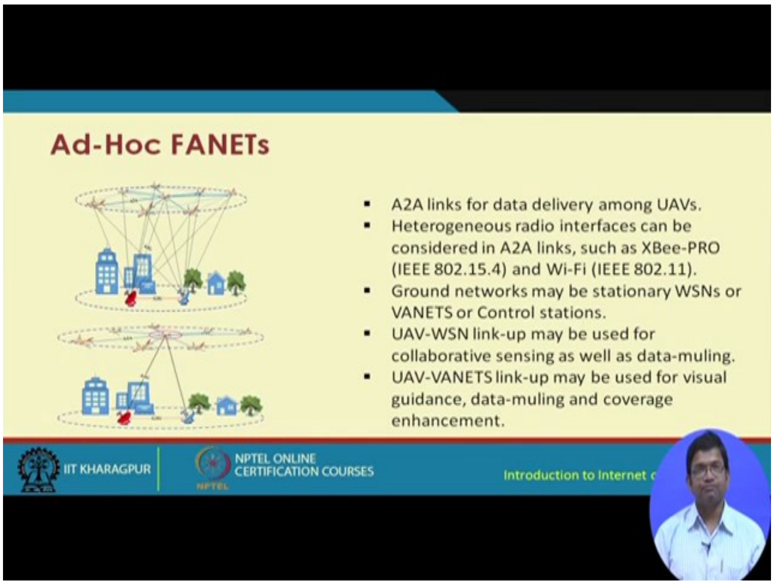


Flying ad hoc networks basically the communication takes place in different planes. One is inter plane communication. So, inter plane communication means that, so as we can see in this particular figure, we have one plane, we have second plane, we have a third plane. Inter plane communication basically takes clear you know, takes into account how the UAV of one plane communicates with UAV of another plane.

So, inter plane communication, then we have intra plane communication like, within the same plane these UAVs communicating with each other is inter plane communication. Ground station communication from a UAV in one of these planes to the ground station, is ground station communication. Ground sensor communication likewise in sensor communication with the ground and then we have fanet vanet communication, so fanet is this one that we are discussing about. Now these could be connected to vehicular ad hoc networks on the ground the vanets on the ground.

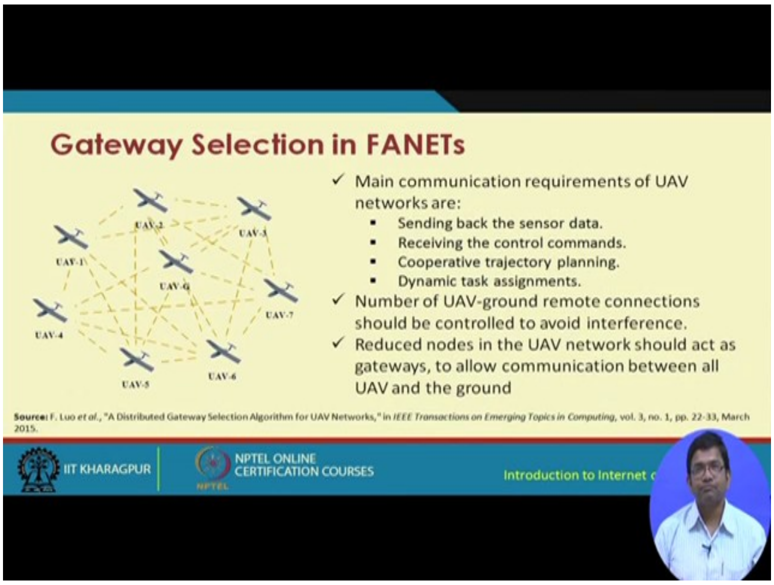
So, flying ad hoc networks vehicular ad hoc networks can be connected together to be able to communicate.

(Refer Slide Time: 17:22)



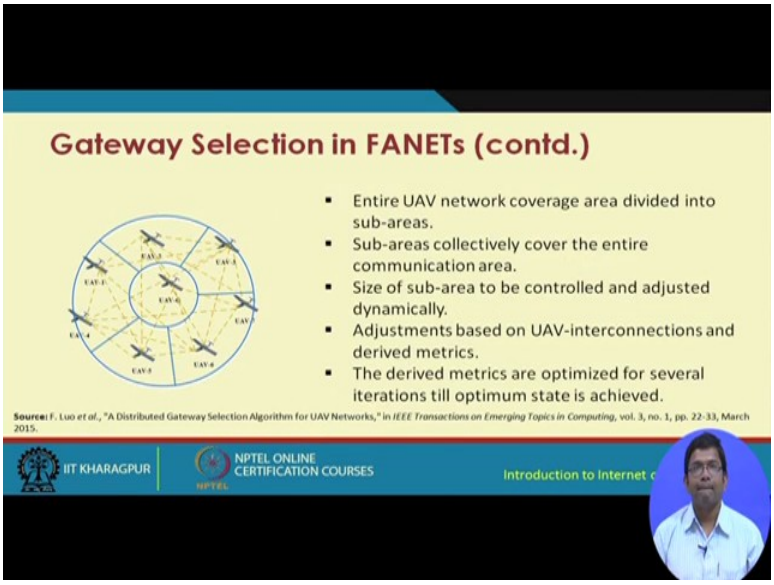
So, we have different types of links, we have the air to air links for data delivery among the UAVs. Then we have heterogeneous radio interfaces in the a to a links, using zigbee pro following 802.15.4 standard or using Wi-Fi 802.11 standard. The ground networks may be stationary sensor networks or vanets or contour stations, and the UAV-WSN link up may be used for collaborative sensing as well as data muling.

(Refer Slide Time: 17:59)



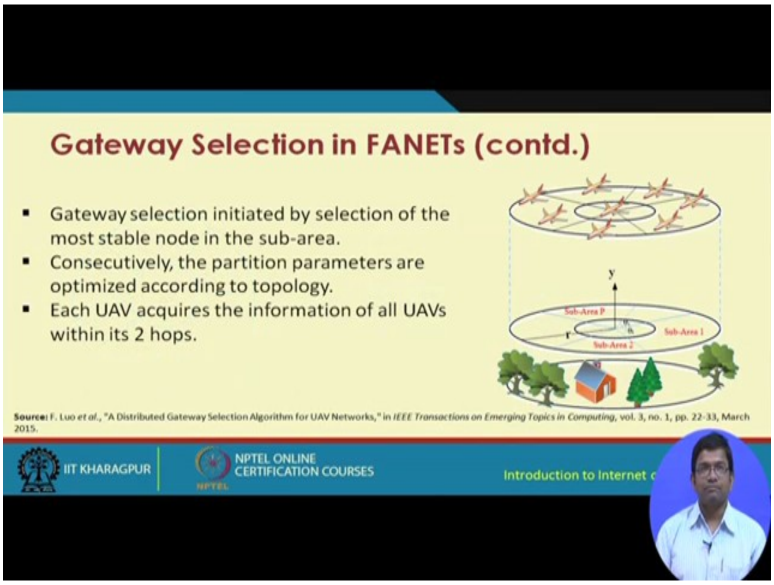
The main communication requirement of UAV networks are sending back of the sensor data, deceiving the control commands, cooperative trajection trajectory planning and dynamic a task assignments.

(Refer Slide Time: 18:15)



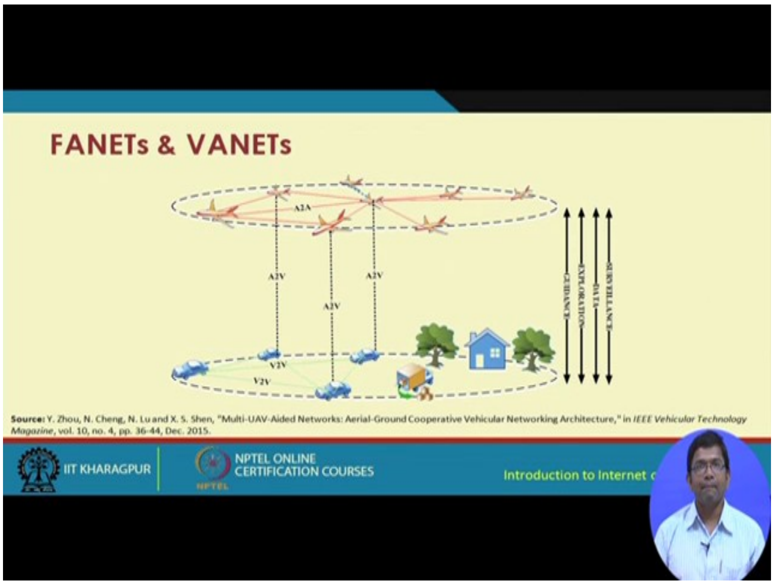
So, in this particular figure as we can see over here. We have a bunch of different UAVs, maybe working in a plane, functioning in a plane. And then we have one of these nodes which is designated as the gateway which acts as a coordinator, with all the other nodes in the same plane. So, inter UAV network coverage area will be divided into sub areas as shown over here. So, this particular coverage area is divided into sub areas like this, this, this, this and this. And the sub areas collectively covered the entire communication area. The size of a sub area to be controlled and adjust is to be controlled and adjusted dynamically. And these adjustments are based on UAV interconnections and derived matrix. The derived matrix are optimized for several iterations till optimal and the till the optimal state is achieved.

(Refer Slide Time: 19:13)



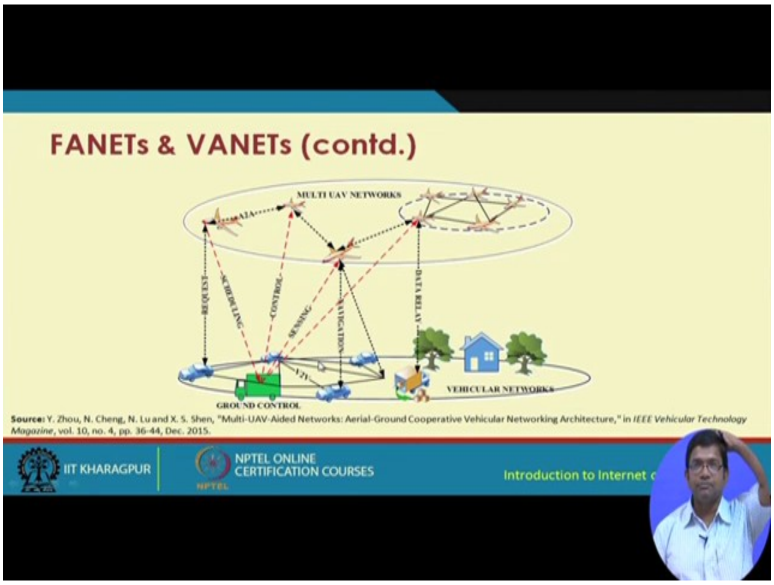
So, how do you select the gateway the gateway selection is initiated by the selection of the most stable node in a particular sub area? So, in a particular sub area the most stable node is considered. That must consecutively the partition parameters are optimized according to the topology where, each UAV acquires the information of all UAVs within it is 2 hops. So, flying ad hoc networks and vehicular ad hoc networks as you can see over here, there is a link up.

(Refer Slide Time: 19:44)



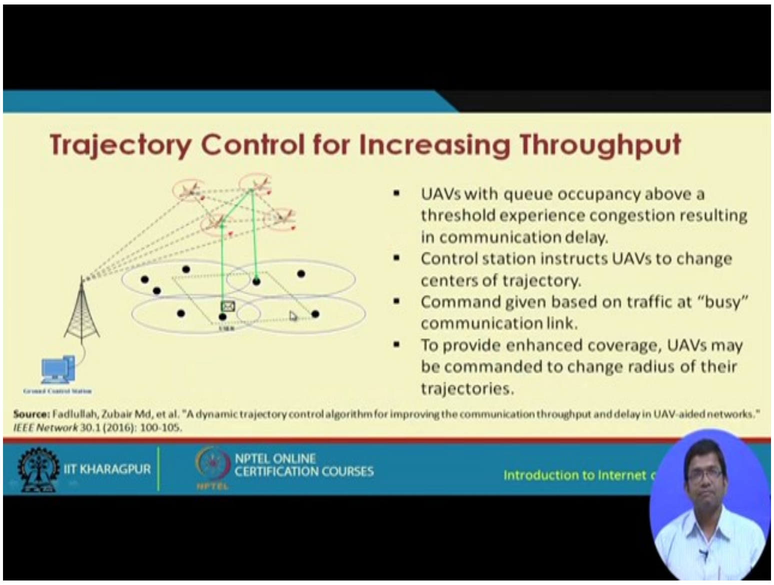
So, this is the flying ad hoc networks with a to a link etcetera, and then we have this v to v link over here in the vehicular network. And then here this connectivity shows the a to v link where, it is basically air to vehicle link.

(Refer Slide Time: 20:03)



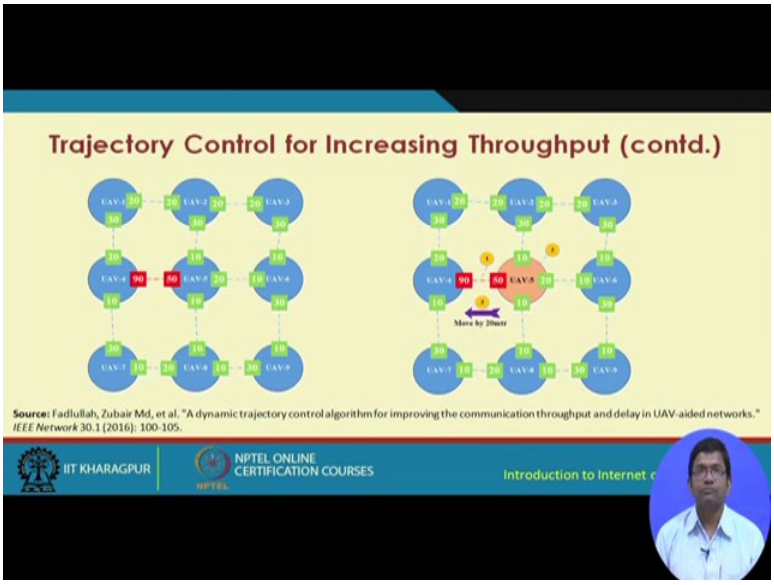
So, meshed kind of network can be formed in a particular particular plane. And then there can be different links between the UAV network and the ground vehicle between the ground vehicle and another flying node, and so on and so forth. So, like this actually the different types of communication are going to take place. So, the trajectory control for increasing the throughput how the trajectory is going to be controlled in order to improve the overall throughput.

(Refer Slide Time: 20:29)



So, typically what happens is UAVs with queue occupancy above a threshold experience condition resulting in communication delay. The control station instructs the UAVs to change the centers of trajectory, and the command is given based on the traffic at the busy communication link.

(Refer Slide Time: 20:56)



So, as we can see over here, in this figure we see that this is a grid like deployment of the UAVs. And the buffer occupancy or the queue occupancy are also shown in this green and red colored nodes. Great not nodes, but these grid colors green colored and red colored symbols.

And then on the other hand we see that if, a particular node like this node will do it is dynamism it has moved 20 meters for example, then we see that these things have to be handled, this has to be handled. This buffer occupancy of 90 and 50 has to be has to be handled.

So, with this we come to an end of the lectures on UAV networks. And I will tell you that UAV networks are very important, they have lot of attractive applications. Military particularly, all over the world, they are they their potential customers of UAVs and UAV networks. And these UAV networks are quite popular and are bit difficult to implement as well and so we have understood the basic concepts for developing, developing these UAV networks. And there is lot of research that is going on UAV networks on different other aspects.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 20
Machine to Machine Communication

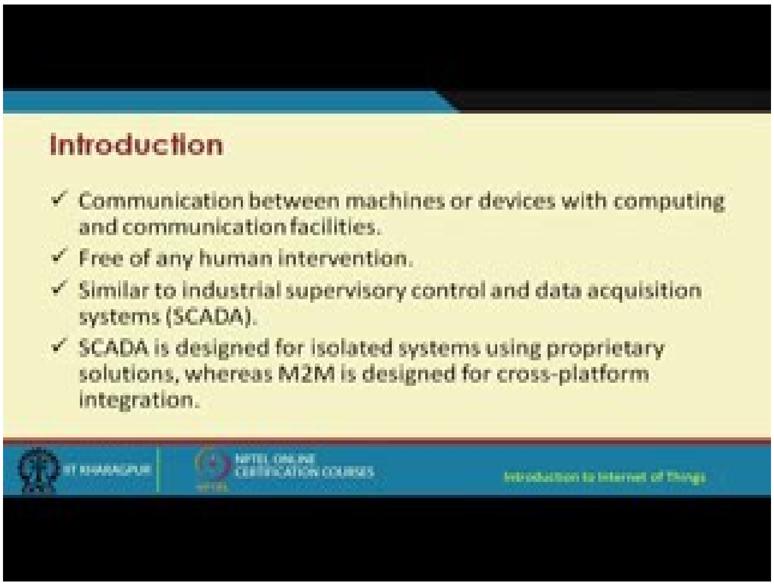
Machine-to-machine communication we are going to cover in this particular lecture. Machine-to-machine communication is one of the very vital very important concepts in building internet of things. When we are talking about internet of things autonomous behavior is something that we strive to imbibe or trust we try to inculcate in this networks that we develop. And for this basically what we have to do is we have to ensure that with minimal intervention how we can achieve different tasks. So, we are talking about sensors, we are talking about actuators, we are talking about mobile phones, we are talking about robotic devices, ground robotic devices, rovers etcetera, etcetera, UAVs and so on. So different types of machines.

And the whole idea of machine to machine communication is that with minimal or strictly speaking no human intervention how we can have communication between two machines, two machines so machine-to-machine communication right. So, this is what we try to achieve in machine-to-machine communication and machine-to-machine communication is considered to be one of the most important building blocks for internet of things. So, IoT based systems have to operate autonomously if it is let us say if we are considering something like a home automation. Let us consider this particular scenario.

Let us say that we have elderly you know elderly care in a smart home and the elderly people they have mobility impairments typically not necessarily, but it is quite common that there are mobility problems with elderly people. And in a smart home environment what might so happen that there might be some robotic devices, which can be helping these residents of a home to undertake different things. So, we can have a ground robot for example, for example, it can go and open the door of a refrigerator, this robot can go and it can open the door of a refrigerator. Then this particular robot it can even take a milk pot out of the refrigerator, then pour the milk into into a glass that milk can be put into a microwave oven. And as you can see that there is no human intervention at all, everything can be done with the help of machines interacting with machines. I will give you one more example in this particular context.

Let us say that the in the robot has opened the refrigerator and it finds that there is no sufficient milk then either the robot or the refrigerator can automatically send an SMS to the milk person. So, what happens machine-to-machine again there is no human intervention, no human has sent that SMS to the to the to the milk person. So, this becomes an example of machine-to-machine communication. So, that is why I was telling you that machine-to-machine communication has become very much attractive for IoT based applications involving applications such as smart homes, smart cities and so on. Let us go ahead and look at some of these concepts.

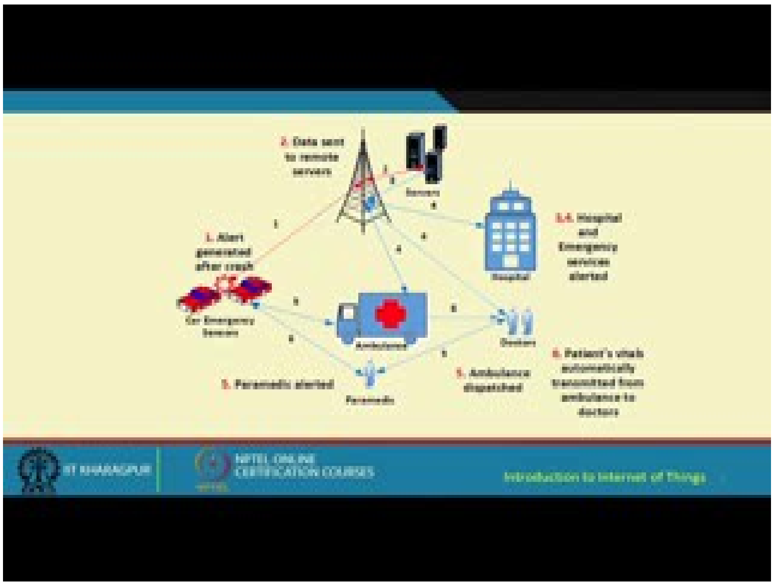
(Refer Slide Time: 04:18)



So, we have communication between machines or devices with communication and computing facilities and ideally or strictly there is no human intervention, there is no human intervention at all. Now, I do not know whether you are already aware of or not traditionally there used to be the SCADA systems. This SCADA systems are supervisory control systems that used to be typically used in industrial plants and so on. So, for you know supervisory and control operations functioning and so on, but typically these used to be not wireless, but wired. So, M2M can be thought of as the wireless variant of SCADA wireless variant of SCADA this is just you know conceptually I am just you know making a comparison with SCADA.

But it is not like you know its wireless SCADA is M2M it is not like that, but you know conceptually we can think of M2M as a wireless variant of SCADA. So, SCADA is designed for isolated systems using proprietary solutions whereas, M2M is designed for cross-platform integration this is very important typically SCADA is used for a single proprietary solutions and on the other hand M2M tries to connect you know cross platform integrate cross platform between different different technologies supporting different platforms. So, even like you know Windows, Linux, android you know all of them different devices supporting different platforms that kind of interconnect can also happen with M2M.

(Refer Slide Time: 06:08)



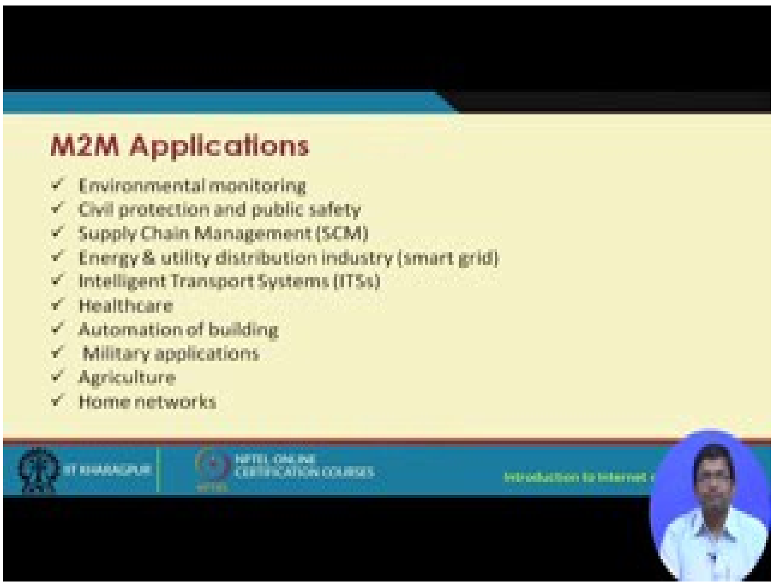
So, let us consider this particular example where it is some some sort of a scenario of offering emergency services on the highway. So, let us say that two cars in this particular example scenario we see that two cars these cars fitted with different types of sensors, emergency sensors collide these cars collide. So, after the crash an alert is generated, an alert is generated and the data is sent to the remote servers. From these servers through these base station that data would be sent to the hospital and emergency services to the patients you know to the doctor sorry to the doctors it can be sent to the ambulance, it can be sent and so on. And accordingly ambulances might be dispatched doctors might be put on alert, paramedics might be alerted and so on.

And as you can see over here like this actually the scenario continues; as you can see over here know where the human came into picture. So, everything human came into picture means that humans can be the receivers like doctors receiving the information is something, but humans were not operators or not they did not function any operation on the network right. So, this is completely M2M scenario that has been shown in this particular figure.

(Refer Slide Time: 08:01)

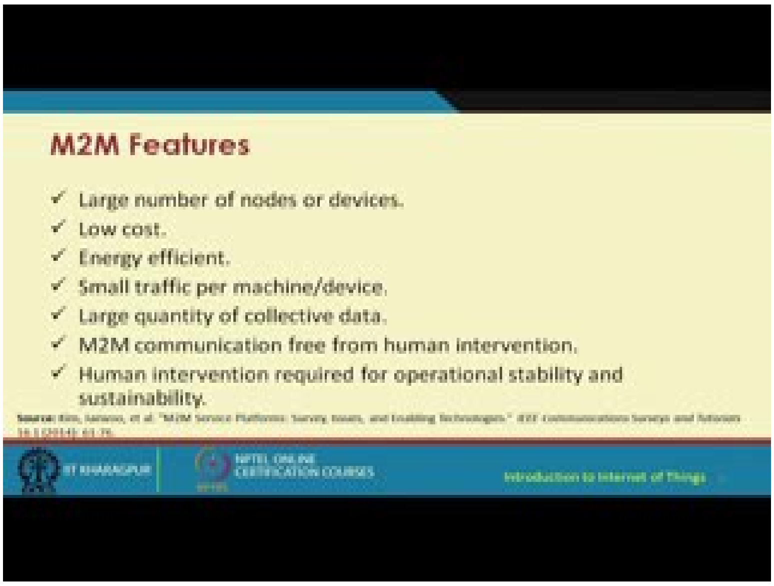
So, in M2M when we are talking about M2M, we are talking about sensors, sensors producing data through the network, information is extracted out of the data that is received, it is processed and if required some actuation is done maybe opening of the valve in an agricultural field if the soil moisture level has gone down.

(Refer Slide Time: 08:28)



There are different M2M applications, environment monitoring, civil protection and public safety, supply chain management, energy and utility distribution as in smart grid, smart grid separately common. In smart grid what we are doing we are using ICT involving sensors, actuators etcetera in a traditional smart grid, so in a smart sorry in a traditional power grid. So, in a traditional power grid we already had flow of electricity in a smart grid we have sensors etcetera, etcetera which are throwing in lot of data which have to be communicated. So, we have communication and networks on top of the traditional power power systems, power flow or energy flow. Then we have intelligent transportation systems, healthcare, automation of buildings, military applications, agriculture, home networks all these are different, different applications of M2M.

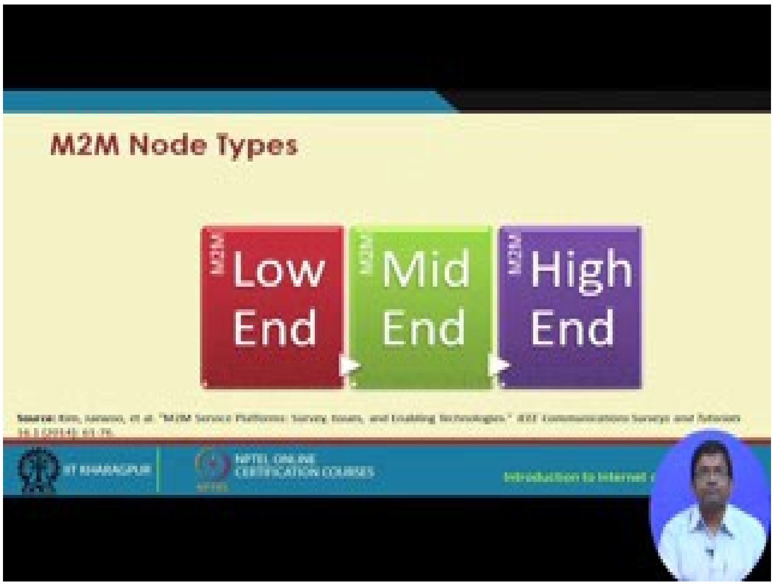
(Refer Slide Time: 09:25)



Let us now look at some of the features of M2M. Let us say the number of nodes that are required. In M2M we are talking typically of large number of nodes or IoT devices which are able you know which where there is no human to intervene they talk to each other directly. These are low cost or energy efficient, these nodes are energy efficient the network as a whole is energy efficient and typically low cost because these nodes are also very small in size, very cheap cheap to buy commercially and so on.

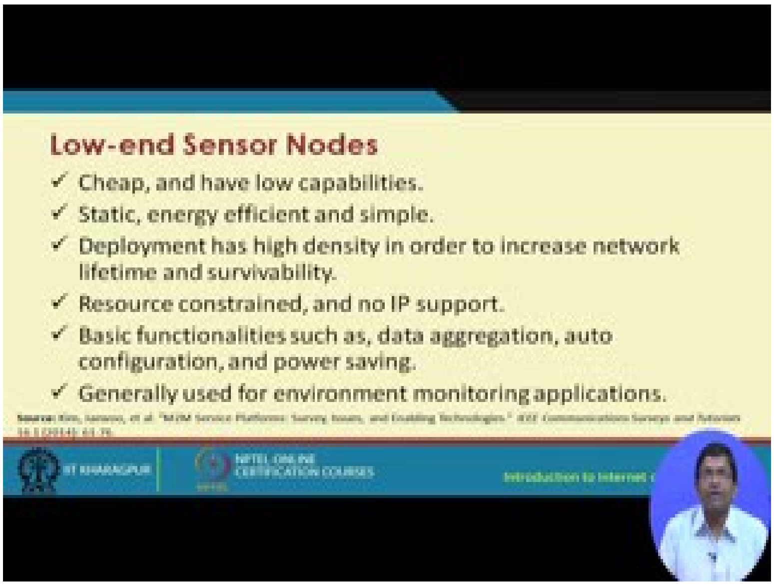
So and there is small traffic that is generated per machine or device, then large quantity of data are collected and the M2M communication is free from human intervention it is free strictly. But you know in practical applications actually sometimes there might be some minimal human intervention, but strictly in M2M basically you know there should not be any human intervention at all. Then human intervention is required for operational stability and sustainability only.

(Refer Slide Time: 10:35)



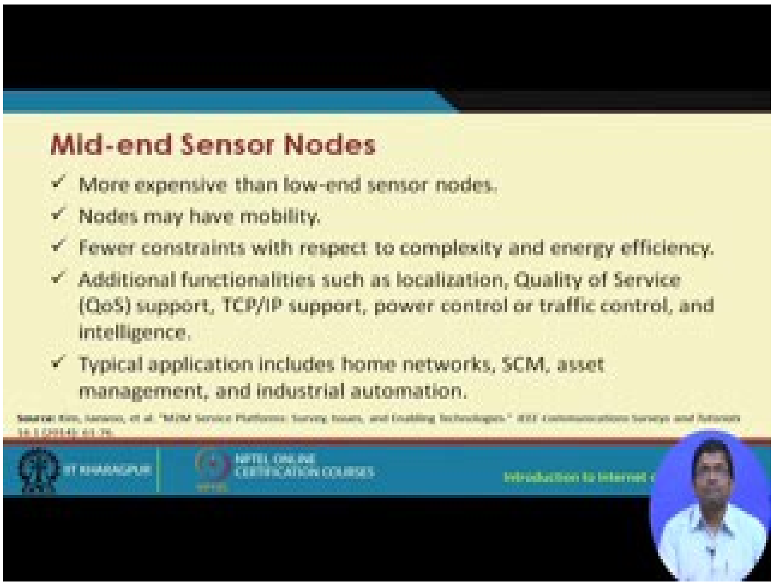
There are different types of M2M nodes. We have the low-end nodes, we have the mid-end nodes and the high-end nodes. Let us look at the features of each of these one-by-one.

(Refer Slide Time: 10:45)



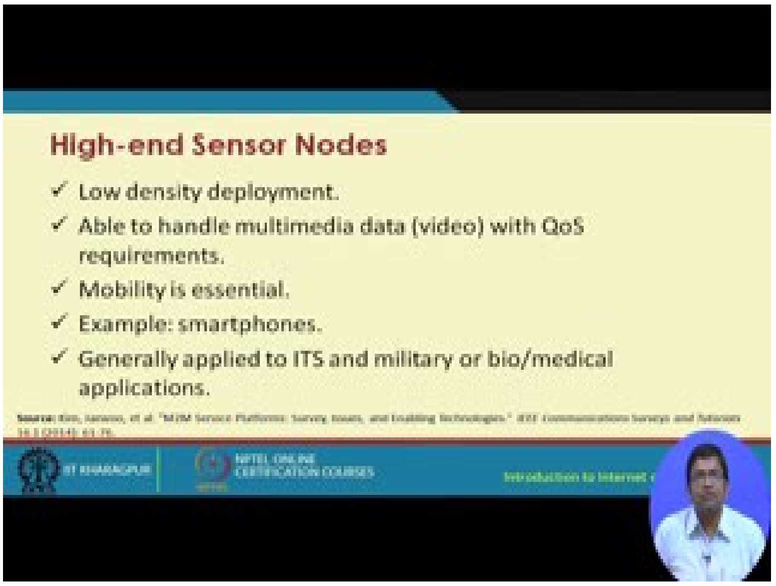
In the low end sensor nodes we have we are talking about nodes which are low in cost with a cheap and also quite justifiably, they have low capabilities their specifications are very, very limited. Then they are typically static energy efficient and simple these low end nodes deployment of these nodes has high density in order to increase the network lifetime and survivability because these are small with small space etcetera, etcetera you need large number of them to be deployed you know in a highly dense manner. These nodes are heavily resource constrained, there is no IP support basic functionalities such as data aggregation, auto configuration and power saving are supported, and these are generally used for environmental monitoring applications.

(Refer Slide Time: 11:42)



Mid-end sensor nodes relatively more expensive than the low-end sensor nodes have some degrees of mobility have fewer constraints with respect to resource complexities or you know computational complexities, energy efficiency and so on. And they support different functionalities for example, they are not like low-end nodes with bare basic you know functionality not like that. They have some little bit more functionality with respect to like localization, quality of service support, TCP, IP support or control traffic control intelligence and so on. Typical application includes home networks, supply chain management, asset management and industrial automation.

(Refer Slide Time: 12:28)

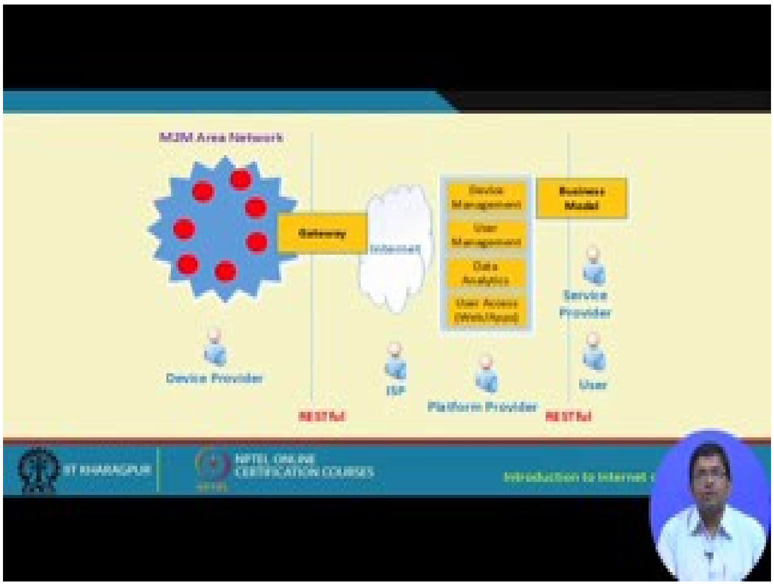


High end sensor nodes low density of deployment, they are able to handle multimedia data or video with quality of service sometimes even quality of service guaranties also they can offer. Then mobility is essential for these nodes you know so like you know these are like full-fledged nodes with lot of different capabilities including mobility as well. So smartphones are good examples of these types of nodes. Then we have these nodes typically used for military or biomedical applications.

(Refer Slide Time: 13:00)

When we consider the M2M ecosystem as a whole we have different components of it. We have device providers, we have internet service providers, platform providers, service providers and service users.

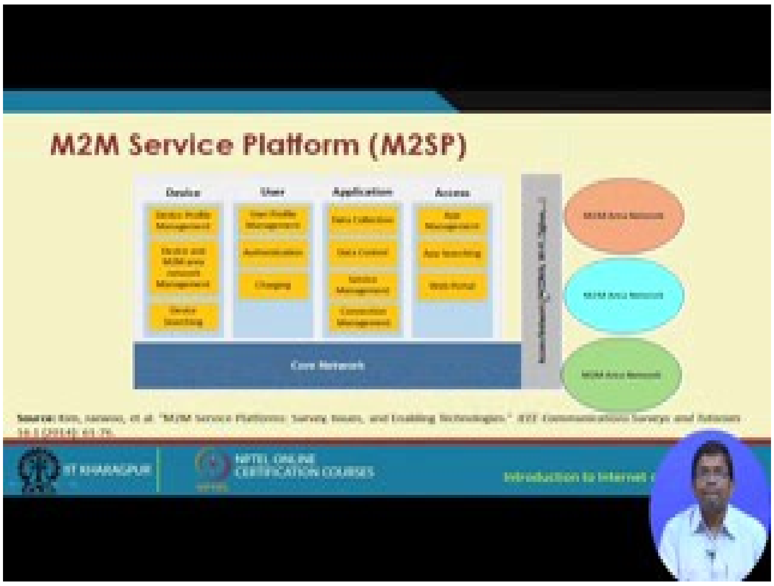
(Refer Slide Time: 13:19)



So, let us look up look at each of these in detail in this particular figure. So, you know in this particular figure what we see is we have this M2M net area network M2M area network and we have the device provider the device provider is the one which basically provides these devices which basically is the owner of these devices. So, this is basically the M2M area network. Then this M2M area network sends the data from this M2M devices, IoT devices through this gateway to the internet which is basically handled by the internet service provider. And when it is passing through it we have this RESTful architecture that basically takes care of it. The restful architecture is a low-end you know low resource consuming resource limited environment it is useful.

And in this case we are using it between as an interface between the device provider and the internet service provider. Then from the internet service provider it comes to the platform provider which takes care of functionalities such as device management, user management, data analytics and user access. And then again through a RESTful architecture interface you know it is sent to the service providers and the users and the corresponding business model is taken care of at this particular stage.

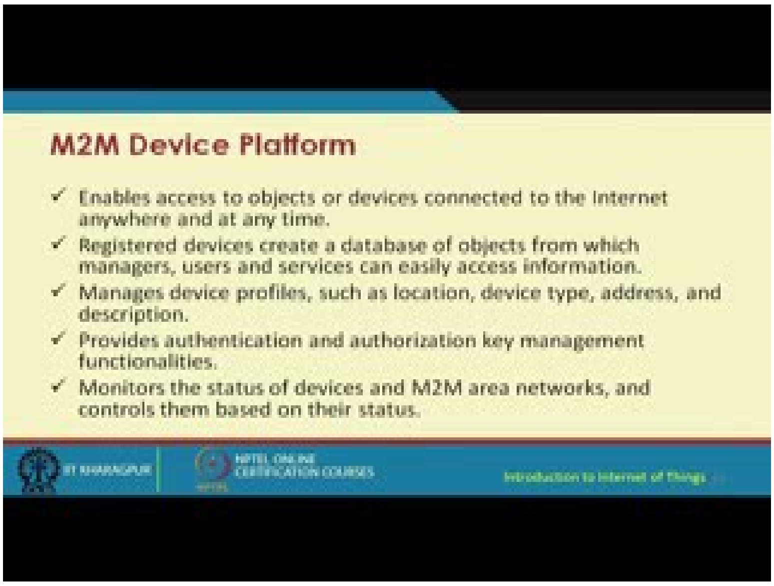
(Refer Slide Time: 14:48)



So, when we talk about this service platform we have the M2M service platform in short it is called the M2SP and in this M2M service platform we are talking about different functionalities of devices, different functionalities of users, different applications and access all these different functionalities right. So, functionalities with respect to device include the device profile management device and M2M network management and device searching. User profile management, authentication and charging are taken care of by the user. Data collection data control, service management, connection management by application. And app management, app searching web portal in the access control

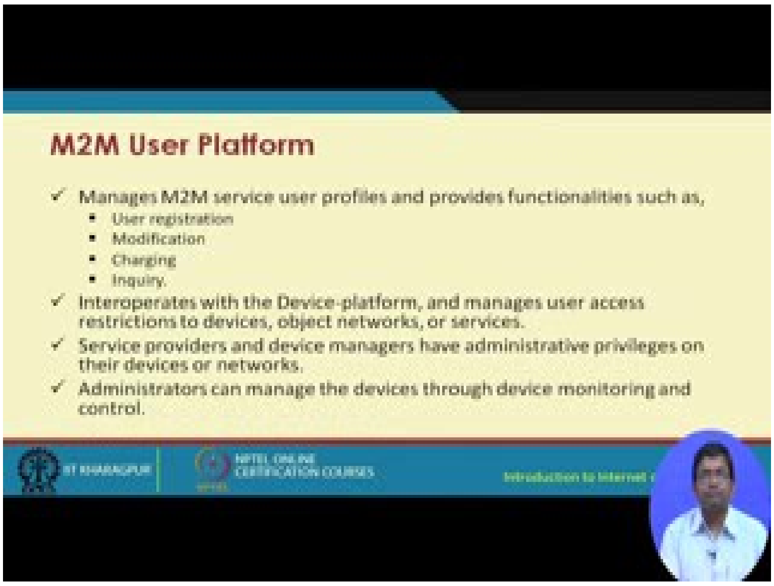
So, all these data are passed through an access network like Wi-Fi, ZigBee etcetera and are sent to the M2M area network. This is one possibility. The other possibility is that from this M2M area network and several such area networks these data are sent through the access network to the core network, which supports these platforms with respect to device, user, application and access. So, both way actually from here we can you know we can either think of it from here when towards the M2M area network or from the M2M area network towards the core network, we can think of both way communication taking place both way. So, the only the flow of the data is different. So, what type of data is flowing that is different.

(Refer Slide Time: 16:48)



So, when we talk about the device platform it enables access to objects or devices connected to the internet anywhere and at any time. The register devices create a database of objects from which the managers, users and services can easily access the information. The device platform manages the device profiles such as location, device type, address and description. It provides authentication and authorization key, management functionalities and monitors the status of devices and M2M area networks, and controls control them based on their status.

(Refer Slide Time: 17:25)

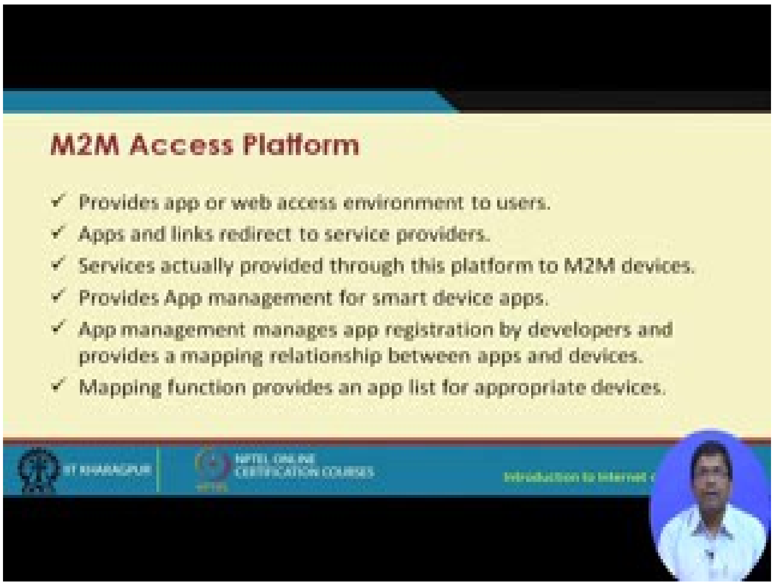


Now the user platform manages the M2M service user profiles and provides functionalities such as user registration, modification, charging, inquiry incorporate. In interoperates with the device platform and manages the user access restrictions to devices object networks or services. And service providers and device managers have administrative privileges privileges on their devices or networks .

(Refer Slide Time: 17:52)

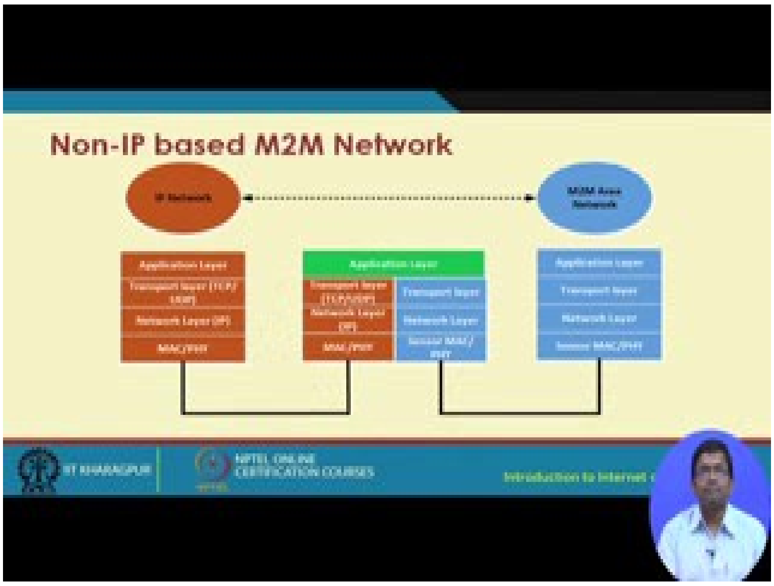
Application platform provides integrated services based on the device collected data. And the heterogeneous data merging is done in this particular platform. From various devices the data that is obtained are used for creating new services.

(Refer Slide Time: 18:11)



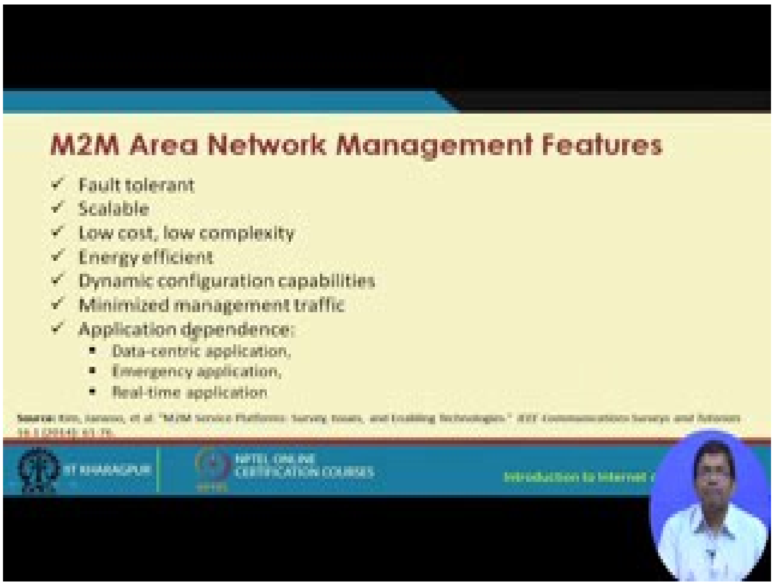
Access platform basically provides app or web access environment to users. The apps and the links redirect to the service providers the services are actually provided through this platform to the M2M devices. And this access platform provides the app management for smart device apps.

(Refer Slide Time: 18:30)



So, this is a scenario of non-IP based M2M network. So, here what we see is as you can see over here we have a non-IP based M2M network M2M area network and here we see an IP based network. And this application layer basically seamlessly integrates these two application layer basically seamlessly integrates the IP network and the M2M network in this manner.

(Refer Slide Time: 19:25)



Then we have the IP based M2M network where everything was as usual. So, we have the same set of layers application layer transport layer network layer sensor or MAC layer. And this is the same all across M2M area network management features are like this that fault tolerance is a very important if there is some fault system is going to take care of it automatically scalability is another important issue or feature of network management of M2M area networks. And so, basically new when we increase the number of nodes M2M nodes or IoT nodes you know that basically does not affect the efficiency quite significantly. So, efficiency is taken care of you know it still remains efficient. Low cost and low complexity are other features if we energy efficiency, configuration capabilities, dynamic configuration capabilities then minimized network management traffic and these are the ones which are important features of M2M area network management.

So, with this we come to an end of understanding more about the basic features of M2M communication. M2M as I said at the outset is one of the important enabling technologies for internet of things and building of IoT based systems. And so, in M2M we are talking about two or more machines you know communicating with one another with minimal or no human intervention at all. So, this as I said is a very important technology for building of internet of things.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

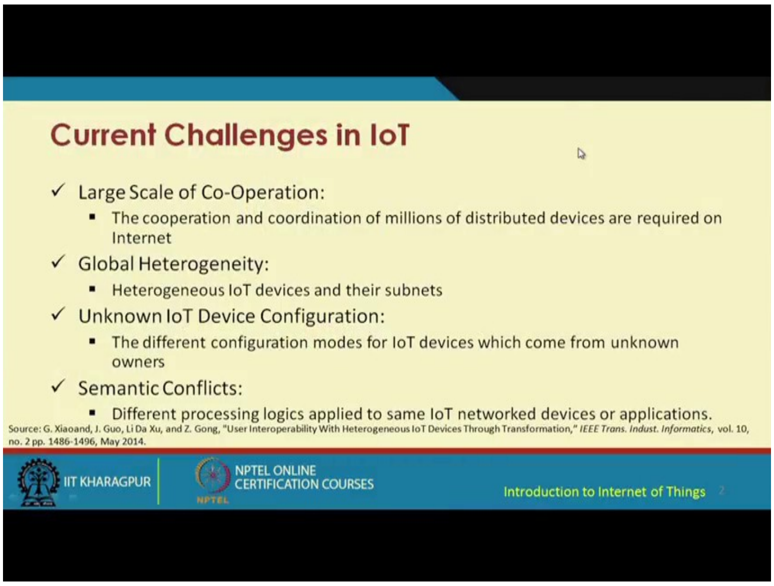
Lecture - 21
Interoperability in Internet of Things

This topic is on interoperability in internet of things. Internet of things uses different types of devices. These devices are made by different vendors following different specifications; there is no one standard for IOT. So, consequently what happens is for different things the different IoT devices are made by different vendors following different specifications. Again these different devices by different vendors they follow different protocols not necessarily that they all follow the same protocol. Even the kind of users their user profiles these can also be different. So, there is so much of diversity that is inherent to these systems IoT systems and that is why it is very important to address this particular issue.

In internet of things one of the core problems or issues that has been studied quite extensively is heterogeneity of devices, protocols, user groups and many other heterogeneity aspects in from different other angles. So, this has been studied quite extensively. And one of the requirements to handle this heterogeneity issue is basically to have some kind of interoperability interoperability between these different heterogeneous aspects. Interoperability means what that let us say that one particular device is following a particular protocol; another device follows another protocol. So, how do they talk to each other they speak the different language they speak language. So, they do not speak the same language. So, how do they talk to each other, this is one aspect.

Similarly, at different physical levels, different specifications, different devices how do they talk to each other, they all have been made in different ways because there is no one standard that has been followed in developing these systems. So, when you want to build a singular IoT system comprising of all these different heterogeneous objects, devices, protocols, standards etcetera you need to have some kind of handshaking. And that handshaking is where these protocols have been devised which can be some kind of a middleman a middleware rather which can help these two different diverse groups to be able to talk to each other.

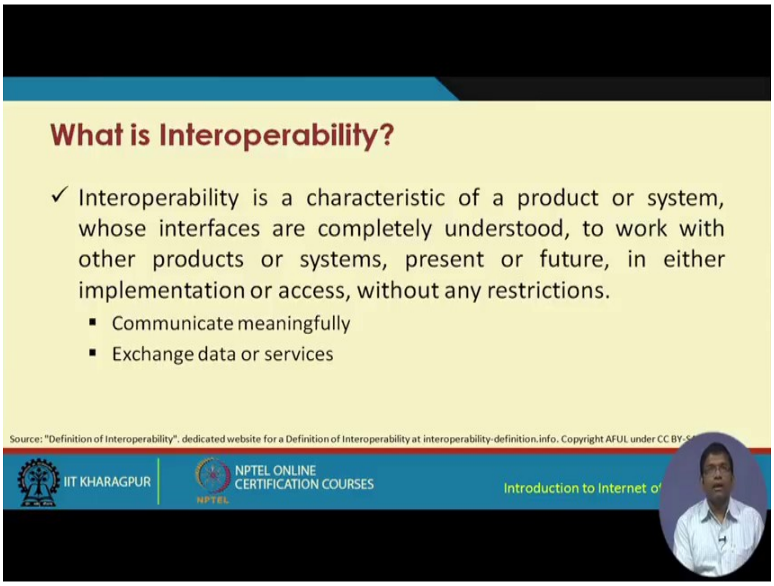
(Refer Slide Time: 03:30)



So, let us try to understand the interoperable interoperability issue in further detail. So, when we talk about IoT we are talking about large scale networks. Large scale networks requiring the use of large number of different devices millions and billions of devices, these devices are distributed all across in the internet or all across in the world. And what is required is to have some kind of cooperation between the different devices, some kind of coordination mechanism to be enforced between these different devices to be able to talk to each other. So, this is one issue.

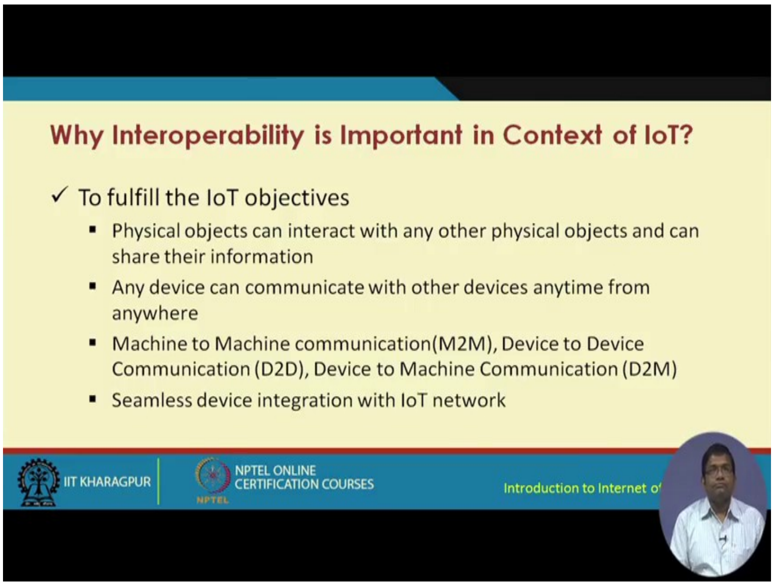
Second issue is that the devices as I was telling you before they all have been designed with different specifications heterogeneous in all respects in the physical device level, in the protocol level, user level, so in all different aspects. So, heterogeneous IoT devices and their subnets is a challenge that has to be worked on in the context of internet of things. Another very typical concern that is specific of IoT is the device configuration. Typically these IoT devices their configuration is unknown, unknown all across. The different configuration modes for IoT devices come from unknown owners and that is you know inherently that brings in lot of complexity and that has to be handled. Another very interesting complexity is how do you handle handle differences in semantics how do you handle differences in semantics not only so there could be conflicting semantics as well. So, different processing logics are applied to the same IoT network devices or applications by different developers, different user groups and so on. So, how do you handle these differences this conflicts in the semantics.

(Refer Slide Time: 05:40)



So, what is interoperability? Interoperability is a characteristic of a product or system whose interfaces are completely understood to work with other products or systems present or future in either implementation or access without any restrictions. I think this is quite understood in the backdrop of what we have discussed so far. So, what is required is to have all these different units devices protocols etcetera, etcetera that I was mentioning before to be able to communicate meaningfully. So, that there is exchange of data, exchange of services and to the user it should the interoperability has to be handled in such a manner that to the user the user should feel that he or she is getting access to the services of the IoT system in a seamless manner. The user should not have to get into how these are implemented what is the translation that is going so on and so forth.

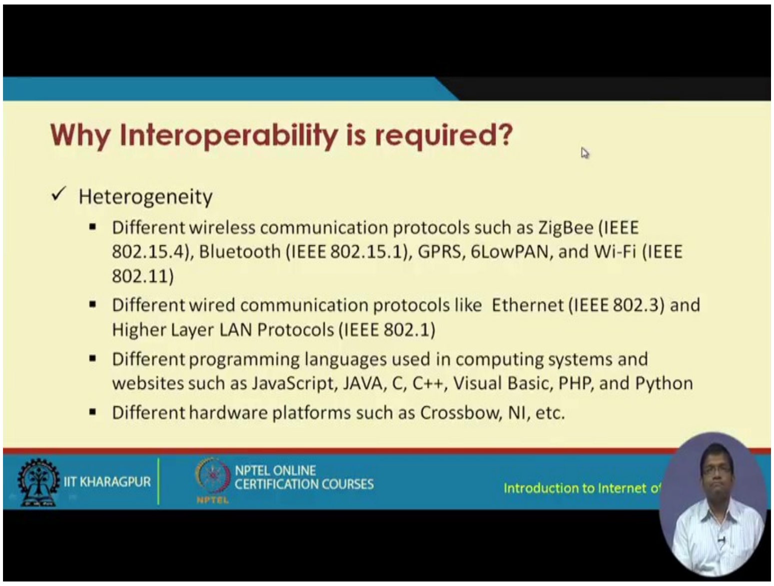
(Refer Slide Time: 06:53)



So, what why interoperability is important in the context of IoT because it is required to fulfill different IoT objectives, seamless device is what I was mentioning, physical objects would have to interact with other physical objects for sharing information, any device can communicate with any other device at any time and at anywhere. So, devices communicating anytime, anywhere and any kind of device that means, anything, anytime anywhere communication, right. So, if we have to have anything, anytime, anywhere communication then obviously we need to handle this problem, so that is the reason why heterogeneity and interoperability are the core issues of IoT that has to be addressed before large scale IoTs are made functional.

Issues such as machine to machine communication, device to device communication. So, machine to machine communication we have already gone through. And then we have the device to device communication. In device to device communication it is basically a standard in the LTE advanced and so where basically one mobile phone talk talking directly to another mobile phone you know that is addressed. And then you have the device to machine communication. So, we have M2M, D2D and D2M communication. And there has to be seamless device integration all across in the IoT network.

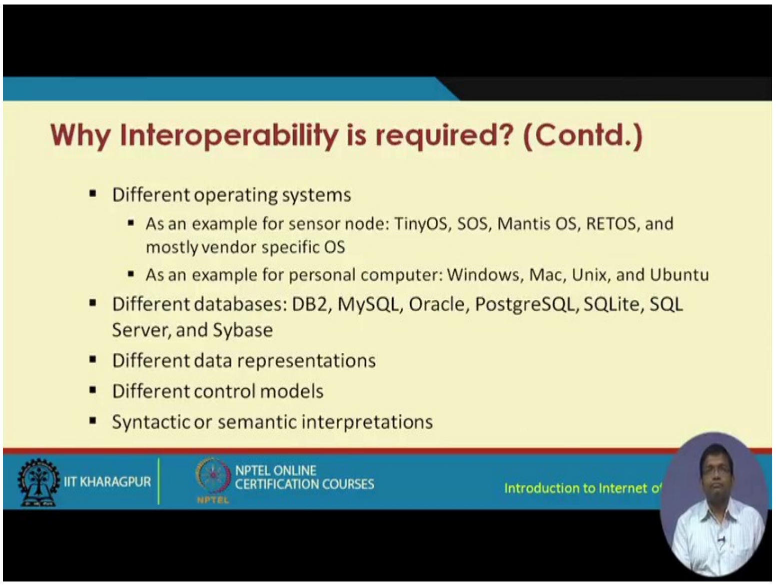
(Refer Slide Time: 08:28)



Heterogeneity - different communication protocols ZigBee following IEEE802.15.4 which we have discussed before. Bluetooth following 802.15.1, GPRS, 6LowPAN, Wi-Fi which follows 802.11 standard. So, all these different types of standards all different types of communication protocols handshaking with each other, communicating with each other. Different wired communication protocols such as 802.3 and 802.1 talking to each other that is required because otherwise we cannot have this seamless you know anytime, anywhere, any device connectivity that is not going to be possible. So, so much of heterogeneity is going to be there all across.

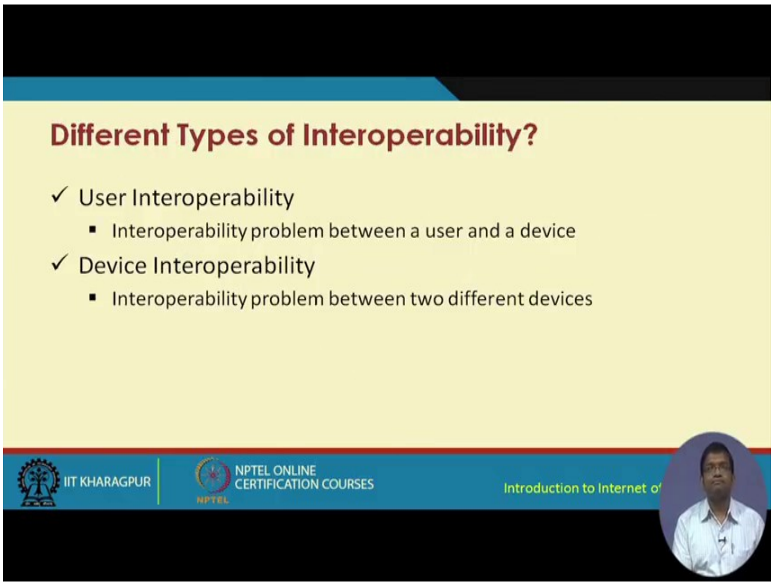
Then different programming languages are used in different computing systems for example, JavaScript in one, Java in another, C, C++, Visual Basic, PHP, python, so many different programming languages platforms of different kinds are used. Again there are different hardware platforms as well not just programming platforms in the hardware platforms such as crossbow based products talking to national instrument products talking to Cisco products and so on. So, all these hardware platforms can also be varying they you know different types of heterogeneous hardware platforms. So, interoperability is very much required in this kind of backdrop.

(Refer Slide Time: 10:06)



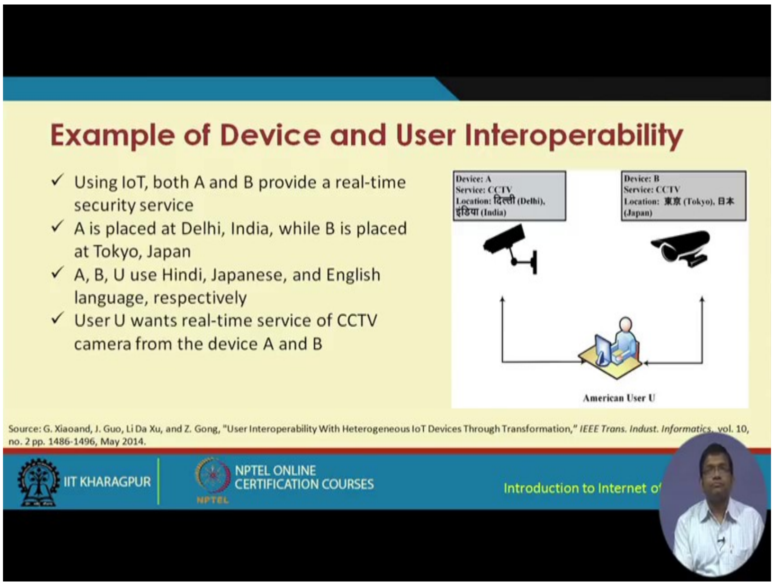
Further when we talk about operating systems for a sensor node some sensor nodes have implemented TinyOS, some SOS, some Mantis OS, some RETOS, and some could be even implementing some vendor specific operating system. And from a user point of view some PCs, for example, might be implementing might be using the Windows OS some MAC OS, some Unix, some Linux, some Ubuntu. So, all these different types of operating system from the device or sensor node point of view as well as the user point of view then different databases - DB 2, MySQL, Oracle, PostgreSQL, SQLite, SQL server, Sybase all these different, different different databases are implemented all across. Different data representations as well the way the data is represented very hard to handle this kind of heterogeneity then different control models, different syntaxes, semantics and so on. So, these have to be handled.

(Refer Slide Time: 11:19)



So, what is required is to have different types of interoperability, and these interopretability issues of different types have to be handled in different ways. User interoperability is between a user and a device. Device interoperability is between two different devices.

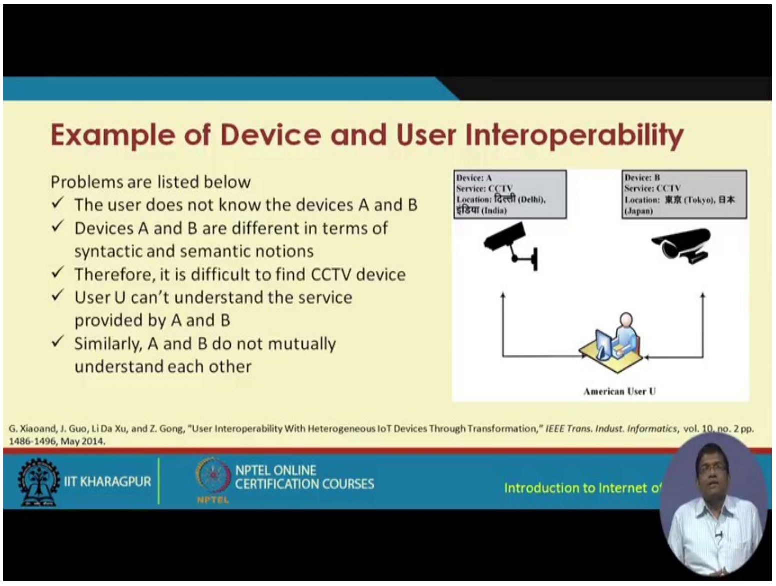
(Refer Slide Time: 11:47)



So, the issues are different user and device, device and device, so how do you handle, right. Now let us take an example to understand why user interoperability is so important. Let us say that there are two devices, one is located a CCTV for example, in this figure which is installed in Delhi. And as you can see that it is also the location it is written in different language. The other device which is another CCTV is located in Tokyo and you know it is its specification sets, not specifications, but you know the device level semantics are handled in Japanese language. And then there is an IoT user who is based in America US.

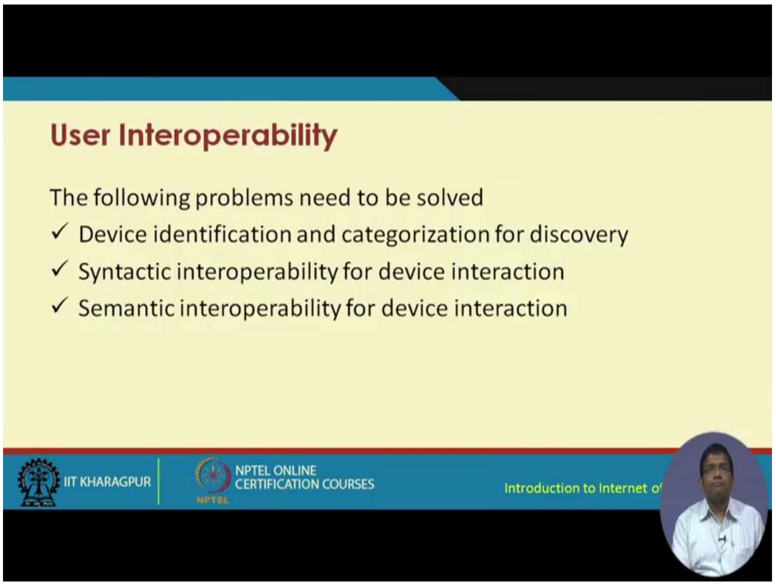
So, this American user has to operate both of these devices remotely from America and this is what IoT does, this is what IoT does that remotely how you can monitor different devices you know the end you know which could be end not only that different devices, but these devices might be themselves located quite far apart. So, using IoT both A and B provide real time security service in this particular example A is placed at Delhi, whereas B is placed in Tokyo. So, A, B and U India, Japan, America, they all use different languages Hindi, Japanese, English respectively. So, user U in America wants real-time service of CCTV camera from the devices A and B.

(Refer Slide Time: 13:45)



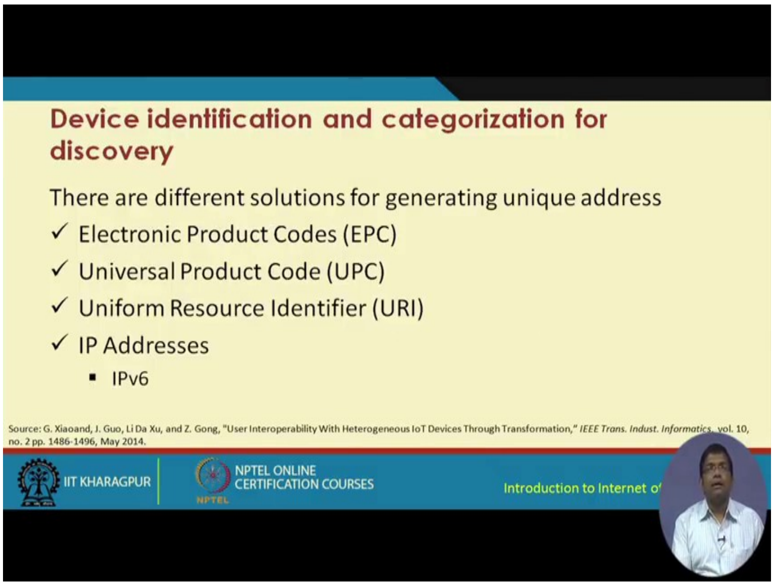
So, what are the problems that are going to happen? Number one the user does not know the devices A and B user does not know the devices A and B. Number two problem devices A and B are different in terms of syntaxes and semantics and this is this is what I was telling you just a minute back. Therefore, it is difficult to find the CCTV device user you cannot understand the service provided by A and B because of the language difference, and similarly A and B do not mutually understand each other for the same reason. So, you see that differences in syntaxes, differences in semantics, differences differences in the user specifications, all these are bringing in lot of complexity for a simple basic problem that is code to IoT.

(Refer Slide Time: 14:43)



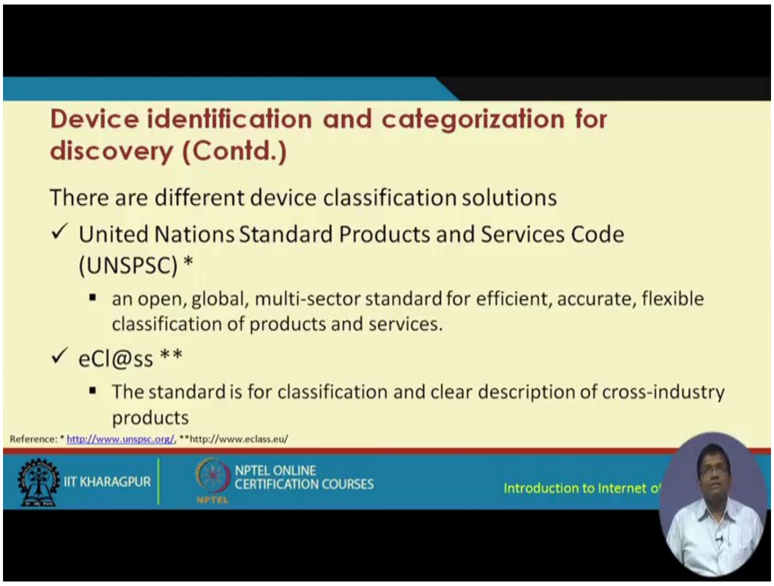
The following problems need to be solved. Number one the device has to be identified and it has to be categorized. So, device identification and categorization for discovery because for discovery you need to have need to identify the device and you need to categorize the device as what type of device whether it is a CCTV device or some other type of device. And you have to also identify the device and there is language issues between these different locations, syntactic interoperability for device integration and semantic interpretability for device interaction. So, these are the different differences in the device level, syntactic level and semantic level that have to be handled by the user. And you see that when we are talking about user interoperability, we have these different device you know different users some user you know using a different syntax, another user using another syntax or semantics or language and the corresponding knowledge basis are also different the devices are also different. So, how do these two users talk to one another this is what user interoperability tries to address.

(Refer Slide Time: 16:02)



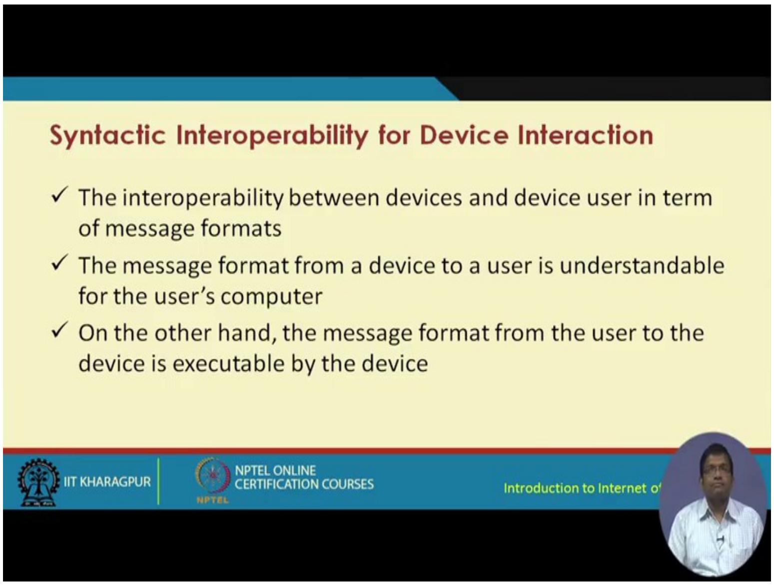
So, for device identification categorization for discovery, there are different solutions for generating unique addresses. So, these includes the EPC - electronic product code, universal product code – UPC, universal resource identifier – URI, and IPv6 the traditional IPv6 based addressing as well.

(Refer Slide Time: 16:28)



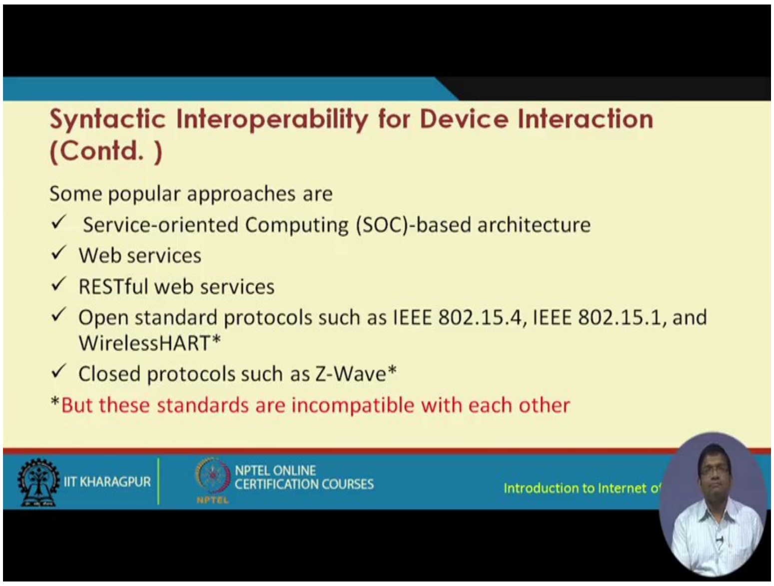
So, there are different device classification solutions and there are two of them that are quite popular one is the UNSPSC which is united nations standards standard products and services code which is an open global multi sector standard for efficient accurate flexible classification of products and services. And the other one is the eCl@ss which is the standard for classification and clear description of cross industry products.

(Refer Slide Time: 17:01)



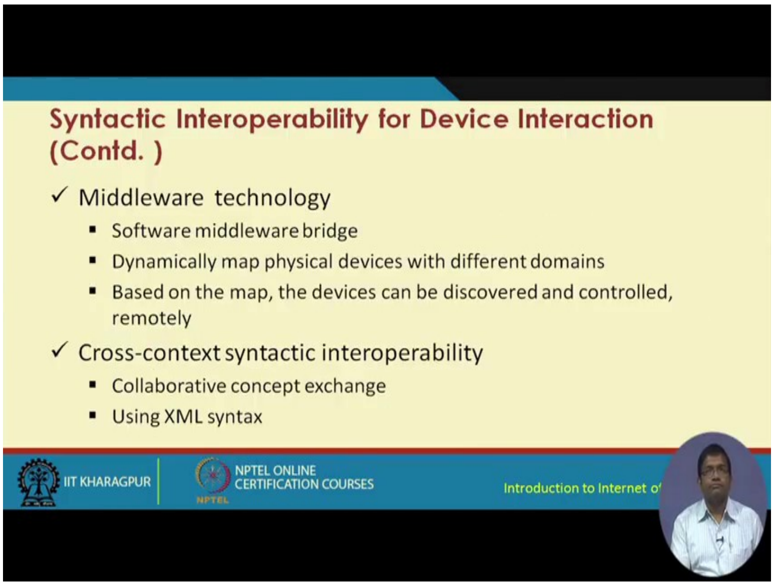
Next comes the syntactic interoperability for device interaction the interoperability between devices and device user in terms of message formats is what is the concern of this type of interoperability. The message format from a device to a user is understandable for the user's computer. On the other hand the message format from the user to the device is executable by the device.

(Refer Slide Time: 17:32)



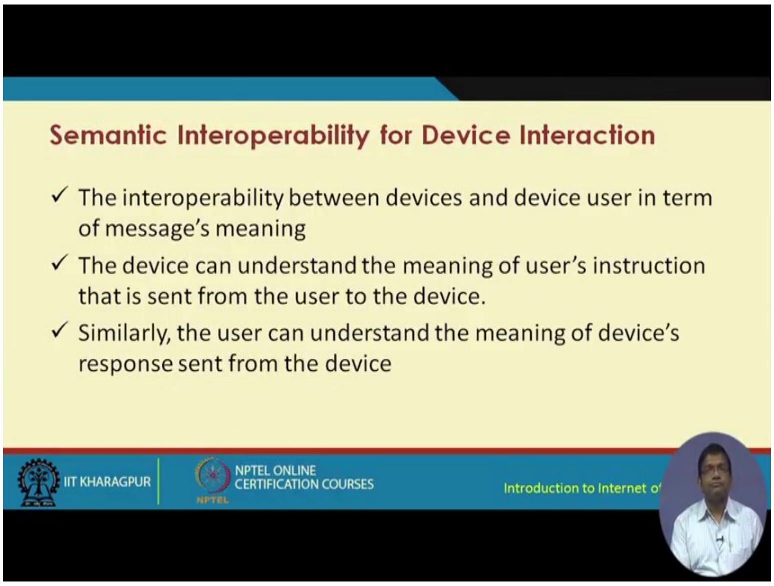
Some popular approaches are service oriented computing SOC based architecture. Then web services using web services RESTful web services, which is quite popular for IoT. So, rest architecture, and the RESTful architecture and the corresponding RESTful web services. Open following some open standard protocols such as 802.15.4, 802.15.1, WirelessHART and then following some closed protocols such as Z-wave. But we have to keep in mind that Z-wave is proprietary and this is a you know proprietary closed protocol not a standard protocol and that is why you know Z-wave devices will talk with Z-wave devices, whereas you know those which follow the WirelessHART you know they can talk to each other.

(Refer Slide Time: 18:31)



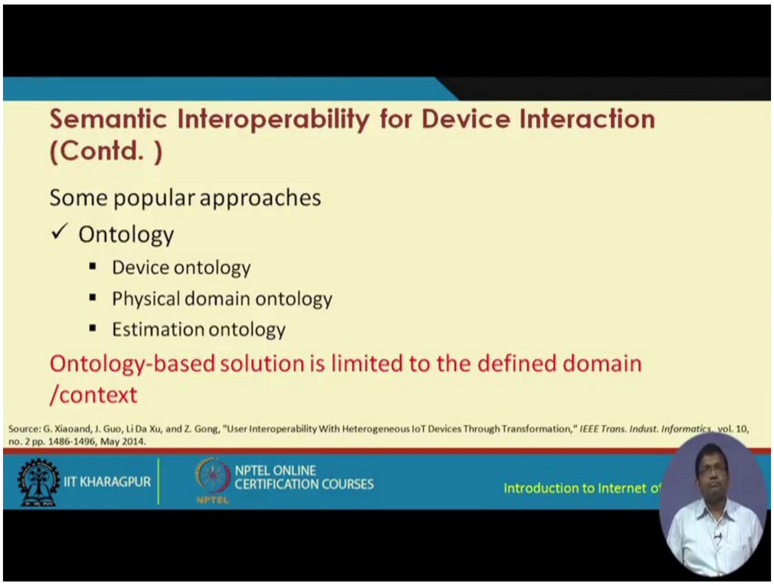
Middleware technology, so this middleware technology is sort of like a software middleware bridge, which dynamically maps the physical devices with the different domains and based on the map the devices can be discovered and controlled remotely. Then we have the cross context syntactic interoperability, which concerns collaborative concept exchange and using XML syntax.

(Refer Slide Time: 18:59)



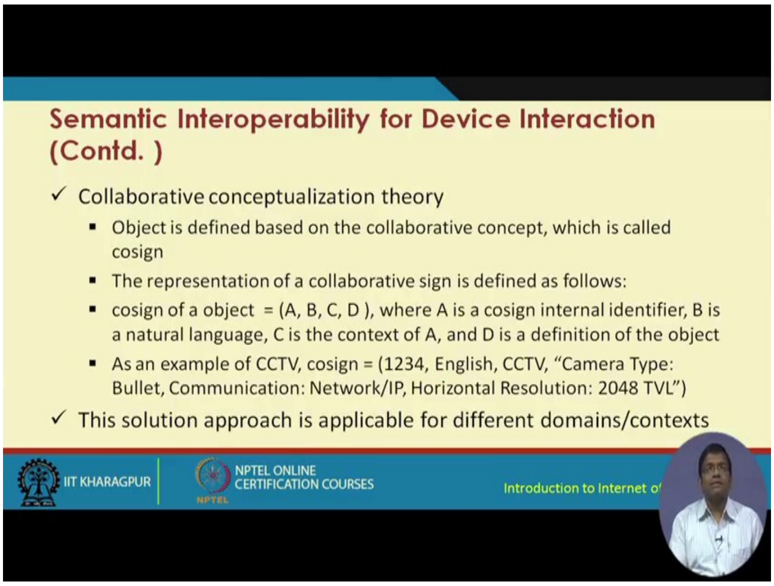
Now, semantic interoperability for device interaction; and here we are talking about the semantics, semantics and the exchange of the semantics. So, the messages that are sent between these different devices whether they are understood by the respective party if not there has to be some middleware in between which has to make it happen. So, the device can understand the meaning of users instructions that is sent from the user to the device, similarly the user can understand the meaning of devices response sent from the device.

(Refer Slide Time: 19:41)



So, some of the popular approaches are ontology based approach number one which again can be classified as device ontology, physical domain ontology and estimation based ontology. Device so, ontology means what some kind of a knowledge base. So, device ontology basically is you know the knowledge base about devices. So, this is required, you know so if two devices have to talk to each other, so the ontology the corresponding knowledge basis of these different devices have to be formed. Physical domain in ontology I do not need to elaborate this further, so you know so knowledge base about the physical domains of operation. And estimation ontology is about you know based on the previous data estimating what is going to happen, so that sort of rule, rule base has to be maintained in some kind of a knowledge base. So, this is estimation ontology. So, ontology based solution is limited to the defined domain or context.

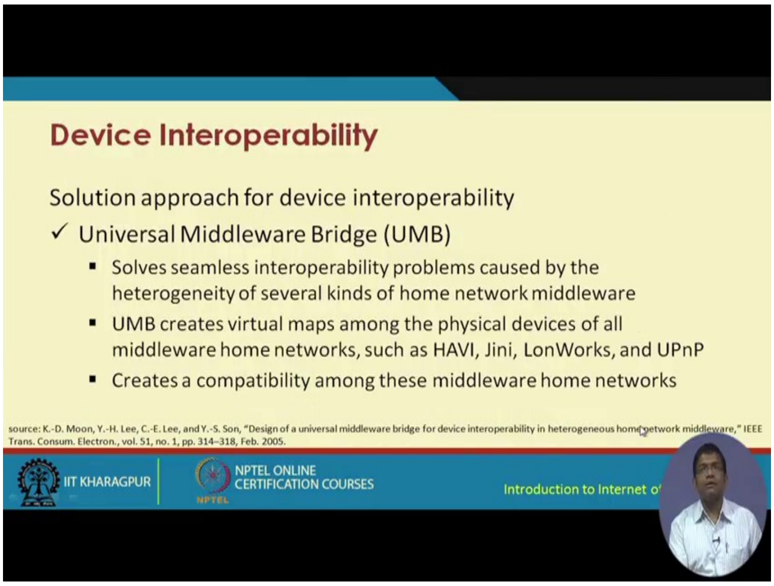
(Refer Slide Time: 20:44)



So that is the reason why there is one theory which is known as the collaborative conceptualization theory that was proposed. So, the object is defined based on this particular collaborative concept which is also known as the cosign concept, cosign is the short form of collaborative sign. So, cosign of an object is defined as a quadruple A, B, C, D where A is the cosign internal identifier, B is the natural language, C is the context of A, and D is the definition of the object.

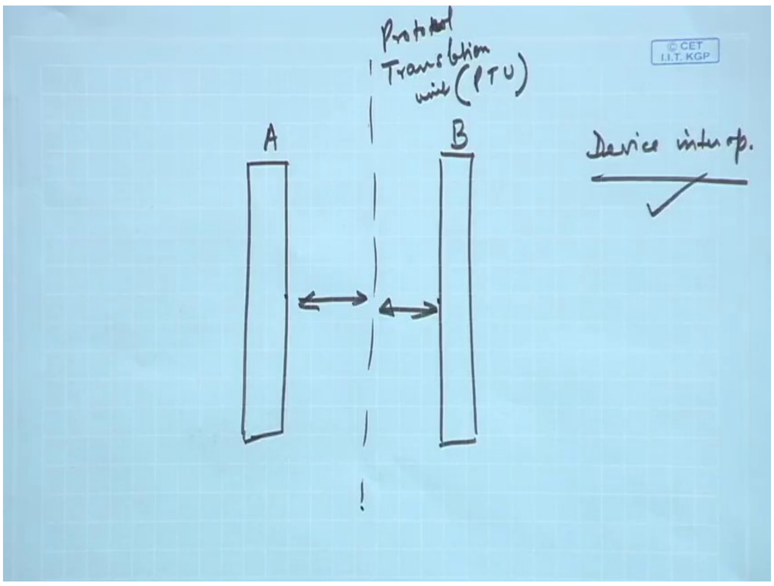
So, in our CCTV example the cosign of the CCTV is equal to 1234 which is some kind of an identifier for this CCTV object, English is the natural language that is used, C is the context of A that means, here it is CCTV the CCTV is the context and D is the definition of the object. So, here we have camera type bullet camera type equal to bullet communication equal to network or IP and horizontal resolution equal 2048 TVL. So, this is basically the definition of the object with respect to this particular specification. So, this solution approach is applicable for different domains and contexts.

(Refer Slide Time: 22:08)



Now, about device interoperability let us try to understand before we go any further how this is going to work.

(Refer Slide Time: 22:28)

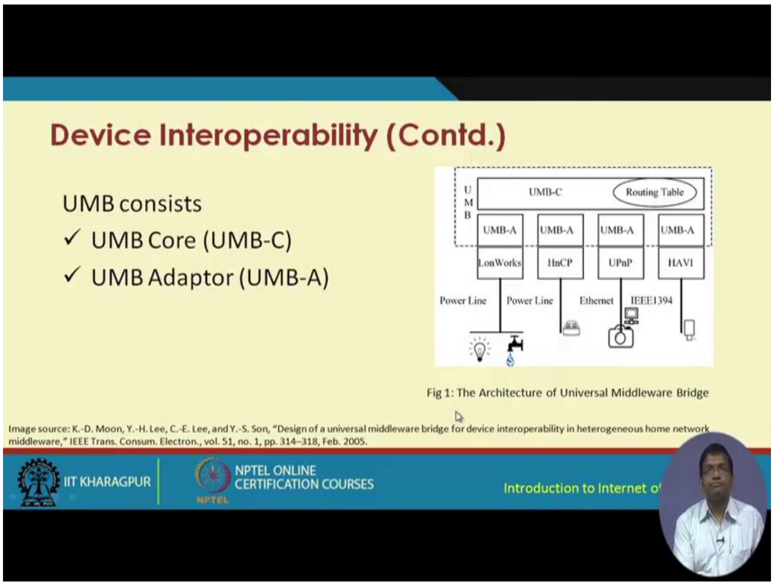


Let us say that even before we start with the device interoperability, let us say that we have you know two devices: device A and device B. And in our example let us assume that A and B as such do not follow the same specific same protocol, they did not have the same specifications at the physical layer or you know the other layers. So, no common protocol is available across all these different layers. So, how do they communicate how do they communicate. So, this is the problem of device interoperability. So, how do they communicate.

So, let us assume initially that we have some kind of a middleware some kind of a middleware, which will understand the language of A and the language of B. So, it will understand the language of A as well as the language of B. So, this will help this one to be able to translate what A is saying A wants to send, he wants to communicate, and similarly what B is say. So, this sort of approach not only can be used for device interoperability, but also other forms of interoperability as well. So, this one basically becomes a translation device translation unit. So, if we are talking about two different protocols we can call it as a protocol translation unit - PTU. So, this protocol translation unit will translate the protocols separate protocols or the languages that are followed by both, ok. So, this is an approach that can be adopted and can be extended for similar other situations as well.

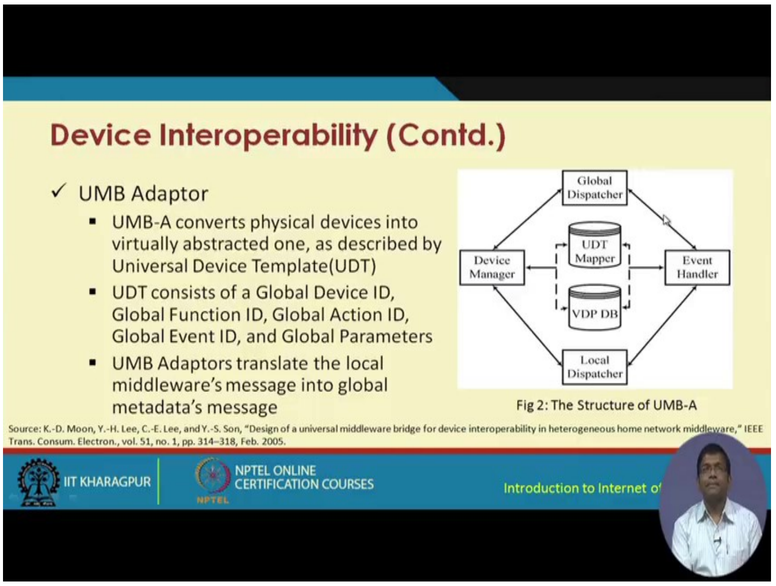
So, we talked about in device interoperability we talked about some kind of a universal middleware bridge which solves seamless interoperability problems caused by heterogeneity of several kinds of home network middleware. So, this bridge is basically it is a middleware that creates a virtual map among the physical devices of all middleware home networks such as HAVI, Jinl, LonWorks, UPnP and so on. And it creates a compatibility among these middleware home networks. So, it is basically some middleware based solution this middleware will act as an agent for this kind of translation or handshaking between two different heterogeneous devices.

(Refer Slide Time: 25:42)



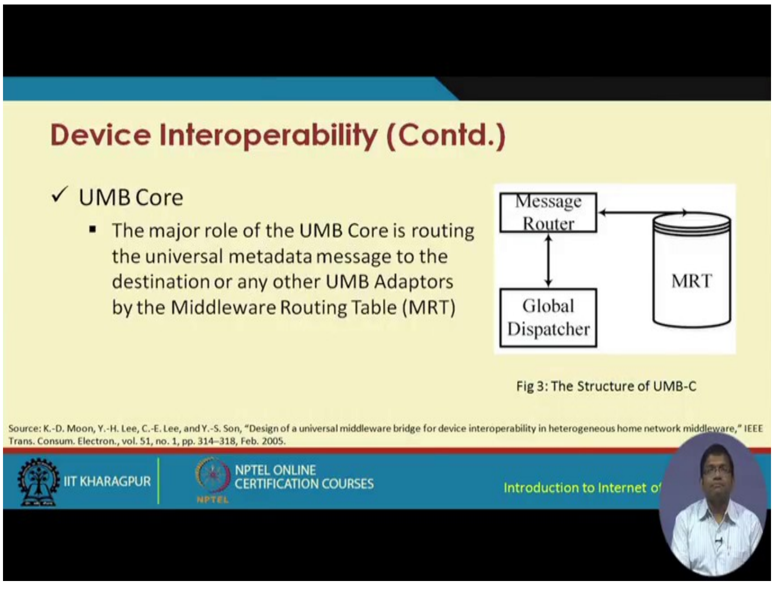
So, in device interoperability we have two parts the UMB core and the UMB adaptor. So, this is let us say that physically these are the devices. So, physically these are the devices, we have a lamp, we have an water tap, we have a camera, we have a computer and so on. So, these are the physical devices and they have to be internetworked together. And let us say that they have they are completely heterogeneous, they do not you know talk to each other as such. So, this is what is going to happen, this is what is going to happen. We are going to create a UMB socket we are going to create a UMB socket with different adaptors like this, which will fit into these ones which are the abstractions of these physical devices. So, these adaptors would fit to these abstractions fit to the abstractions of these devices and that is how this communication is going to take place. So, this is the function of the adaptor. Then what is this UMB-C the code does what it does is it basically helps in communication dissemination of the data between these different adaptors using with the help of Routing tables.

(Refer Slide Time: 27:15)



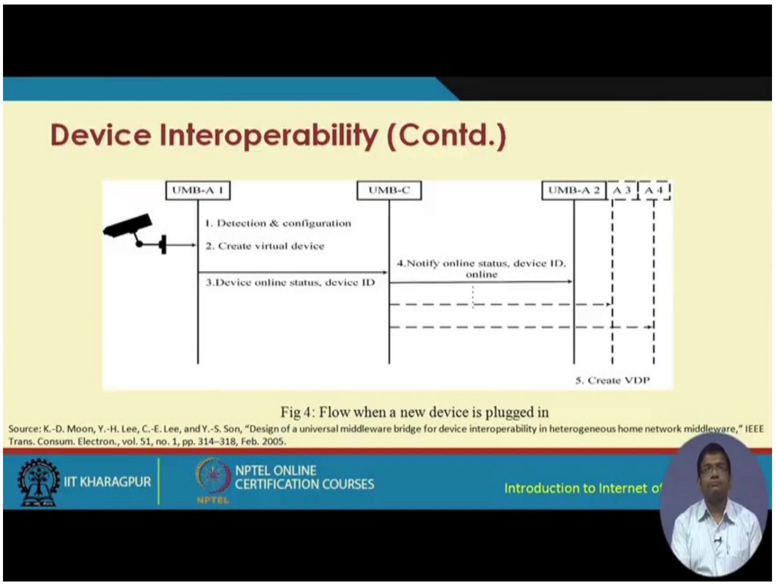
So, the adaptor basically converts the physical devices into some virtual abstractions and this is done with the help of something known as the universal device template. So, this universal device template or the UDT basically helps in coming up with the abstraction the virtual abstractions and that is stored in some kind of a database. So, this UDT mapper will come up with these virtual abstractions which are stored in the database and this UDT basically consists of the global device identifier, global function identifier, global action identifier, global event identifier and global parameters and the UMB adaptors translates the local middleware's message into the global metadata message.

(Refer Slide Time: 28:04)



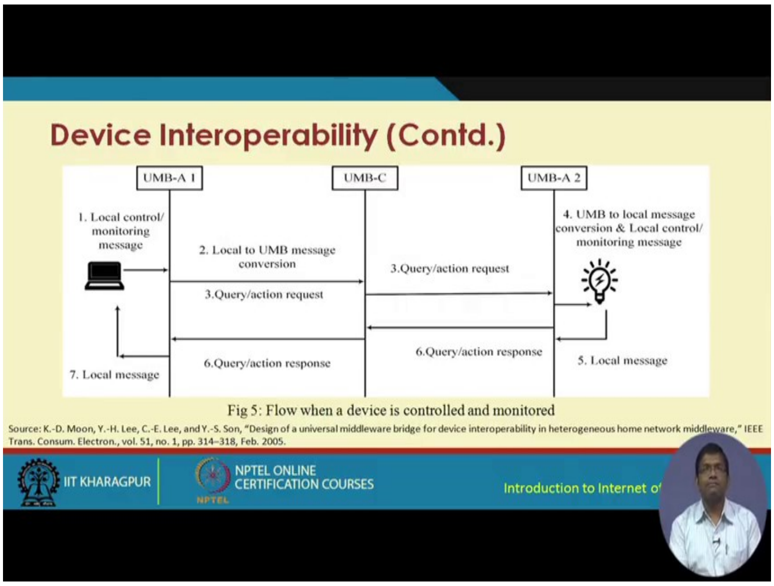
Now comes the core which is on top of the adaptor in that architecture. So, the core basically has the role of routing this is the main the most important role of the core. So, it uses something known as a middleware routing table; and from that from the middleware routing table with the help of the data that is residing in it, it creates the message router and from the message router we get the global dispatcher that information is basically used at the core to send the data between these different devices.

(Refer Slide Time: 28:47)



So, let us consider some few basic scenarios we have this particular device connected to this adaptor it detects and in first it has to detect and it has to configure then it creates some virtual device. So, then the device online status the device ID etcetera are sent across from the adaptor to the core and then from the core this message is sent to another adaptor notifying the online status the device ID and ID and whether it is online or not and it is sent to another adaptor, third adaptor, fourth adaptor and so on. So, this is how communication using UMB-A and UMB-C takes place between two heterogeneous devices following different configurations.

(Refer Slide Time: 29:54)



Now, let us look at a scenario when the device is controlled and monitored. So, we have UMB-A 1, then UMB-C and UMB-A 2. So, this, the first message let us say that these two would have to be talking to each other. So, this one has to control this and this has to be monitored right. So, the local control or monitoring message is first sent from the device to the adaptor A 1, then the local to UMB message conversion takes place then it is sent to the UMB-C. Then from here a query or action request is sent to the second adaptor and then the UMB is used to local message conversion for local message conversion and local control or monitoring message. Then this local message is sent to this particular adaptor from the device then a response is sent back another response is sent back and the local message is delivered to this particular device.

So, we have thus come to the end of how the communication using adaptors happen in the context of interoperability in internet of things. So, we have seen that in this interoperability architecture, we have two types of components one is the adaptor which basically is a virtual or software abstraction of the actual physical device. And this you know this abstracted virtual or softwarized device talks to other similar kind of abstracted devices with the help of this particular core the UMB-C. And this is how the communication takes place across different heterogeneous devices in internet of things.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 22
Introduction to Arduino- I

So, in this lecture we are going to get some hands on of ardunio programming, so this lecture and the next one as well. So, two lectures are completely devoted to ardunio programming. So, in the first lecture, you are going to get some of the ideas about the basics of arduino and in the second one some of the examples about how the programming can be done with ardunio. So, before we proceed further I would like to remind you a few things that ardunio is very much popular. At present it is used in for different implementations of IoT throughout the world arduino devices are very much cheap, they are low resource consuming and that is why they are very much popular for use in implementation of internet of things.

So, in the first module, we have seen different things we have understood the concepts of internet of things, basic concepts the overall philosophy of internet of things. We have also seen that there are different types of sensors, different types of sensing possible, different types of actuators that principles behind different types of sensing, different types of actuation. We have seen that there are different types of networks that are possible for use for adoption for use in IoT, different types of communication devices standards can also be used for communicating in internet of things.

So, having understood those how can we use these concepts for building a real internet of things may be in a smart phone scenario at home to improve some of the you know daily tasks that we do at home. Or in a smart homes smart cities scenario like in a smart hospital smart you know smart transportation connected vehicles and so on. So, of are all these we need to take help of different IoT devices. And one of the very popular once is arduino. So, arduino if you have to use for the building of internet of things, you have to you have to buy this which are very cheap and then you have to program these and this is what I am going to teach you in this particular course.

So, with me actually I have Mr. Anandroop Mukharjee who is going take over and Mr. Mukharjee is going to take you through the hands on of arduino programming through the from the starting from the basics to the little bit moderately advance concepts of arduino programming.

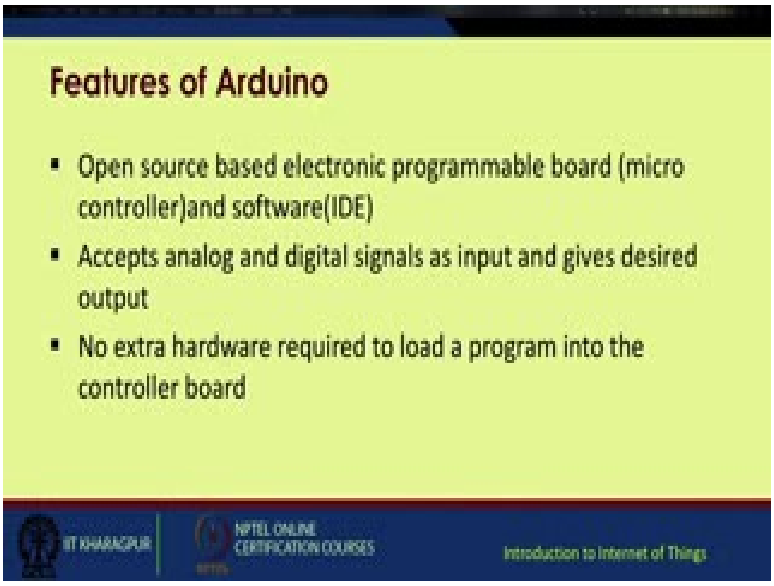
(Refer Slide Time: 03:33)

.

So, I would like to show you first how a arduino device looks like. So, this is the arduino UNO. So, arduino UNO, arduino has different variants they all have different you know differences in specifications and so on. So, this is the arduino UNO. And this is this device that has to be program, this has to be programmed. As you can see over here this is very small in size and it can be very much integrated with this internet of things you know when you are trying to implement internet of things it can be implemented on top. So, this device actually you know the difference sensors that you have you know learnt in this particular course.

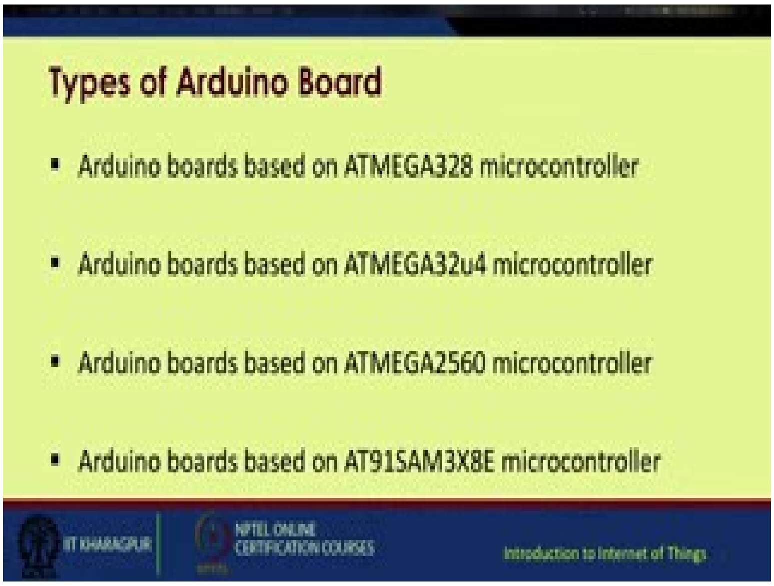
So, these different sensors can be fitted to this device, the different actuators can be fitted to this device, and this sensors the different sensors and the different actuators in after fitting the data that is received from the sensors. These can be sent through the communication unit in this which Anandroop is going to talk about, and how this data can be disseminated and can be sent for further analytics further storage and so on.

(Refer Slide Time: 05:08)



Hello, I am Anandhroop Mukharjee. I am the TF for this course. I will be taking you through the basic features of arduino in this lecture. So, to start off with as you already have heard arduino has become very popular nowadays. So, first of all the main reasons is it is an open source programmable board with a built in microcontroller and the software IDE. And this software IDE will help you change the behavior of the microcontroller according to your needs. So, it accepts analog as well as digital signals which can be given as inputs and it will give outputs which are mainly digital. So, no extra hardware is required to load a program into the controller board. So, for the people who have work with 8051 series microcontrollers, 8085 microprocessors, they must have remembered that you needed an extra programmer to actually program the processor board and they are well lots of interfacing ICs and all those things are not required with the arduino base systems.

(Refer Slide Time: 06:02)

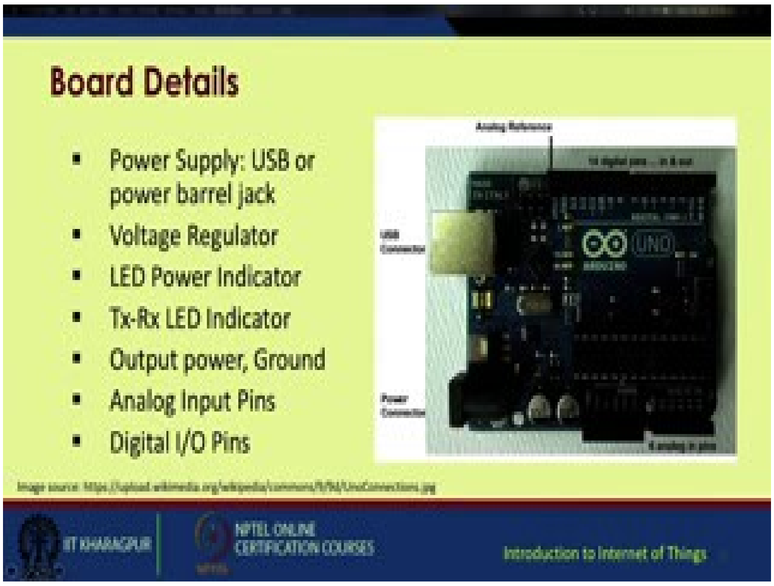


So, to start off with there are few basic variations of the arduino boards they have there are ATMEGA328 base microcontroller, they have ATMEGA32u4 four series microcontrollers, they have ATMEGA2560 series microcontrollers and then there are ATMEGA91SAM3X8E series microcontrollers. So, these are some of the core microcontrollers as you can see if you focus on this IC this arduino board, so we are using a UNO board to give a demonstration. So, this is the IC chip. And basically all the other once are either the voltage converters or interfacing ICs which are required for the input output functions with this ATMEGA series chip.

(Refer Slide Time: 06:57)

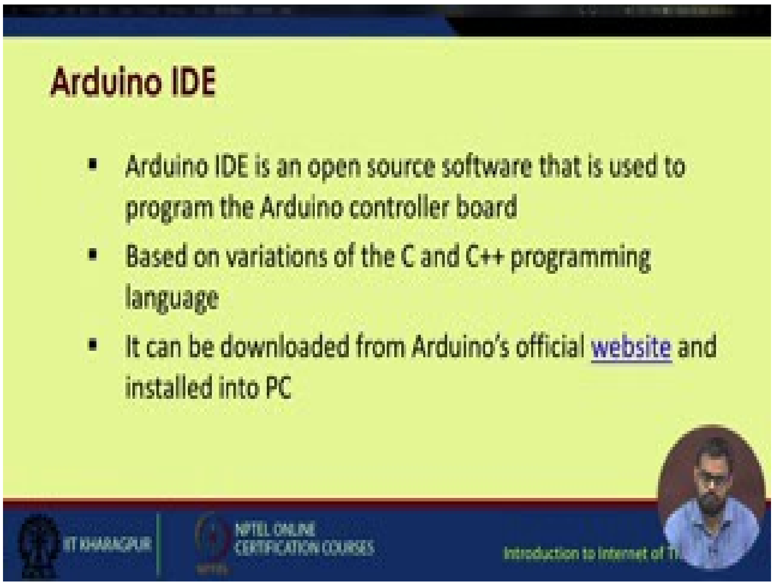
So, basic features of arduino UNO they operate at a voltage of five volt with the clock speed of 16 megahertz, and they have 14 normally arduino UNO has 14 digital input output pins, 6 analog input pins, 6 PWM pins, 1 UART that is universal asynchronous receiver and transmitter. And the interface is mainly via USB of ATMEGA16u2.

(Refer Slide Time: 07:26)



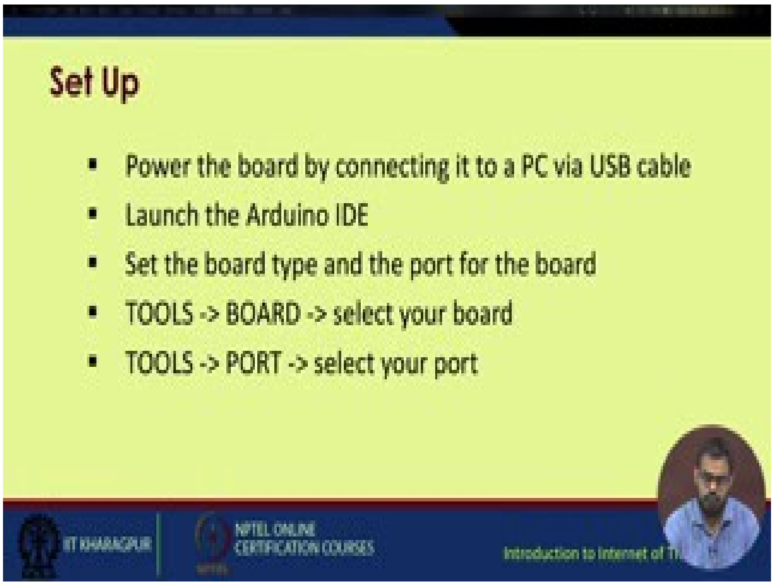
So, the board details are as you can see from this figure you have a USB connector to which you connector ATMEGA board to your PC it. The best thing about this is the interfacing is very easy you can connect your system arduino baseboard to a either a window base pc or a macintosh or Ubuntu or Linux base system. So, this is the USB connector then you have the power connector to power on the device in standalone mode; otherwise if you connected to a pc address power from the pc itself. And this is the analog reference pin you have 14 digital pins which can be used as input and output. As you can see starting from 0 to 13, these are the fourteen input output pins. And over here you have 6 analog pins A 0 to A 5 which can receive analog inputs and these are some of the power connectors you have 5 volt, 3.3 volt and ground connection and so on. So, these are just some of the basic components of the arduino.

(Refer Slide Time: 08:36)



Now, the arduino IDE is basically an open source software, the arduino system itself is an open source system, the hardware's specifications are available you can in fact, if you have fabrication facilities you can actually fabricate your own arduino device. So, this arduino IDE is an open source software that is used to program the arduino board. So, it is based on the variations of C and C plus plus programming languages and it can be freely downloaded from the arduinos official website.

(Refer Slide Time: 09:10)

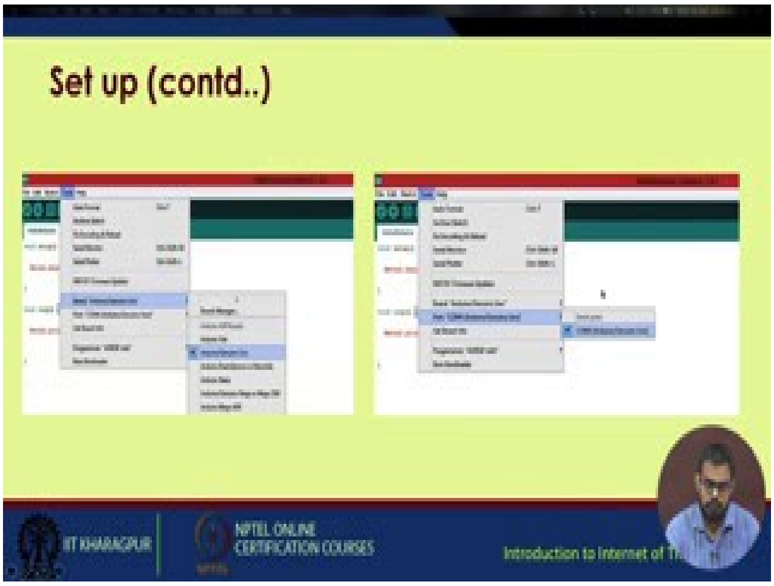


So, the basic set up is the power from the board is derive as you can see the power from the board is derive from the PC using the USB. So, if you are initially for testing purposes you will be connecting it to the PC to upload your program and when you are running at in standalone mode when your program has been uploaded on this board you can run it from this power supply input. You plug in a DC adapter of 5 volts and it is going to work fine Then next will launch the IDE then select the board type.

So, let me show you, so over here I have my arduino IDE. As you can see so you have some basic functionalities; this is the code verification button; this is code upload button. Then you have the file menu you can create a new sketch, a sketch is actually the program you write for an arduino then you can open an existing program open recent programs and so on. You even have examples basic examples provided with the IDE which can work with various arduino base board.

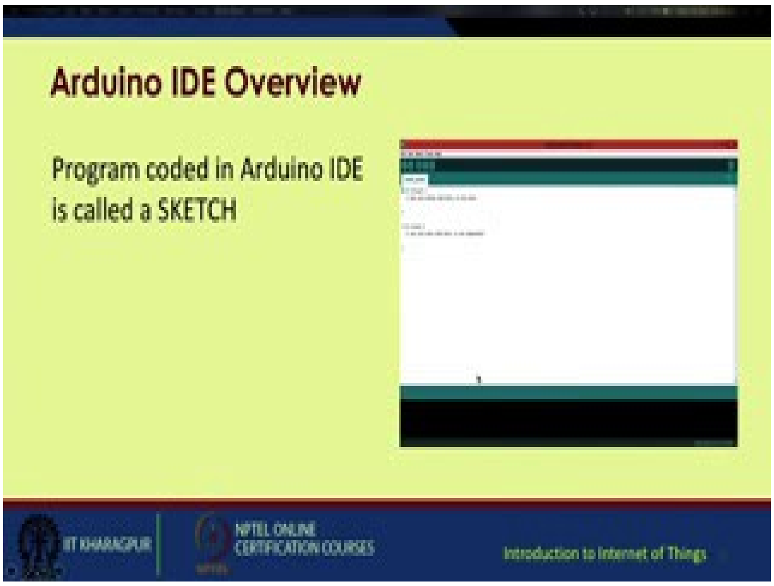
Now moving on to this sketch the most important part is this tool. Whenever you connect arduino board, so I have connected my arduino board to my PC. Now, from this tool these are the available boards you can see since I am using an arduino UNO it has been automatically selected, but in case it is not automatically selected you can choose the appropriate board arduino UNO. Now, for my MAC the port is already this USB modem 1421 you can see arduino UNO has already in selected. So, now, you are all set. One more important thing is over here you can see this button this is the serial monitor this is one of the good features are arduino that while executing serial programs, you do not need to have an external consoler that kind of software, you can just use the inbuilt serial monitor to view the program.

(Refer Slide Time: 11:55)



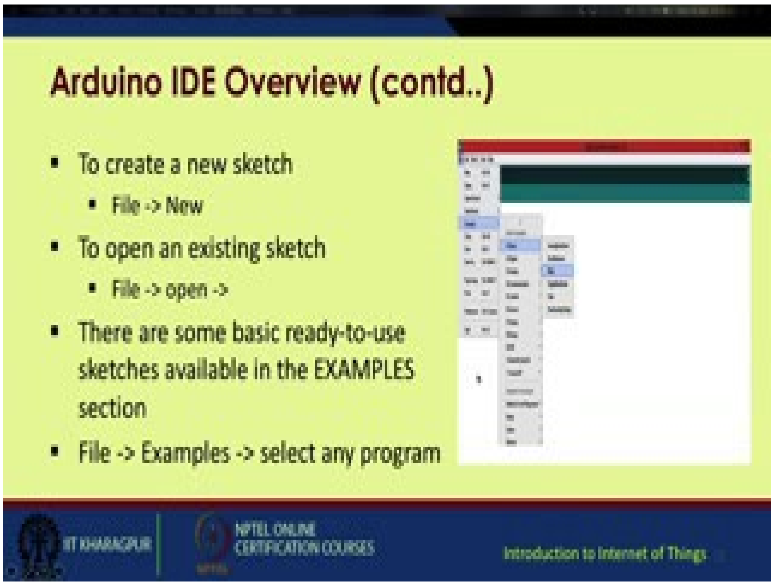
So, now the once the board and the ports have been appropriately selected as I have told you select the board then the corresponding port in your PC. For windows base systems it will be more or less direct it will show you a com base port it may be com 4, 10, 15 anything you choose it appropriately.

(Refer Slide Time: 12:12)



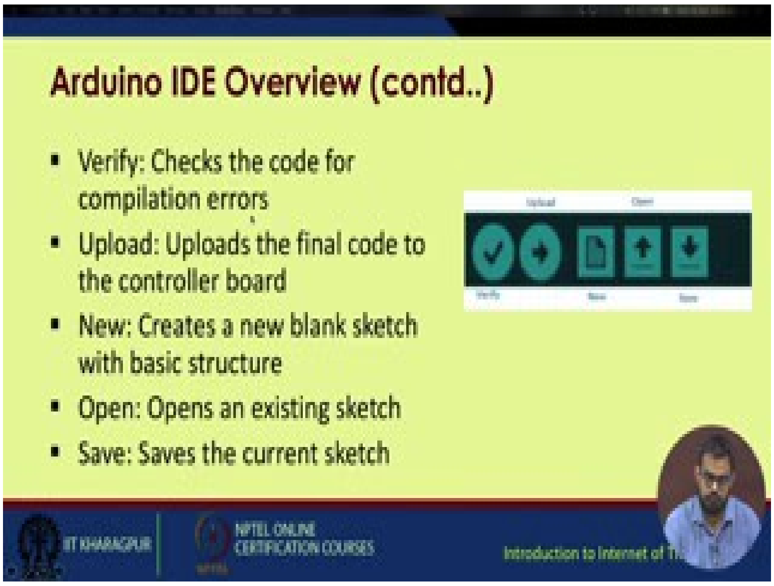
Then I have already shown you this. So, your arduino sketch as you remember the program which is written in to the arduino for written for the ardunio is called a sketch. So, it consists mainly of two parts one is the setup and one is called the loop. Setup is analogous to for normal mean C, C plus plus based program the main function you use it is analogous us to the setup function in arduino. And as the name suggest the loop function it is used for iteratively looping over instances.

(Refer Slide Time: 12:54)



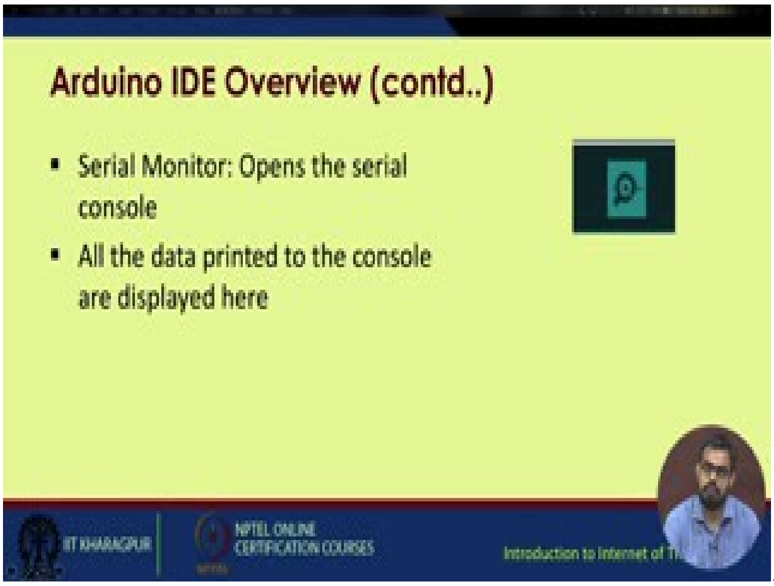
So, its more or less common from file you click on new it will open a new file and you can tryout various examples and sketches.

(Refer Slide Time: 13:06)



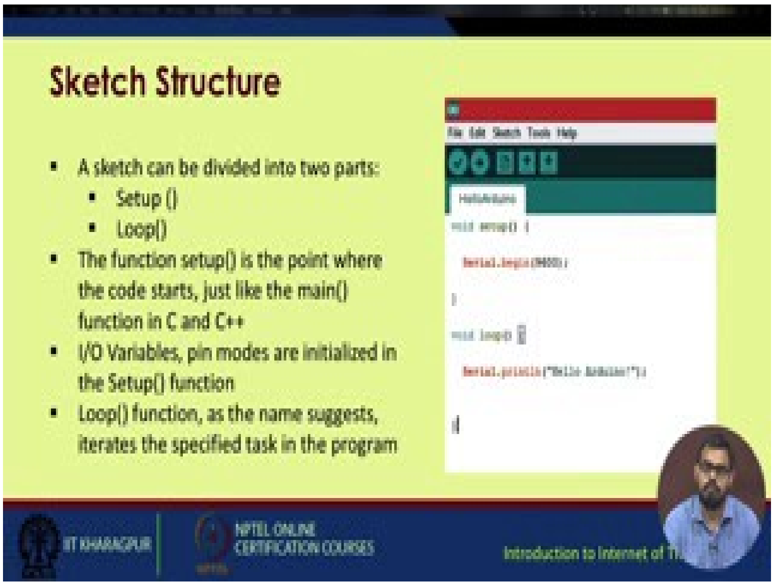
So, have also covered this one, this is the verify button. So, the main feature is prior to uploading your code if you have syntax errors or any such logical errors it will be caught during verification, it will say your compilation has failed. Once you pass this verification check you can upload your code.

(Refer Slide Time: 13:37)



Now, this we talked about this is the serial monitor whatever data is transmitted through the serial port is printed on the serial monitor.

(Refer Slide Time: 13:43)



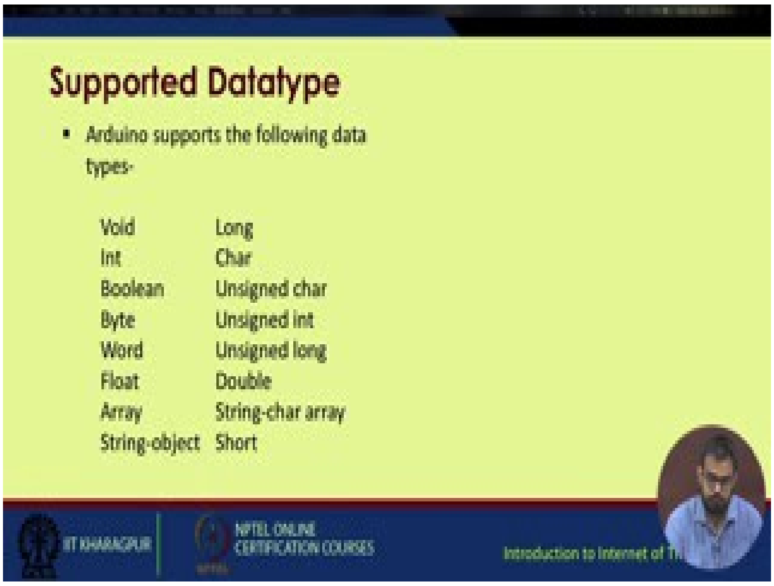
So, a sketch structure as I have told you it consists of two parts a setup part and the loop part. The function setup is the point where the arduino compiler actually starts the code. So, it is just like analogous to the main function in C and C plus plus and various input output variables pin modes whether you need to as you remember you have 14 digital input output pins. So, you have to explicitly tell your system whether you want to use the pin in a read mode or the input mode or the output mode then the loop function is used for iteration.

So, in this example code you can see you just use a serial port the inbuilt serial port. So, we just write serial dot begin 9600 and 9600 is the baud rate. So, you can have various baud rates will come to that will cover that in the consecutive lectures you can have various baud rates for different systems, but 9600 is more or less the commonly use baud rate for most of the systems and within void loop you want to iteratively loop this hello arduino. So, this serial.println that is if you write serial.print it just prints the hello arduino string otherwise if you write println ln is actually new line. So, it will print hello arduino in the new line.

So, prior to this we will look at the sample code. So, as you can see in this hello arduino code within the word setup we have written serial dot begin 9600 and within void loop we have just written serial.println hello arduino. Now, prior to doing anything we verify the code as you can see it is compiling the sketch. If your code compilation is correct, so its correct just shows how much memory it is using in those. If you are in error, suppose I delete this semicolon. Now, again I verify the sketch, it will give an error. So, this is the good practice prior to uploading blindly, you just verify your code. Now, the code verification is successful, the ports have already been chosen, I upload my code. So, it is now compiling the sketch and it is uploading at to the arduino board.

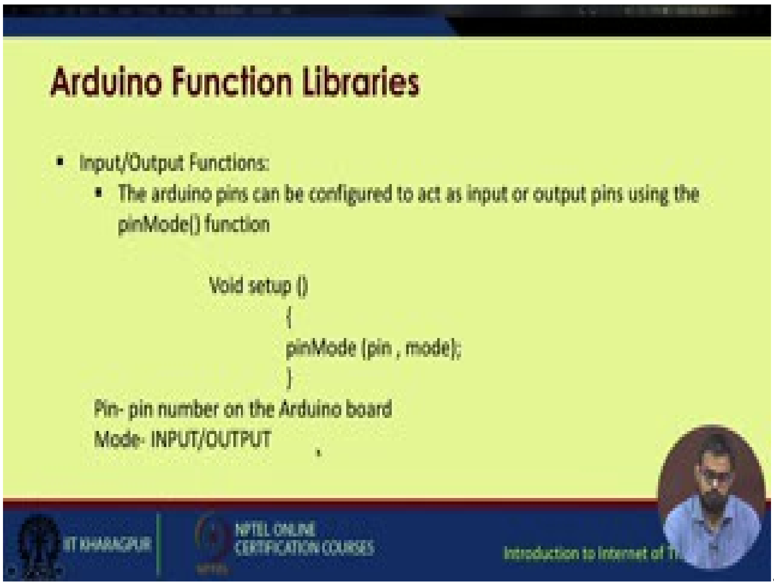
Now, the code has been uploaded to the arduino board since the function of this program is to print hello arduino on the serial port iteratively will open the serial monitor. As you can see, it is printing hello arduino right. So, it is actually quite fast. We can actually modify it will put up function call delay let us say delay of 1 second. So, this thousand days actually the delay in milliseconds will put of a delay of 1 second. The code has been verified we upload it again. Now, again we open the serial monitor. Now, you can see now the delay has been in case. So, it prints after 1 second. So, I hope this was easy.

(Refer Slide Time: 18:17)



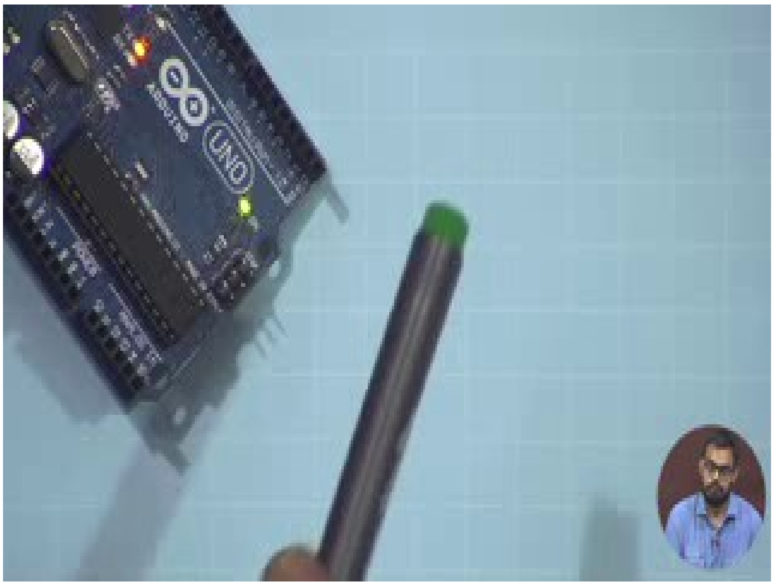
Now, let us move on to the next menu, ok. So, like other programs arduino also supports various data types you have void, int, Boolean, byte, word, float, array, string-object, long. char, unsigned, char, it is somewhat similar to your normal C programs. So, arduino has lots and lots of libraries since it is an open source flat form collaboratively people also people and companies and organizations they upload their own arduino libraries

(Refer Slide Time: 18:37)



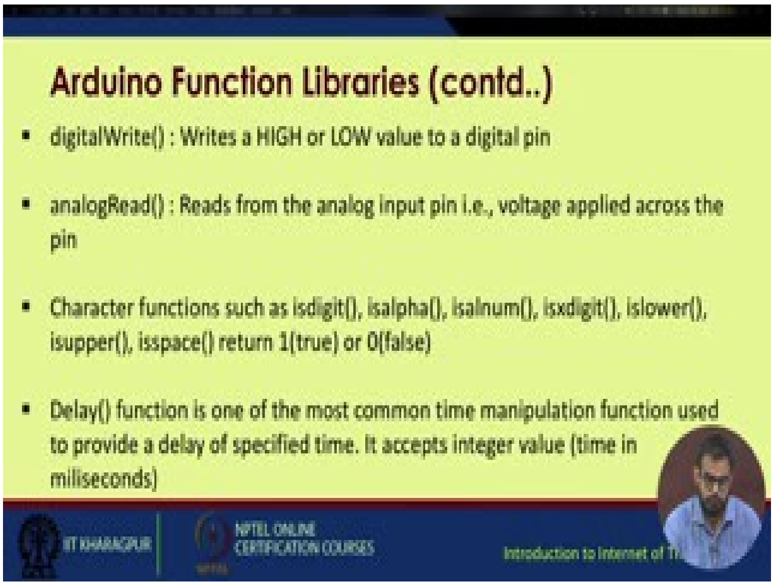
So, for most of the functions will obviously, get easy access to various libraries. So, as you already know the pins can be configured to act as input or output depending on your requirement. So, to do this, this function pin mode is used. So, you can see this syntax is pinMode(pin , mode).

(Refer Slide Time: 19:23)



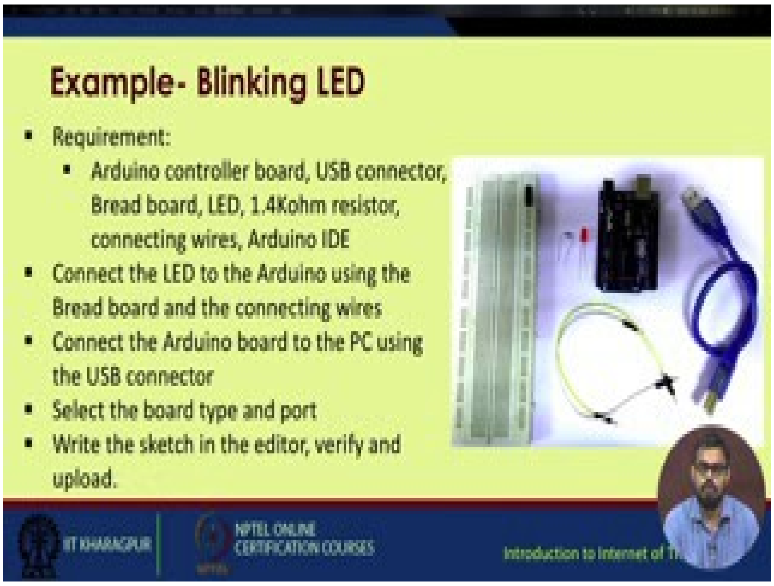
So, this pin is the number, the pin number actual pin number on the arduino board as you can if you focus on this board, you will see various pin numbers are written over here 1, 2, 3 since these are the digital pins it is also written digital. So, in the pin mode against the pin you just write the number of the pin. So, it is that simple and the mode you just write input or output if you want the pins to work in input mode like you are connecting various sensors to it which you will acquire sensor a inputs you put the pin in input mode. And if you want to actuate something maybe a light or LED or a motor, you put the pin in output mode.

(Refer Slide Time: 20:04)



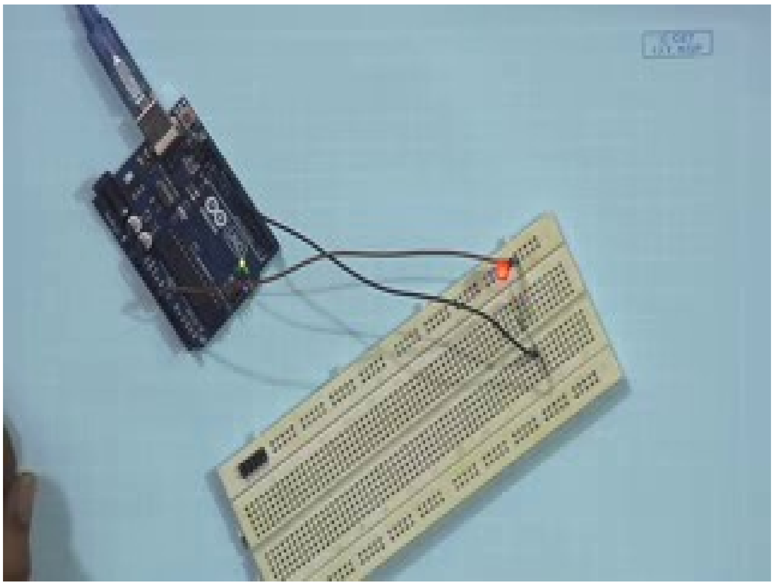
So, various arduino function libraries you have digital write, so which writes high or low values to a digital pin. Whenever since you have to remember this thing mainly works on a binary logic you either have a high voltage or a low voltage corresponding to 1 or 0. So, your digital write it either writes a high or low value to the pin then analog read function, it reads an analog function analog input from the analog pins, you have six analog pins. Then character function you have various character functions to check whether it is a character or a digit. So, you can see the various functions isdigit(), isalpha(), isalphanumeric(), isxdigit(), islower() and various of the functions you can use to check whether the input is the character or a number or a alpha numeric combination and so on. So, this next one you have already covered this delay function. So, you will find it is one of the most versatile and commonly use functions in arduino. So, input is taken in milliseconds as you recall we put 1000 for the delay. So, 1000 milliseconds converts to 1 second.

(Refer Slide Time: 21:19)



So, next one is will use a arduino and the normal bread board to switch on and off a LED.

(Refer Slide Time: 21:34)



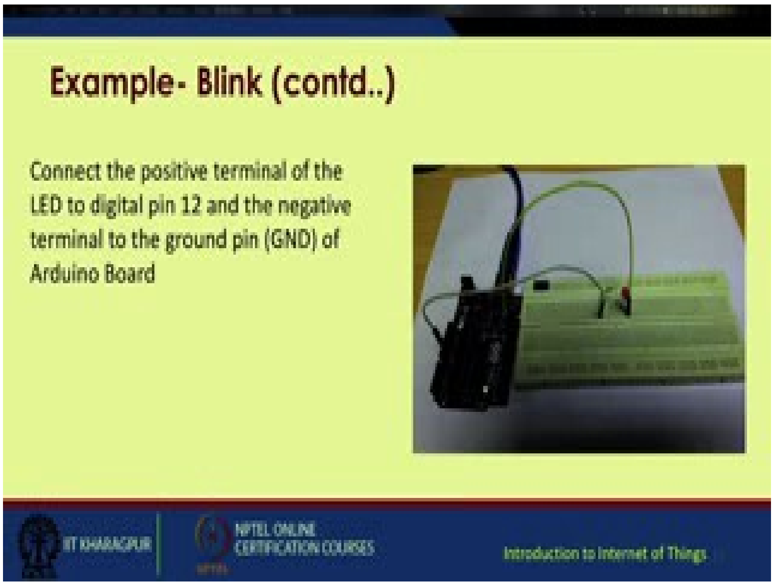
Now, we have got a LED. We have got a arduino board as you remember these are just basics of electronics. So, for a LED the longer terminal is the positive one, whereas the shorter is the ground. So, we connect the longer terminal to one port, other to the ground. Across this LED we connect a 220 ohm resistance in series prior to taking input from the arduino board. So, this is LED blink.

So, if you concentrate on the setup part within the setup you see the pin mode selected is 12 and it has been selected as output. Basically translates to pin 12 will act as output. So, we will connect the LED to pin 12. Whereas, in the void loop you can see this digital write if you recall digital write either writes high or low values to a particular pin. So, digital write 12 high means you are writing high value to the digital pin to pin 12 and you gave a delay of for 1 second then again you put the pin 12 to low then again a delay. So, this will calls the LED to blink on and off with 1 second delay each.

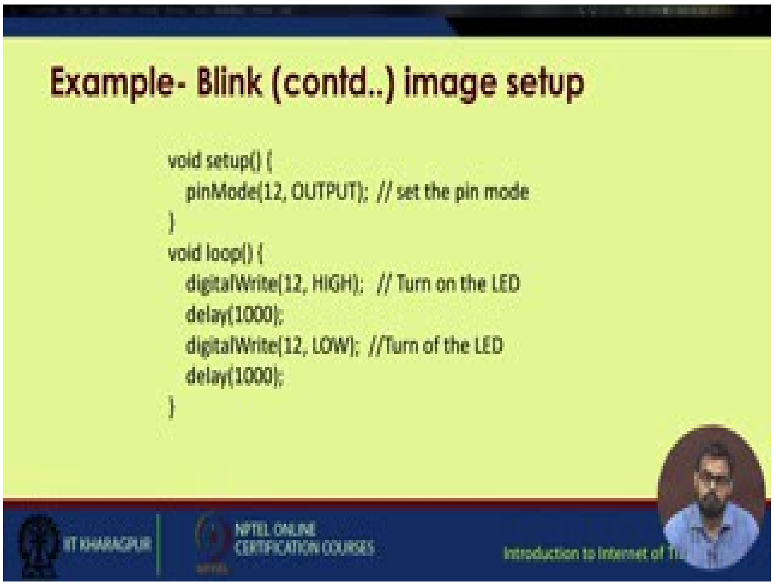
Now if you come back to the processer board, so we have connected the LED and the resister on the bread board from one side of the bread board we connect a jumper cable to pin 12 one the arduino and for the other since this side was the negative side or the ground we connected to a ground. So, we simply connect this to ground pin. So, again refreshing we have just created the simple circuit. We verify our board is arduino UNO, the port is already selected, we verify our code. Now, the code has been verified we upload our code. Just as soon as the code is uploaded, you will see the LED starts blinking with a delay of 1 second right.

Now for easier checks, you can always use pin 13, pin 13 is by default for arduino UNO at least is connected to the inbuilt LED. So, I mainly check validity of a code based on pin 13, you would not require external interfaces then. So, if you focus on the arduino board this small LED over here, this is the inbuilt LED or the indicator. Now, uploaded my code, the same function you saw on the external LED is being applied on this code, I will just change the pin number from 12 to 13.

(Refer Slide Time: 25:21)

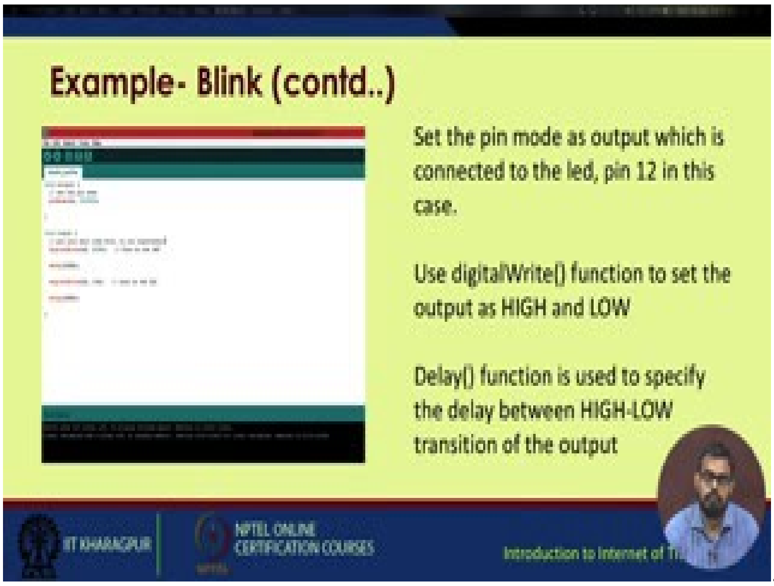


(Refer Slide Time: 25:28)



So, we have covered these things, we have connected pin 12 and the other side to the ground. We uploaded the load the code and uploaded it.

(Refer Slide Time: 25:31)



So, ok this was it. So, in the next part, we will go into more details of arduino programming.

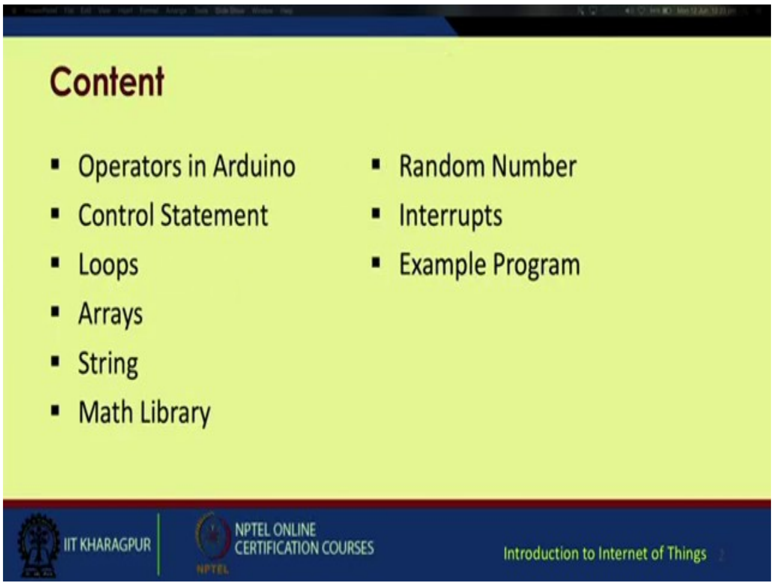
For now thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 23
Introduction to Arduino- II

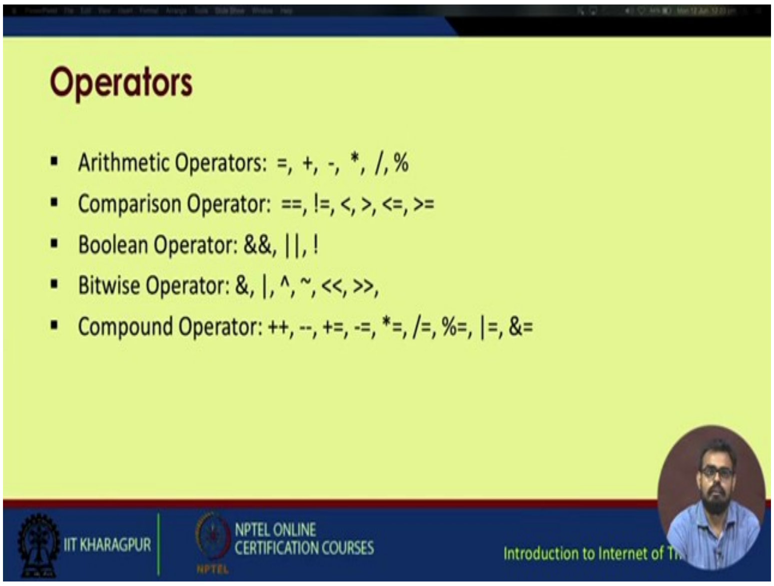
Hi. Now, we will continue with the Introduction to Arduino Programming. This will be the 2nd part and the continuation of the previous one.

(Refer Slide Time: 00:28)



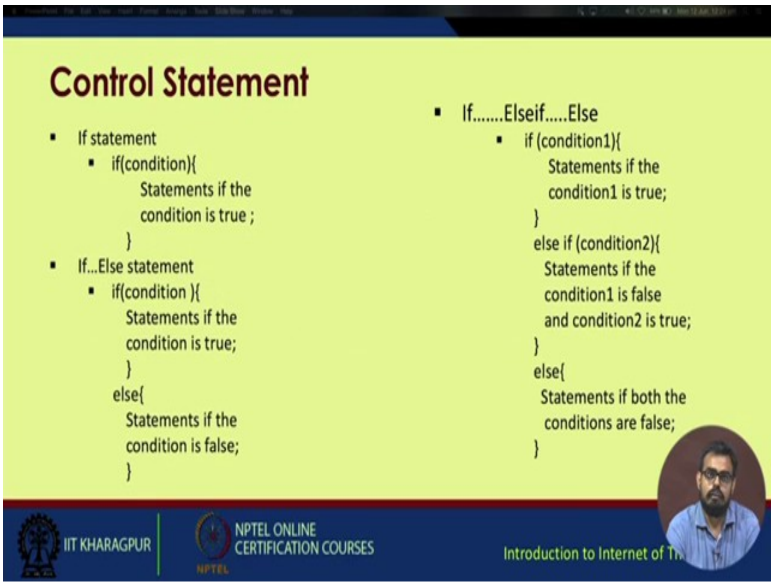
So, we will cover the basic topics, the Operators in Arduino, Control Statements, Loops, Arrays, Strings, The Mathematics Library, Random Number Interrupts and Example Program which will be bit complicated than the previous one.

(Refer Slide Time: 00:44).



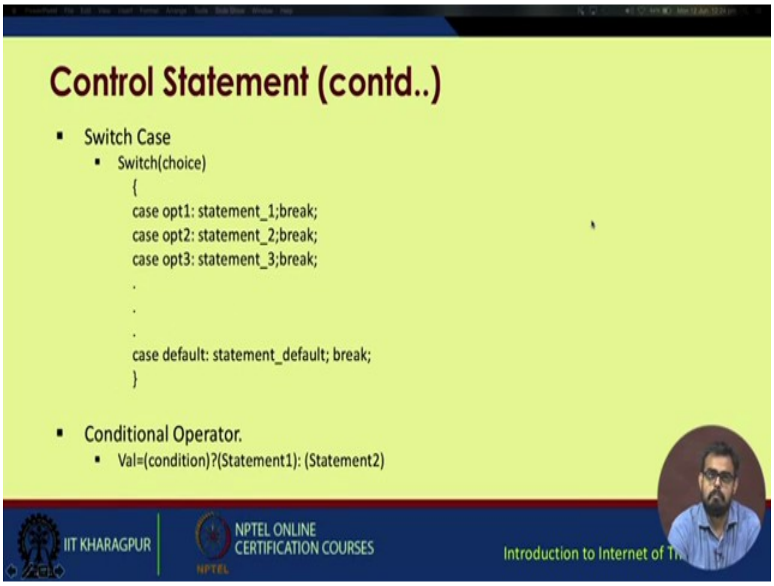
So, basic operators as normal C, C++ or python programming or other languages, you have the basic equal to, plus, minus, multiplication, division module, division operators, then comparison operators, we have equal to, not equal to, less than, greater than and all those operators. Then, we have Boolean operators, bitwise operators and compound operators.

(Refer Slide Time: 01:14)



Moving on to control statements, these will basically cover the various checking and looping parts. So, a normal if else statement in Arduino, we start off with if statement.

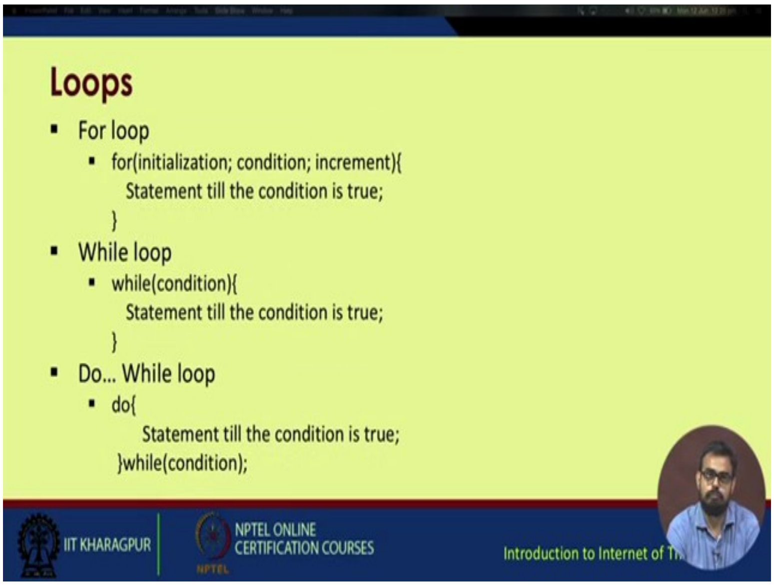
(Refer Slide Time: 01:49)



So, if you have a condition and within this curly braces, if the statement condition is true.

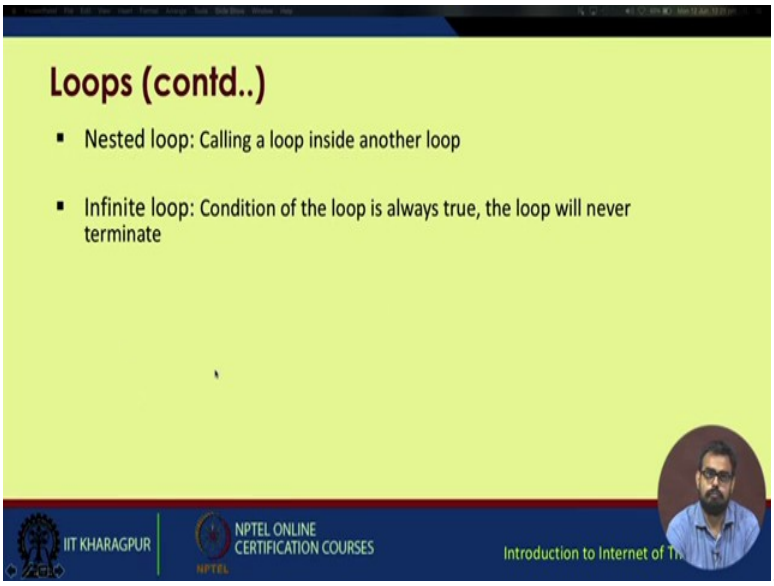
If else, if another statement condition is true or else if none of the above statements are true, then this loop will execute moving on to switch case. You have switch and choices, you have case option 1 and statement and then, a break function after each case. So, case option 2 is statement 2, then again a break and so on and at the end, you have a default case. After that we again have a break function, then you have a conditional operator and we will avoid using conditional operators such as these in Arduino. So, it is condition if it is true, it will execute statement 1, else it will execute statement 2. These kind of statement operators are best avoided during Arduino programming.

(Refer Slide Time: 02:35)



So, in loops you have the basic for loop, then you have the while loop you have a, do while loop, these are pretty common examples.

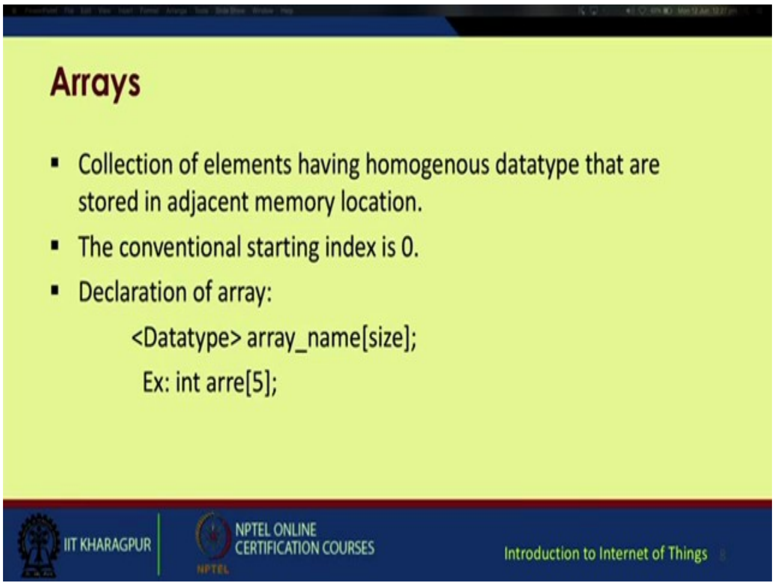
(Refer Slide Time: 02:47)



You have a nested loop that is a loop inside another loop. You can have many nested loops inside each other. So, you have an infinite loop. So, to run an infinite loop for example, all you need, you develop a system in which you need to turn on and off a light or a LED or any other device infinitely as long as the devices on your system is checking. So, recall from the last lecture which I showed the blinking LED example.

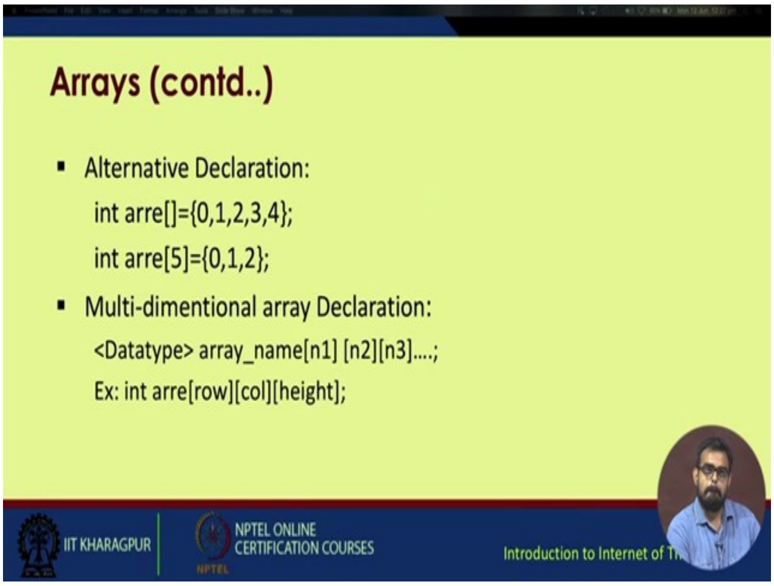
So, you can see if you put it inside an infinite loop as long as the Arduino board is powered, it will keep on blinking. So, your functions can be made more complicated. Instead of LEDs, you can have motors. Instead of motors, you can have actually cameras mounted on the motors and they keep on rotating. You can have a multitude of sensors which are interface with the cameras and the motors. So, for example you can build the security systems which will keep on running as long as your processor board is fine and the power is being supplied, you can always connected to a battery supply to generate power for it.

(Refer Slide Time: 04:08)



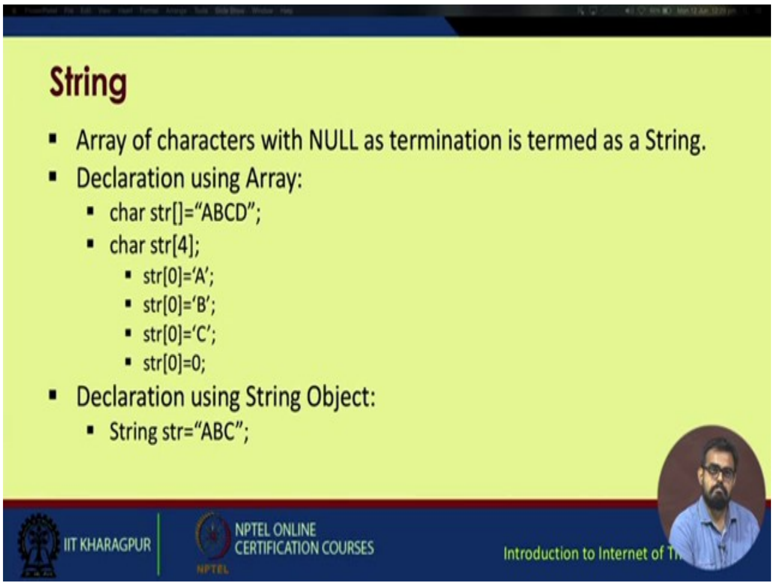
Then, you have arrays. Arrays are collection of elements having homogeneous data type and which are stored in adjacent memory locations. The conventional starting index is 0 in Arduino. So, declaration of array you just start off with the data type. It maybe arrays of integers, so int array name and the size. So, for example, int arre this a variable name are[5], it will allocate five spaces for your array, then you can have an alternate declarations.

(Refer Slide Time: 04:44)



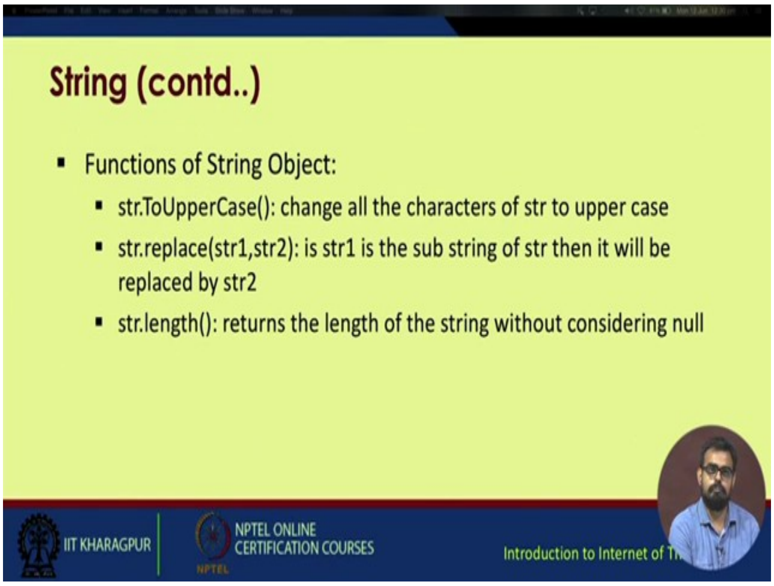
Suppose int array and this blank bracket [] equal to within this curly braces, you have 0 1 2 3 4. So, these will be automatically stored in this array. Then, again you have enter a five, you can just put in three variable, three values inside this array and the remaining will be kept blank maybe for later use. You can fill those also. Then, you have multi-dimensional array declarations same as previous one, you have the data type, then array name, then the dimensions for the first dimension let it be n1 n2 n3. So, for example, if you want to declare an array for an image which normally normal rgb image, so you have three channels red, green and blue. So, each image will have a 2D structures, rows and columns and there will be a depth for each r, g and b. So, maybe for those types of data, we have int array row column height.

(Refer Slide Time: 06:03)



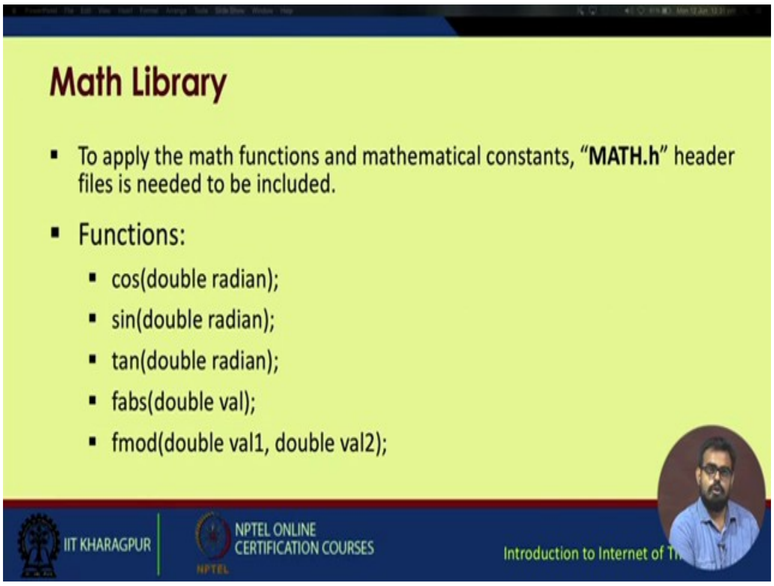
So, then moving on to string, string is an array of characters with null as the termination declaration is maybe using char char string. Here str is the array. So, abcd, so this is stored in str char str[4] and you can individually access each ids, you can store A B C or maybe 0. So, this using the same location if you want to individually store in different locations. So, sorry come in the same location if you keep on storing this. The last one will be last character stored will be updated and other will be overwritten. If you want to store in different locations, you just change it from string it from string 0, str[1], str[2], str[3] and so on. So, you will have consecutive A B C 0 side by side these locations. Another thing you can also, you also have a data type string. So, string str = "ABC" will give you ABC. All together you do not have to store in individual locations. So, this is one of the benefits of using Arduino.

(Refer Slide Time: 07:31)



So, some commonly used functions of string. So, str to upper case point to note is to upper case T U and C are caps. So, this has to be follow strictly since this is part of the syntax. So, it changes all the characters of string to upper case and then, you have string str.replace string 1 and string 2. So, string 1 if it is sub string of str, then it will be replaced by str 2, then str.length, it returns the length of the string without considering the null character.

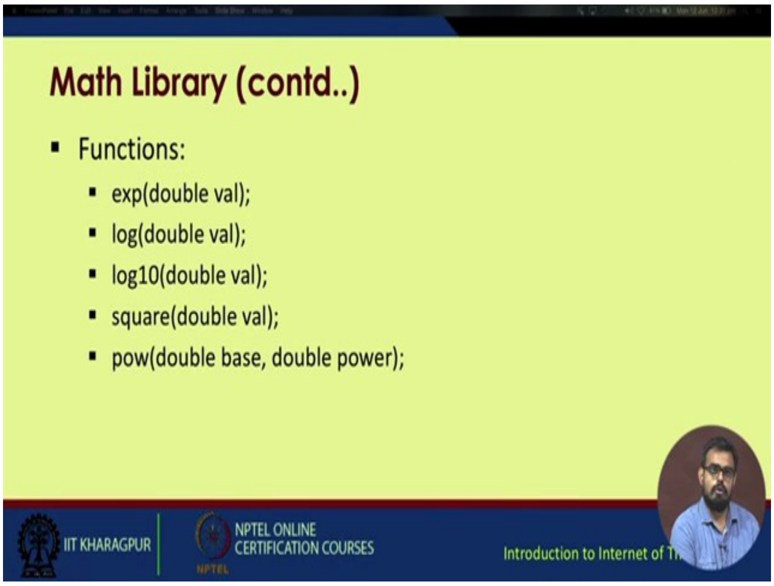
(Refer Slide Time: 08:12)



Then, another commonly used library is the math library. To apply the math functions, the math.h header must be initially called, otherwise you will not be able to access these functions. So, some of the common functions are cos which is in double radian and sin tan floating absolute fabs right floating mod.

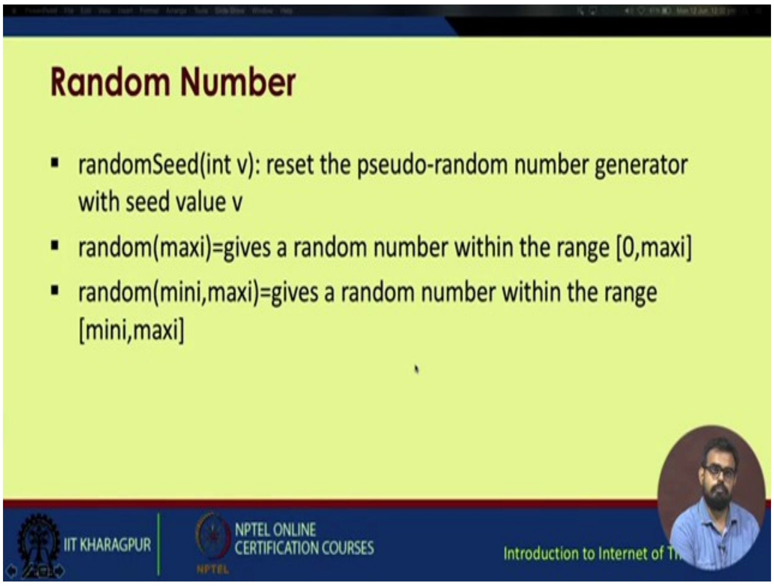
So, double value 1 and double value 2, so you have two values and f mod will give you the modular division and the result point will be a floating point number.

(Refer Slide Time: 08:52)



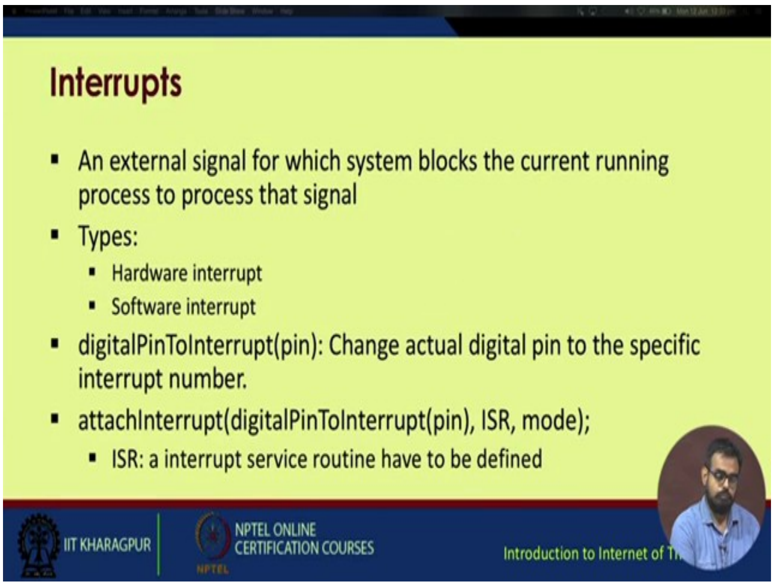
Then, continuing with the math library again you have exp which signifies the exponential function. You have log function. This will give the national logarithm of the value. Then, you have log 10, then you have square function, power function. First argument is the base, the second argument signifies the power, then another commonly used example is random number.

(Refer Slide Time: 09:19)



So, one of the functions of this random number is random seed. So, the syntax is randomSeed , S capital. You need to focus on this one because this is the inbuilt syntax for Arduino. So, randomSeed(int v), it reset the pseudo random number generator with seed value v. So, you already the seed value is the starting point from which the random number will initialize its function. So, you gave a starring value, from it the random number will generate, then random(maxi) gives the random number within the range 0 to maxi, then you have random(mini ,maxi) and it gives the random number within the range mini and max.

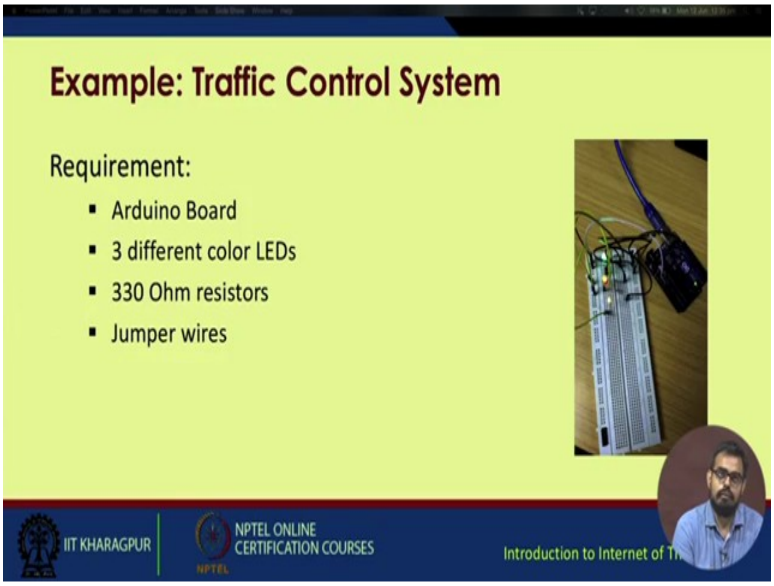
(Refer Slide Time: 10:24)



Then, moving on to interrupts, you have an external signal interrupts. These are basically an external signal for which the system blocks the current running process till receiving that signal.

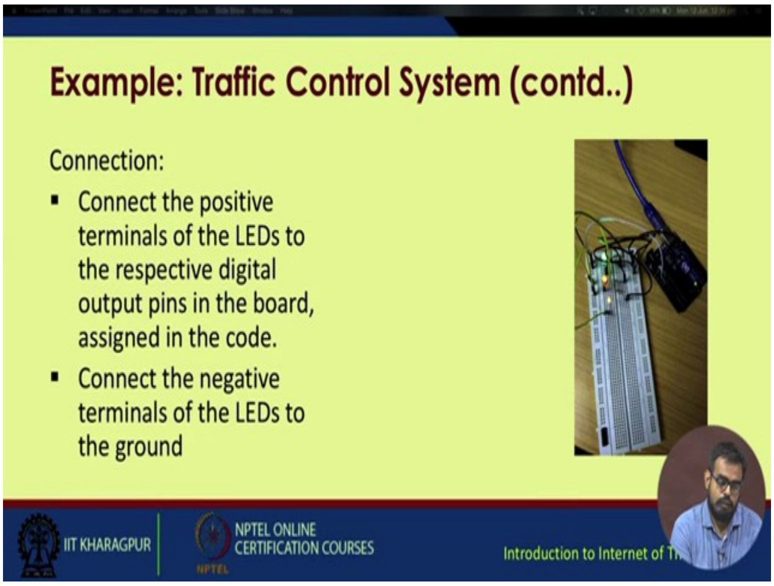
So, basically you have two types of interrupts. One is hardware and another is software. So, I will give one example. Suppose you are in a loop here waiting for a checking condition whether that checking condition holds true or not and maybe from an external source you are getting that checking condition. For example, you have a button or a digital switch connected to a Arduino board. So, whenever you are pressing that switch, your system will blink an LED, otherwise it will keep the LED off. So, this may be considered as a, partially considered as an interrupt. So, this will be an external interrupt. So, as you can see digital pin to interrupt and then, the pin number it actually changes that digital pin to the specific interrupt number, then attach interrupt digital pin to interrupt, then pin, then ISR, then mode. So, isr is basically known as an Interrupt Service Routine. It has to be defined explicitly. So, these are some of the more complicated function. So, we will not focus on these interruption. Other complications we will just try to keep it as easy as possible.

(Refer Slide Time: 12:07)



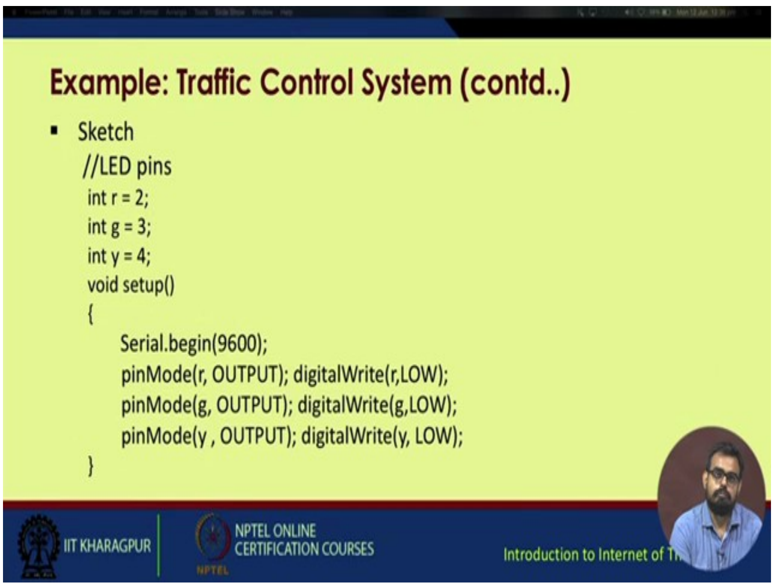
So, we will try to implement within this lecture, we will try to implement a basic rudimentary traffic control system. So, we need Arduino board, three different LEDs, some resistors maybe 220 ohm or 330 ohm and a few connecting jumper wires to connect the various components on the breadboard as you can see from the previous, as you remember from the previous example.

(Refer Slide Time: 12:31)



We connected an LED with the Arduino board. The same process has to be repeated three times using different colored LEDs and at different pins. So, in the last example, we connected the LED to pin 12. So, maybe in this example, we will connect to pin 2 3 and 4 side by side.

(Refer Slide Time: 13:59)

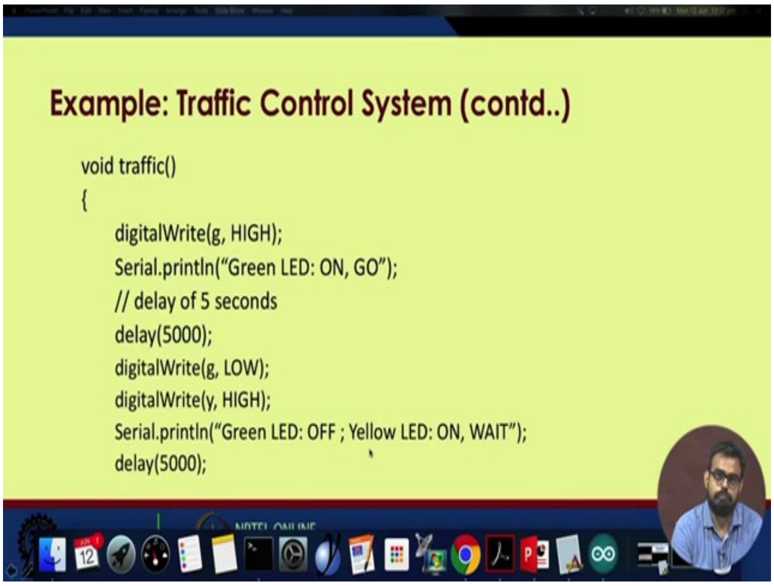


So, this is the sample sketch. So, as you can see tried to using void setup, we globally define a few value int r = 2. Basically we are taking three colors r g and b, we are not giving b. We are written y.

So, r g and y, red green and yellow, so globally we are defining r as integer equal to 2, g equal to 3, y equal to 4 in within void setup. We initialize the serial port at 9600 baud rate, then pin mode we write r and and output. So, as you can remember the first one was the actual pin on the Arduino device and the second one was the mode either input or output. So, since you are connecting LEDs will be obviously using it as output. So, r was globally assigned as 2. So, this will be 2 and output. So, it translates to pin 2 will work as output and then, digitalWrite r low. So, this function will initially set the a value of pin 2 to 0. So, it will be turned up. The same process is repeated for pin 3 and pin 4 which connected to the green and yellow LEDs.

Now, we define the function traffic. So, data type you have given as void.

(Refer Slide Time: 14:34)

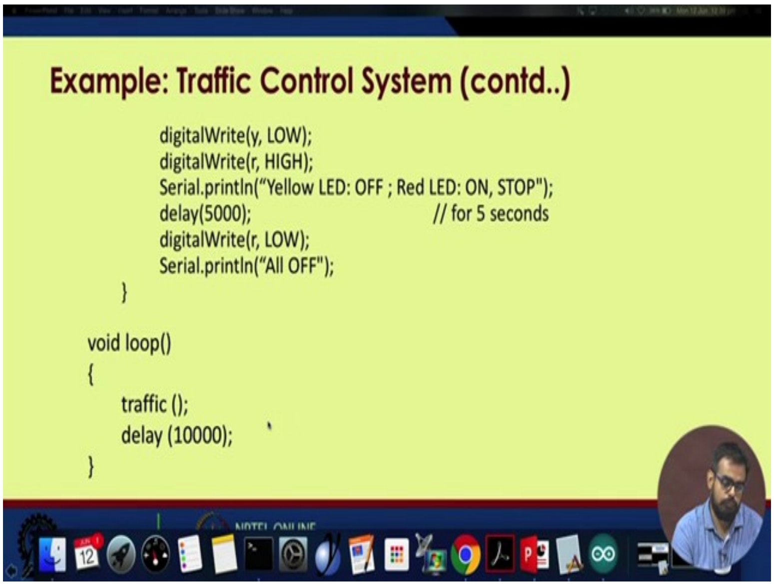


So, void traffic we digit, so digitalWrite g high that was g was defined as pin 3. So, over here pin 3 becomes high, then serial be over the serial port, we print green LED on go. So, since it simulates a traffic signal, you will have a go signal denoted by green, a stop signal denoted by red and a wait signal denoted by yellow. So, green LEDs when it switches on, it signifies go this will be printed on the serial port you can all obviously comment this out.

Then, we induce a delay of 5 seconds using this command delay 5000. So, if you remember from the previous example, delay takes an input in the terms of milliseconds. One more thing this double slash, it denotes commenting the character. So, whenever you put // in front of a statement, it will not execute. Your compiler will skip the execution.

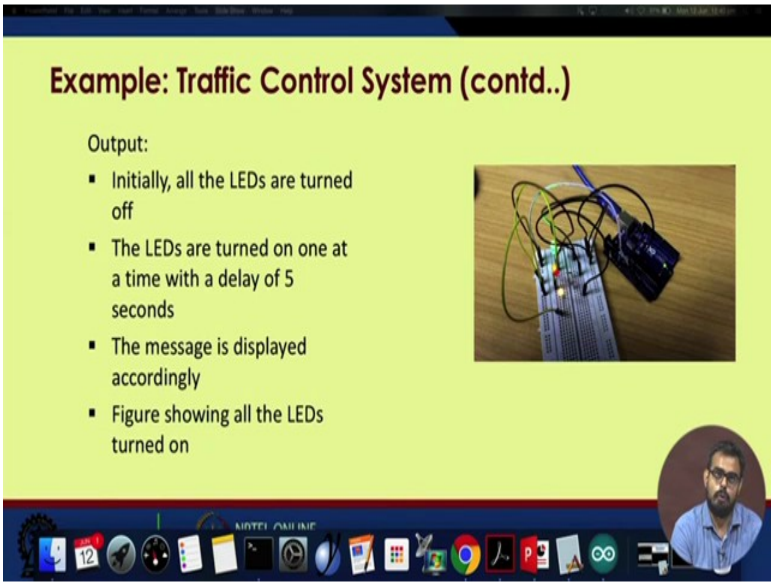
Next we go to digitalWrite g low. So, what is physically happening is at the start of the loop, you have the green signal is glowing and then, after 5 second delay, the green signal is off.

(Refer Slide Time: 16:25)



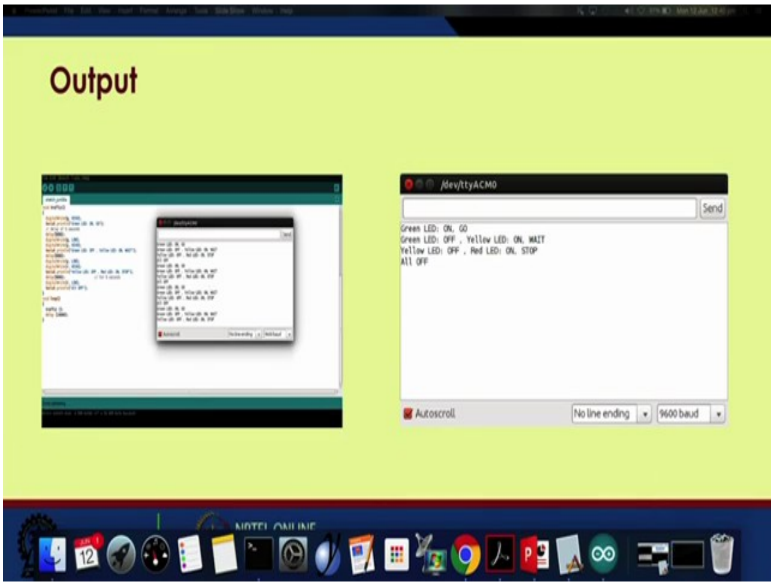
Then, the yellow signal goes high. So, your print again green LED off yellow LED on. So, the status is wait, then again a delay of 5 seconds, then followed by digitalWrite y or yellow as low and digitalWrite r as high. So, your wait signal will turn off and the stop signal will go high. Same thing is printed on the serial port, then again you have a delay of 5 seconds, then digitalWrite r as low. Now, you have all three LEDs turned off and you serially print all off now within this void loop, you call this traffic function. So, this traffic will iteratively run again and again and again till your device is powered and if call a delay of 10000 that is 10 seconds, so your traffic signal loop will run once and then stop for 10 seconds, then it will the whole loop will once again and it will keep on going.

(Refer Slide Time: 17:29)



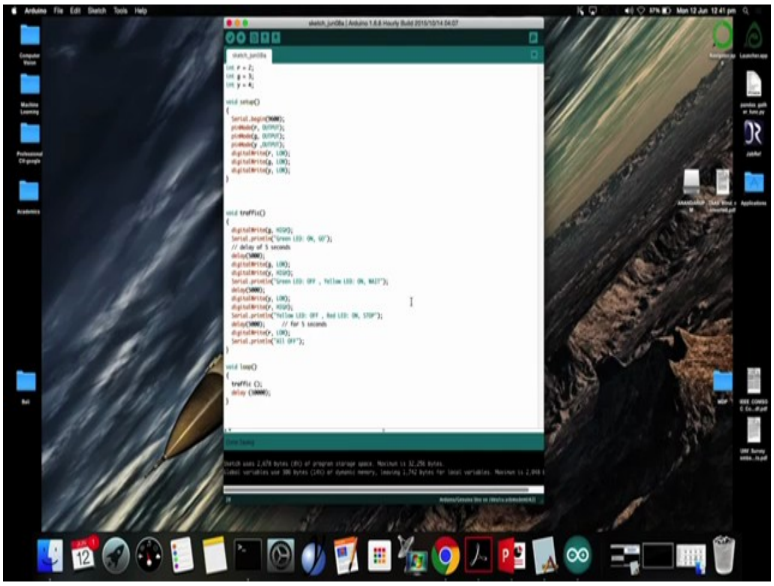
So, as you can see over here in the image, the LEDs are glowing sequentially. We will come to that on the hands on.

(Refer Slide Time: 17:39)



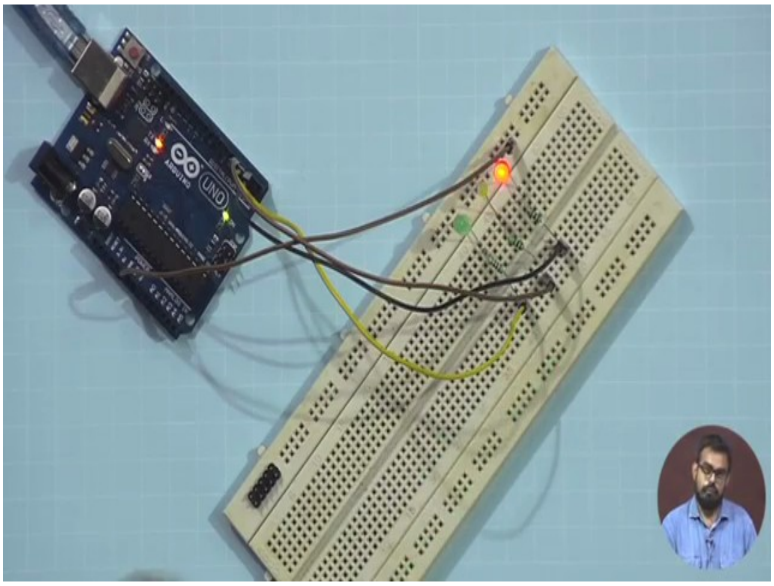
The various outputs are printed on the terminal. Now, if you come back to the circuit part as you can see the code I showed you.

(Refer Slide Time: 17:59)



I have already made the code ready. I have connected the Arduino board.

(Refer Slide Time: 18:14)

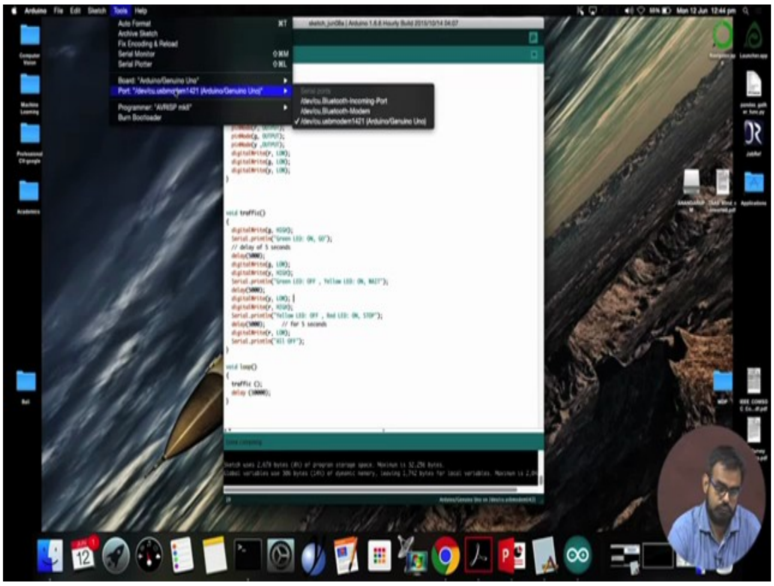


So, I have three differently colored LEDs red, green and yellow. I have three 330 ohm registers, I have Arduino UNO and I have a bread board. I will just connect these sequentially green, yellow, red.

You must always remember this convention that the smaller pin is for ground, the longer pin is for positive signal. So, let us check again this row is supposed to be ground. Since the yellow is properly connected, green is properly connected. Now, across each LED, we will put up a register, 330 ohm register.

First of all sense in a breadboard, these channels are fused. So, I will only need one signal, single signal to connect to the Arduino. This was negative part will connect to ground. Now, if you remember the green was connected to pin 3, green was assigned a pin 3 in the code. Pin 2 was assigned to red and yellow was assigned pin 4. So, now we have our connections ready. So, three wires for r g and y and one for the ground.

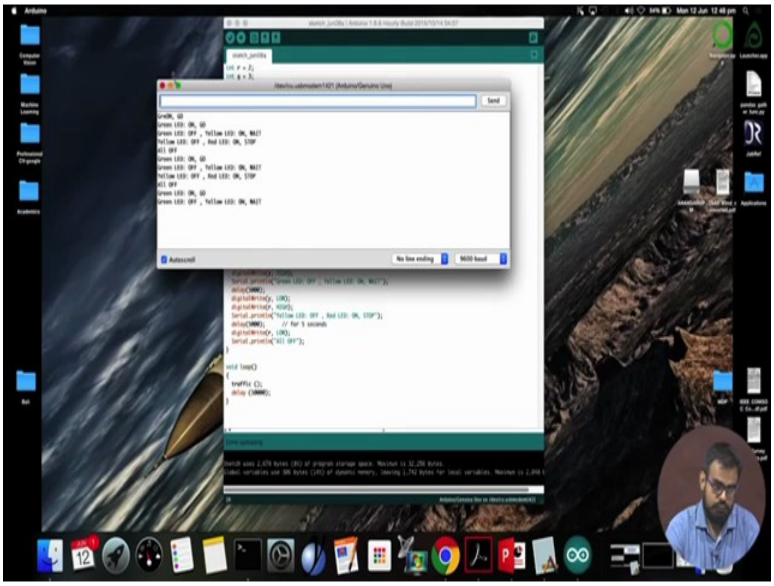
(Refer Slide Time: 20:50)



Now, if you go through the code again, so you have globally declared r as pin 2 , g as pin 3 and y as pin 4. So, we have been implemented on the breadboard, then serial port starting baud rate is 9600 pin mode, r g and y as outputs digital write, r g and y as low that is initially at the very beginning everything will be turned off and within void traffic you switch on each LED one at a time starting from green, then yellow, then red. So, this basically what a traffic signal does is, so we will compile this code.

You see the code has been compiled without any errors. I will check whether my board is connected. Yes it is Arduino UNO the port is, so the board and the ports are fine. We will upload the code or the sketch. Now the uploading part is complete. So, if you focus on the Arduino board as you can see you have a reset button. So, it has already entered into a loop. So, we will push the reset button, so that the code execution starts from the very beginning. You see the green LED glows on it will glow for 5 seconds followed by the yellow one which will again glow for 5 seconds and then, it is followed by the red one which glows for 5 seconds. All three turn off. It will wait for 10 seconds before going again into the loop that void traffic loop.

(Refer Slide Time: 22:44)



Now, same thing if you focus on the serial monitor, you can see green LEDs is on go green off yellow on wait. Now, yellow off red is on stop, right. So, now everything is off. So, it will be wait for 10 seconds.

Then, again the loop starts from the green LED. So, it is actually not required to have a serial communication for this automated traffic control signal, but for the sake of debugging, I actually prefer this thing. So, you can actually when you connected your system to PC, you can actually see which part of the loop your code or the hardware is executing. So, it helps you in debugging your code effectively. So, this is it for now, ok.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 24
Integration of Sensors and Actuators with Arduino- I

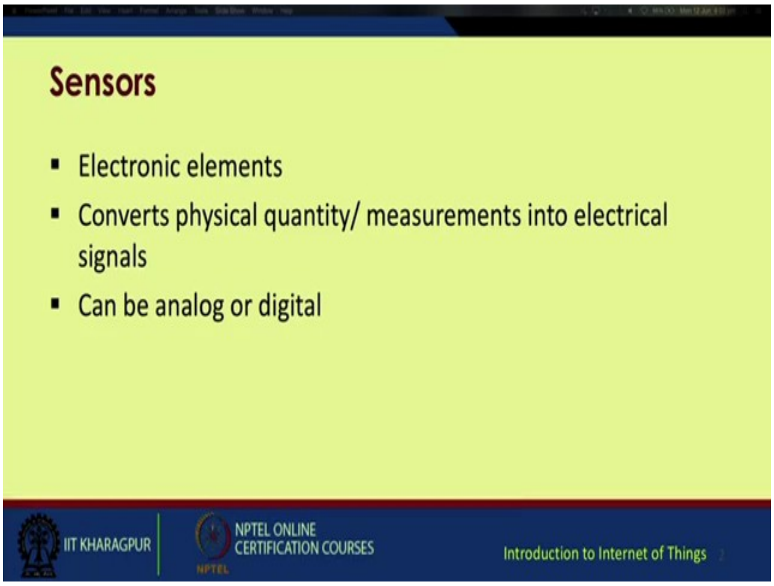
This lecture and the next one are dedicated to discussing the integration of sensors and actuators with Arduino platform. So, in a previous lecture we have taught you about how to you know what is Arduino and how to use it for building IoT systems and in this lecture we are going to show you further that how we can integrate sensors and actuators with Arduino. I told you that a multitude of several types of several types and several sensors can be integrated in to Arduino platform it supports for that and at the same time seen for are actuators as well. So, here I am going to teach you about how to do it.

And I have with me Mister Anandroop Mukharji the TA of the course and he will explain to you how to do this hands on. So, as I said before that if you have the set up, if you have the requisite small electronic equipments with you then you can also do the same to practice yourself. So, that way it will give you a hands on experience about how to create a small scale small sized sensor actuated based Arduino platform for used in IoT. So, this specific type of sensor that we are going to show you here we are using only one sensor and we are using only one actuator, the sensor that we are using is the temperature humidity sensor and the actuator is the motor, the survey motor.

So, let us know have a look at how to build a small sensor actuated based Arduino platform for use in IoT.

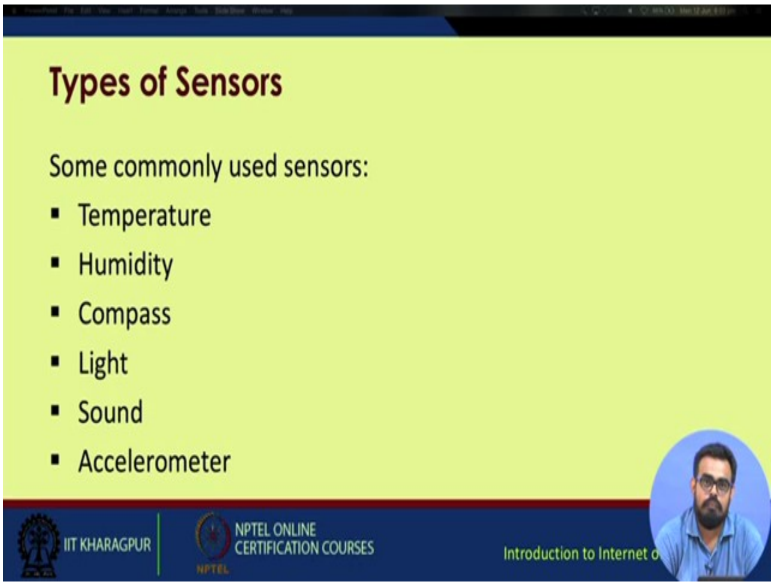
Hello I will be now talking about the integration of sensors and actuators with Arduino. So, this will be again in two parts in the first part I will cover integration of sensors with Arduino and in the second part integration of actuators with Arduino.

(Refer Slide Time: 02:29)



So, first of all as we have already learned by now; sensors are basic electronic elements they convert physical quantities or measurements into electrical signals and more or less sensors can be classified into either analog or digital sensors.

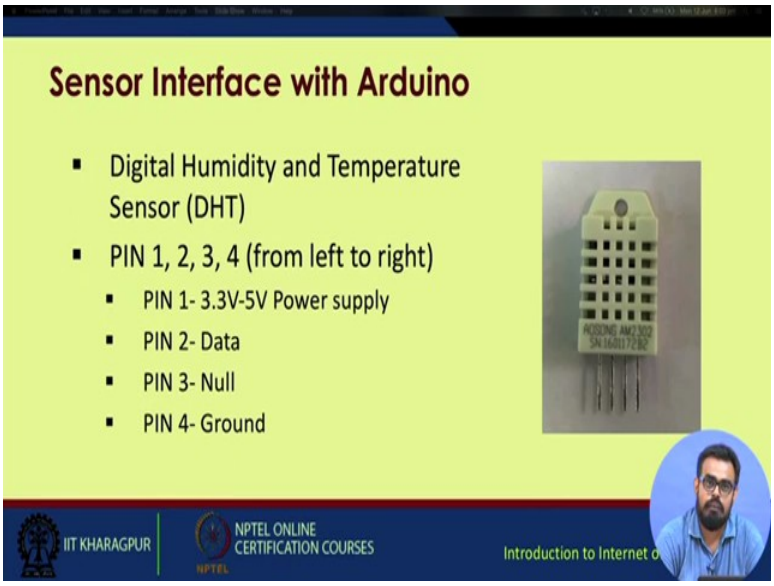
(Refer Slide Time: 02:46)



So, there are few common type of sensors we actually use with IoT they include temperature sensors, humidity sensors, compass or direction sensors light sensors, sound sensors accelerometers or motion sensors.

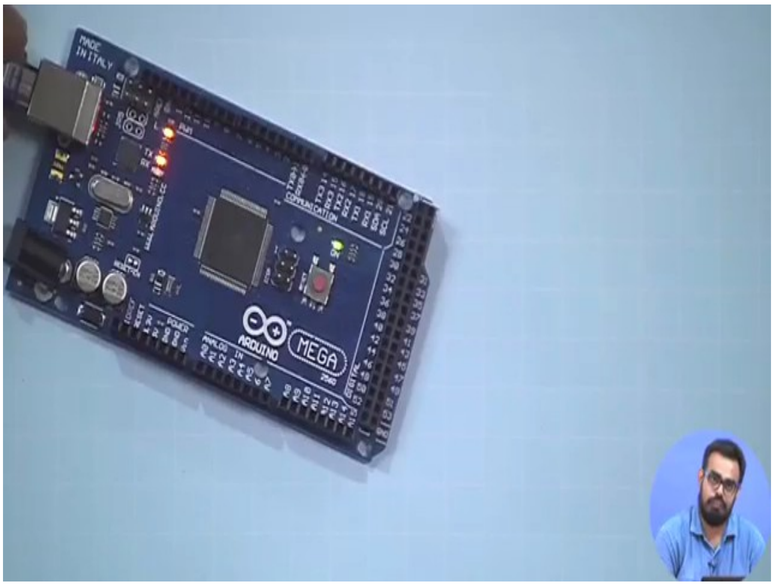
And there are lot many varities of sensors we could not accommodate everything over here, but I am sure if you find search online you will come across huge number of sensors.

(Refer Slide Time: 03:16)



So, now in this lecture will be covering interfacing of a humidity and temperature sensor with your Arduino board. So, in our previous lectures we use an Arduino uno just for the sake of bringing in some variety.

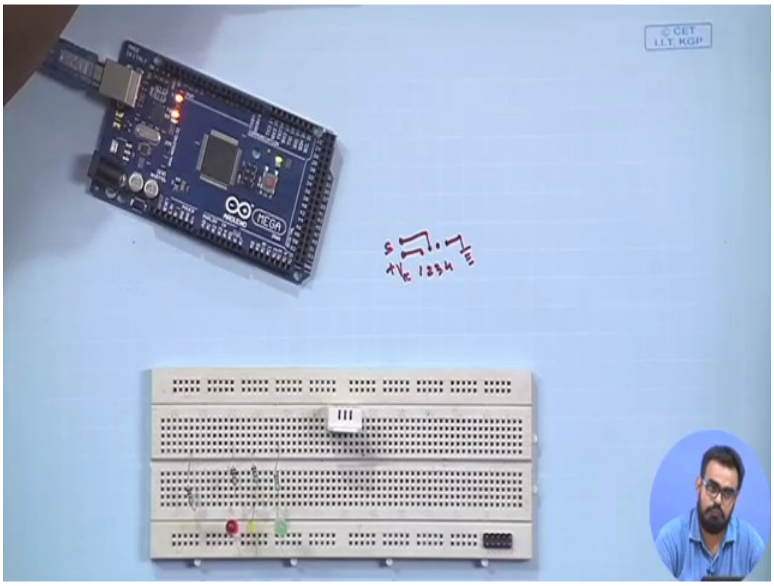
(Refer Slide Time: 03:39)



Now, we are using and Arduino at mega; so, Arduino mega. So, in the market you can just get it by the name of Arduino mega or mega 2560. So, its bit bigger than your traditional Arduino uno this one has got 4 uarts, Arduino uno if you recall had only one uart and obviously, there are much more digital input output pins there are much more analog input pins.

There are 16 analog input versus 7 for 7 or 8 for your uno, and the voltage inputs and power lines are more or less same. So, we take this one.

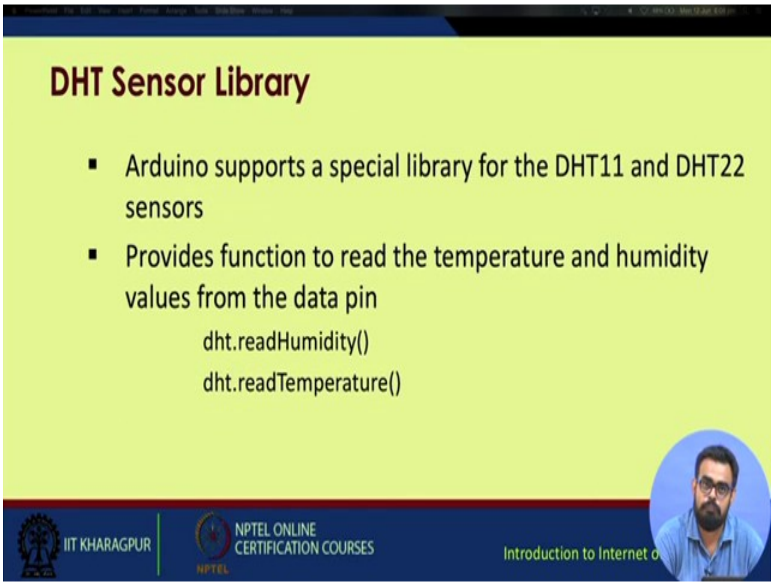
(Refer Slide Time: 04:37).



Now, we again have our breadboard. So, these we have the LEDs and registers left from the previous slides, this one is known as a DHT sensor. So, DHT stands for digital humidity and temperature. So, as we can see it has 4 pins and starting from left to right if you keep this upfront this mesh region upfront starting from left to right you number them as 1 2 3 and 4. So, basically you have four pins pin one we give a positive voltage the last pin we keep as ground, the third pin is the signal pin and the sorry the second pin is the signal pin and the third pin is left open or no connection.

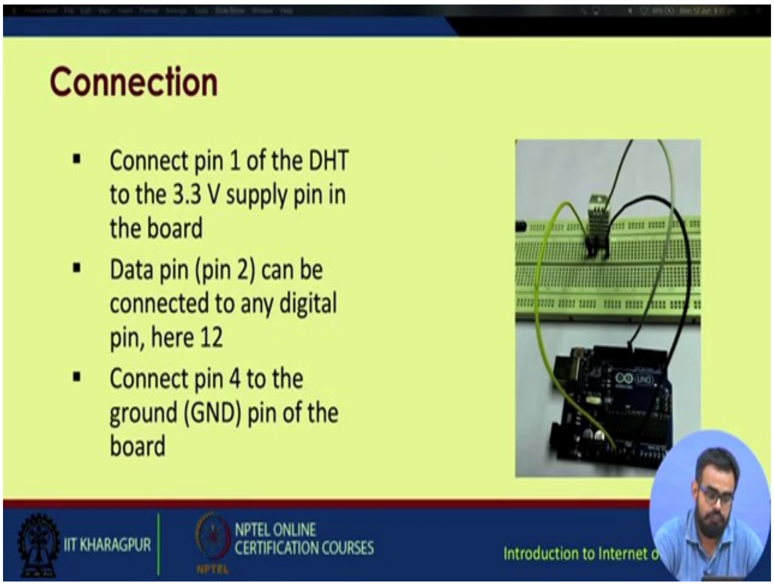
So, following this basic connection idea we put it on the breadboard; now your pin one has to be connected between to a supply ranging from 3.3 volt to 5 volt you should take precautions not to exceed this 5 volt range, otherwise your sensor will be damaged. Pin 2 is the data pin from which the actual sensor data is coming to the board, pin 3 as I have told you before it is null on no connection and pin 4 is ground.

(Refer Slide Time: 06:18)

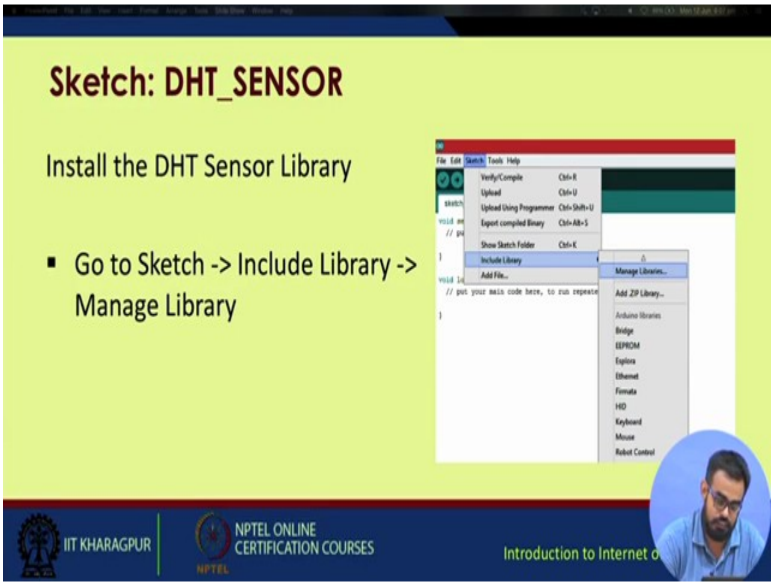


So, prior to interfacing the hardware with the Arduino ide, we actually need the support of a few libraries available online. So, this sensor was acquired from your Adafruit it is a company which supplies various Arduino boards and related components and other processor boards. So, we are going to use the Adafruit library for DHT11 of DHT22. So, this sensor we are using is actually DHT22; your DHT sensor library it provides some basic facilities for reading the humidity reading the temperature and so on.

(Refer Slide Time: 07:04)

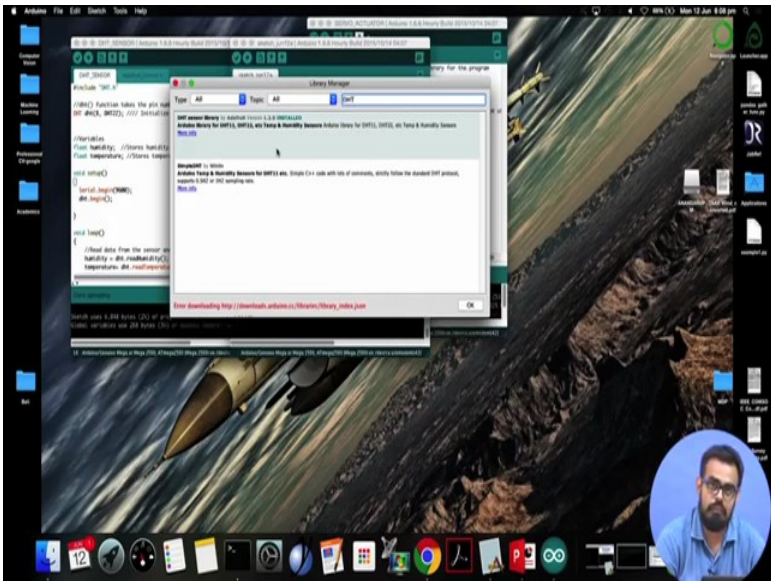


(Refer Slide Time: 07:09)



So, for now will just skip the connection ok first will look for the sensor integration look for the updation of the library your existing Arduino ide.

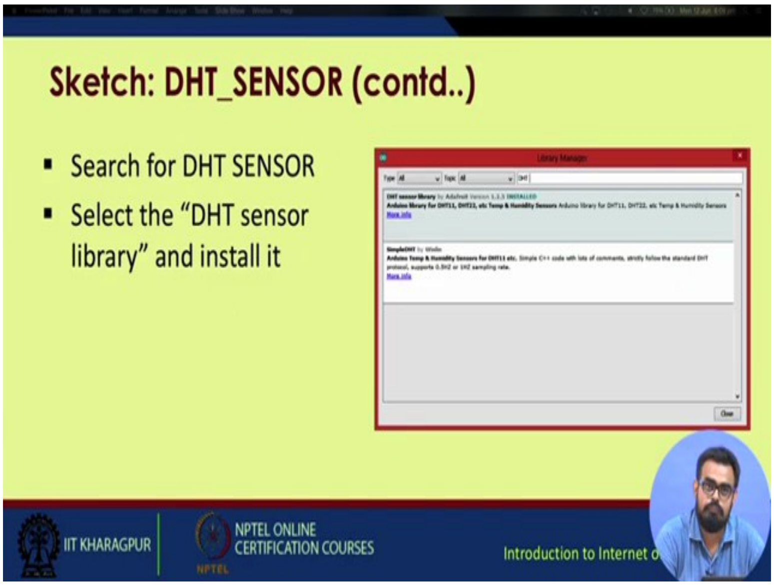
(Refer Slide Time: 07:19)



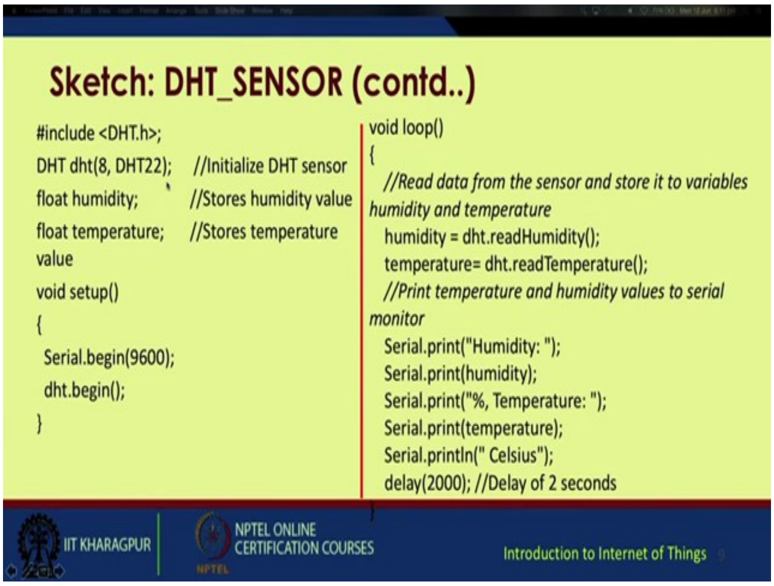
So, we start off with we go to tool sorry you go to sketch on the menu bar then there is a option for include library and then manage libraries generally it is on the top. So, and the library manager you write sorry you just write DHT. So, as you can see I have already installed this library file.

So, you get a DHT sensor library, you just click on it and if your pc is connected to the internet your Arduino ide will do the rest you just download it will download the library integrated with the system you restart your Arduino ide in you are ready to go. So, as I have already installed this library no need for anymore action.

(Refer Slide Time: 08:27)



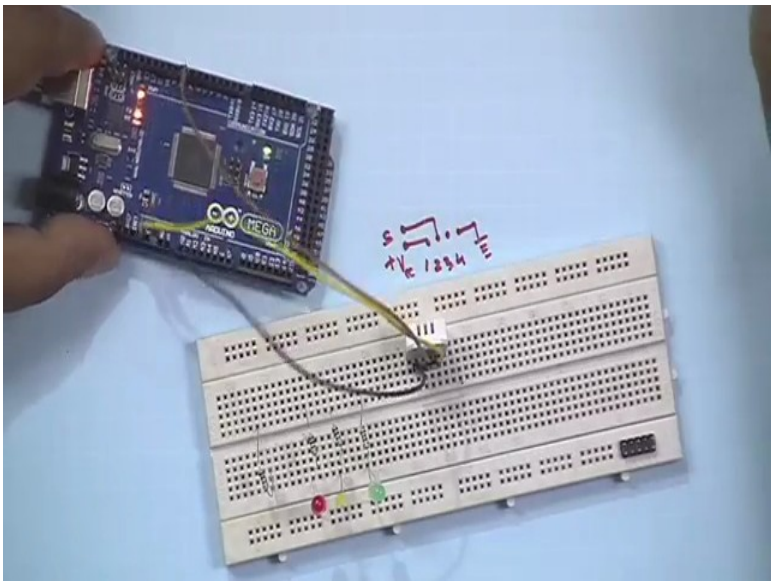
(Refer Slide Time: 08:33)



So, this is actually how you update the Arduino ide with the required library. So, you have already selected the DHT sensor you click on it and it installs.

Now, coming to the actual sketch for the DHT, prior to that will just install the hardware with the Arduino board. So, if you recall these four pins starting from 1 2 3 and 4 you place it on the breadboard.

(Refer Slide Time: 08:59)



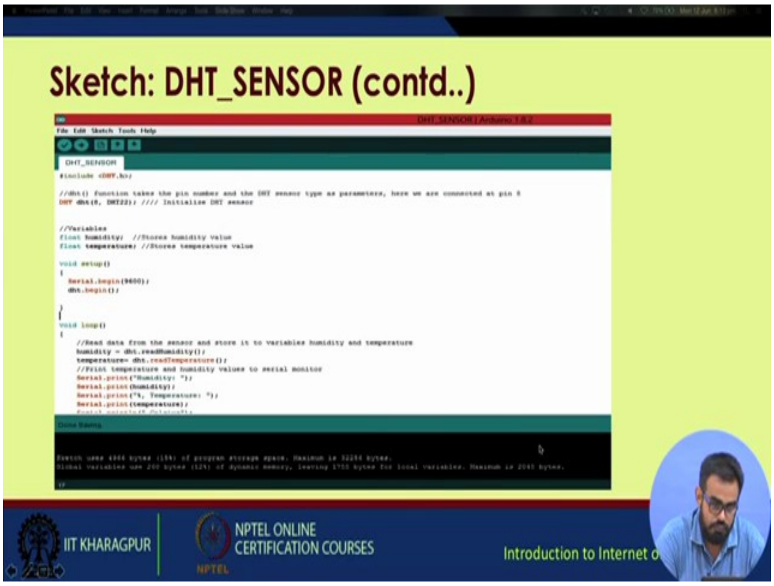
We take four jumper cables. So, pin 4 was ground, I connect pin four to ground pin one was Vcc it should be between 3.3 and 5 volt, just to place if I will put it at 3.3 volts, and pin two is the actual signal input which will come to the Arduino board. So, let us say we choose any digital port let say we choose pin number 8 or port 8. So, we connect the signal wire from the DHT to pin 8, you can choose from any of the digital input output pins. So, now our hardware is ready it is quite easy. So, focusing back to the sketch part for the DHT sensor, this you have to for this you have to include the library file you downloaded it contains a few header files and other definitions. So, you must include that particular library file. So, first line is hash include DHT.h right.

Then from its own syntax from the syntax of the DHT sensors library installed you just call DHT then DHT pin and sensor. So, you are initializing that DHT sensor. So, this is the syntax and we have to follow this syntax strictly because it is according to that library we just downloaded, now we are defining to variables both of floating type. So, one is float humidity and another is float temperature right. So, the humidity this variable humidity will store the humidity values acquired from the sensor and temperature will store the temperature values acquired from the sensor.

Now, within the setup since we are going to view whatever readings we have getting from the board or the sensor on the serial port, we just initialize the serial connection. So, again serial dot begin at baud rate of 9600 after that we initialize the dht dht.begin(). Over here in the second line you have just assigned your dht to pin number 8 and we have given that sensor as dht 22 suppose you go for the variant dht 11 then you just update this part as dht 11 or if you plan to change the pin number on the Arduino board you have update that part over here. So, once the setup part is complete you go into the looping part.

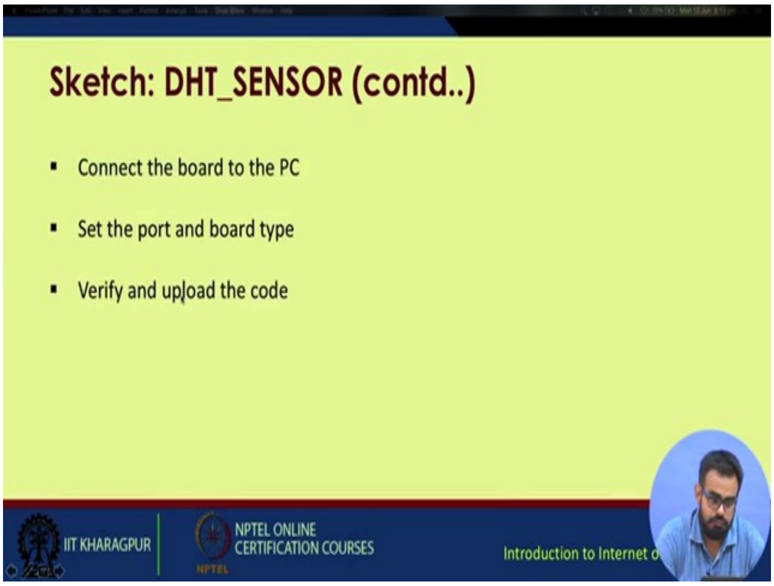
So, over here you can see the variable humidity it is being assigned the dht.readHumidity function. So, whatever function whatever sensor offsets and operations need to be done is being taken care of the taken care of the dht.h library. So, you just call this function read humidity, then temperature as dht.readTemperature once you have call these to you just serially print these variations. So, as I have given a delay of two seconds. So, after every two seconds your humidity and temperature will keep on updating.

(Refer Slide Time: 12:55).



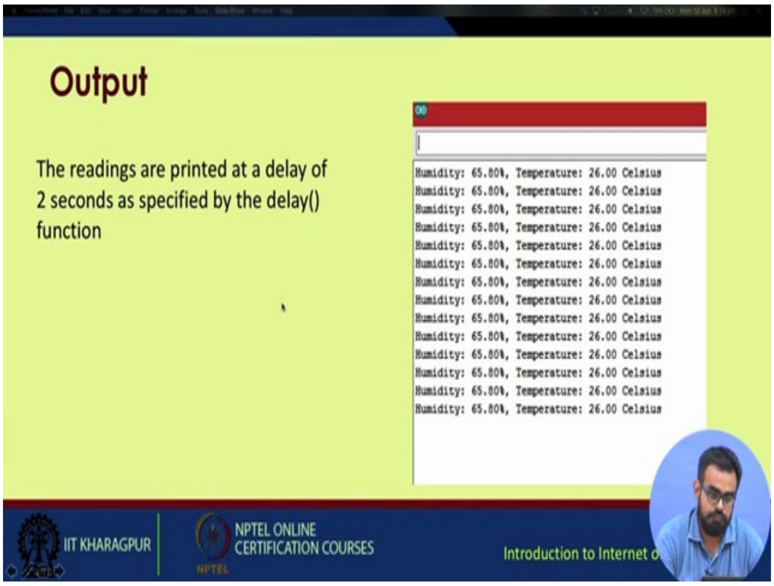
So, let us go to the next slide. So, we have already interfaced these sensors this is the code you just saw in the previous slide this one, then again we go through the basic steps we connect to board to the pc.

(Refer Slide Time: 13:08)



We set the port and board type now remember the port and board type may change because board type will definitely change, the port may or be not change for this we choose mega. There will be an option for mega we chose it then prior to uploading we verify the code and then upload the code.

(Refer Slide Time: 13:34)

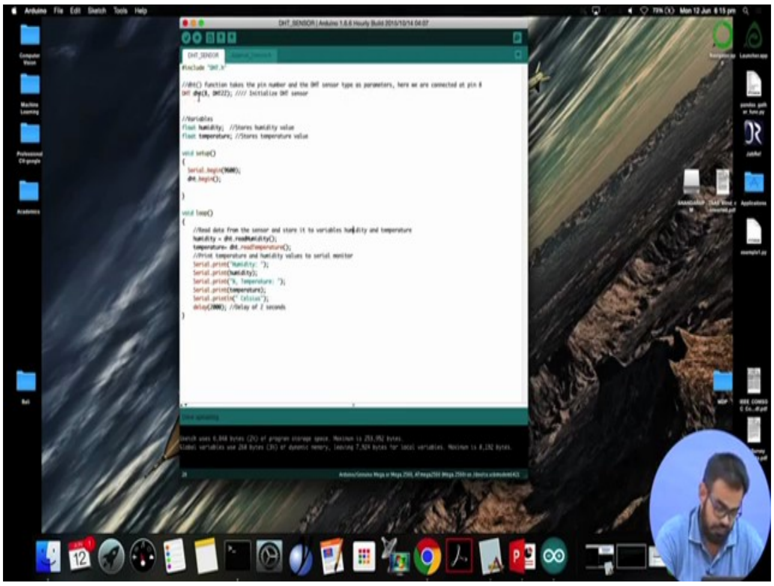


So, this is the output we are expecting like humidity is giving in percentage and temperature in degree Celsius, and these each row is separated by time duration of two seconds. So, after every two seconds your temperature readings and humidity readings are getting updated.

So, now, back to the hardware part.

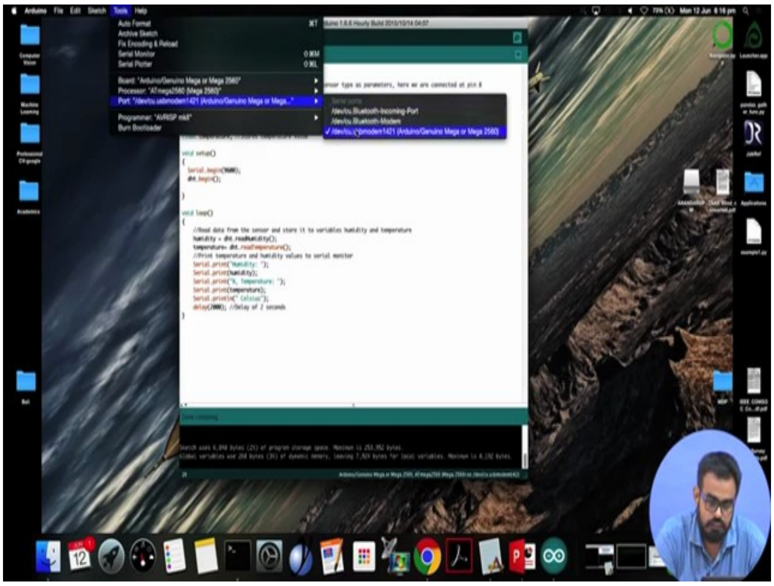
So, I already have the code openened in front of me.

(Refer Slide Time: 14:04)



Right as you can see # include dht.h then we have set the pin number at 8 in the input pin sensor type is DHT 22 humidity flowed temperature within void setup serial dot begin at baud rate 9600 dht.begin(). So, setup is ready and within loop we just call the humidity and the temperature reading functions and that is it and just serially print it over and over again with the delay of two seconds. Now since everything is connected we just verify our code. So, its compiling the sketch; sketch is complied there is seems to be no error.

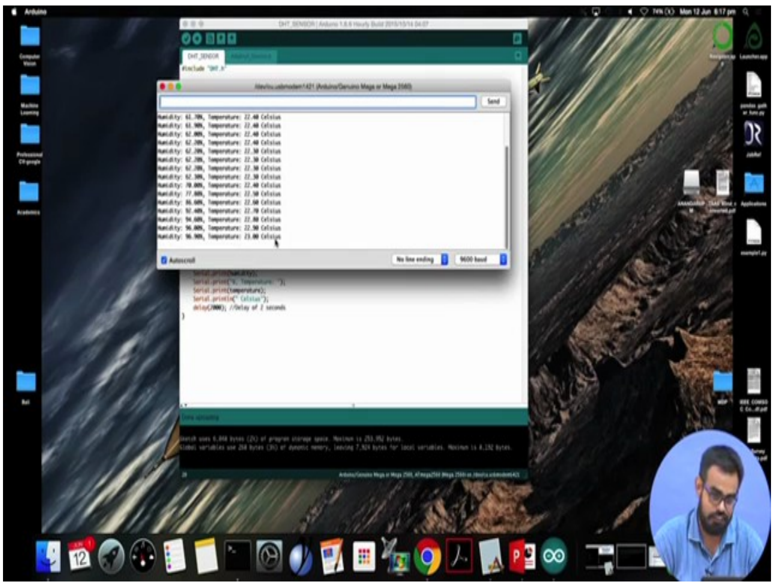
(Refer Slide Time: 14:59)



Prior to uploading will choose the board has already been chosen as Arduino mega or mega 25680 sorry 2560 the port is already set now we can safely upload our program if you pay attention to the Arduino board you can see this board over here.

We have uploaded the code to the board as you can see now I will again upload the code these two lights the tx and rx whenever you are uploading it, they will bring blink rapidly; that means, your code is being uploaded. So, now, your code has been uploaded just for the sake of it you just press the refresh button now we open the serial monitor.

(Refer Slide Time: 16:07)



As you can see your humidity and temperature readings are changing. So, may be if you can light a fire in front of it temperature readings go up, and this hoping the temperature changes a bit you see yes the temperature is changing, but very slowly 22.7, 22.8 it will keep on increasing I am hoping till it reaches my body temperature is now its touching 23, the humidity is almost 98 percent 98.6 percent and so on. So, I hope you get some ideas and you can thinker around with these stuff. So, these are some of the basic sensors other sensors you can; obviously, integrate are like dependent registers, you can integrate light bit sensors, you can integrate accelerometers gyroscope those are a bit complicated, but yes they are find to work with. So, that was the part covering sensor integration with Arduino.

Thank you.

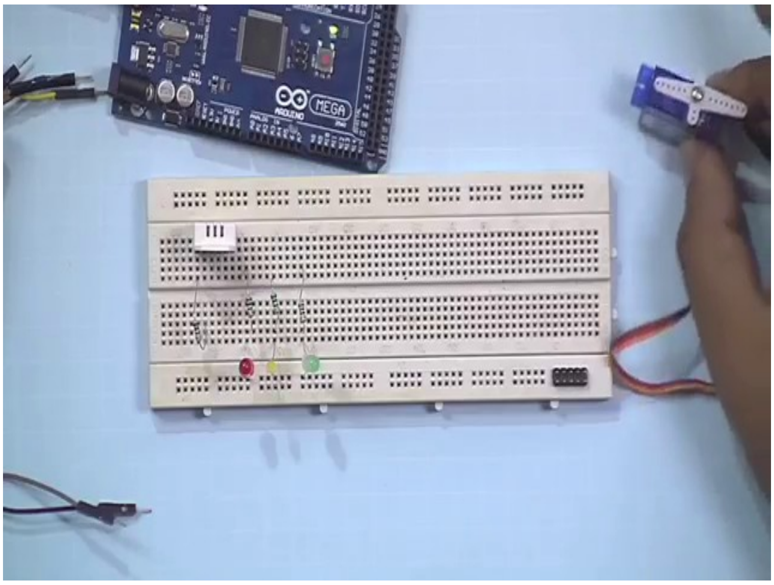
Introduction to Internet of Things

Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 25
Integration of Sensors and Actuators with Arduino- II

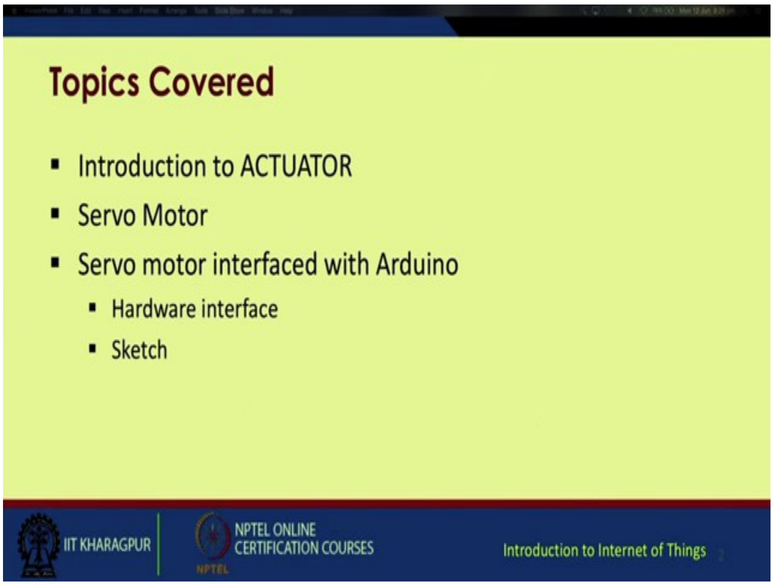
Hello, now after completing the integration of various sensors with arduino, and we have completed integration of basic actuators like lights, LEDs and the external LEDs, inbuilt LEDs. So, we will now in this lecture we will now move on to integration of a motor based actuator.

(Refer Slide Time: 00:42)



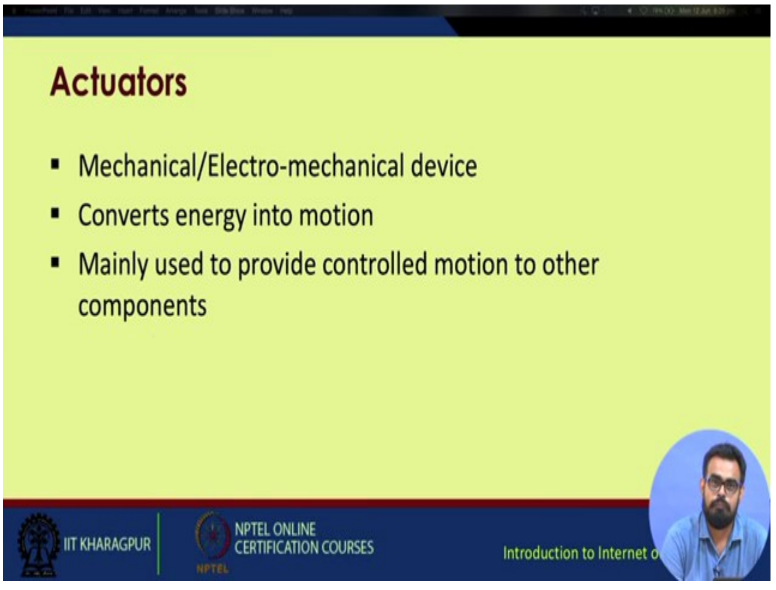
So, over here I have got a small servo motor. So, this one particularly is use for controlling the wings and tail adders of remote control planes or RC planes see. So, this is just a there is a geared mechanism inside. I do not know whether it is visible or not. So, there is a motor and you when you send pulses of various widths, the motor rotates to just that bit. So, there are various gears inside ok.

(Refer Slide Time: 01:38)



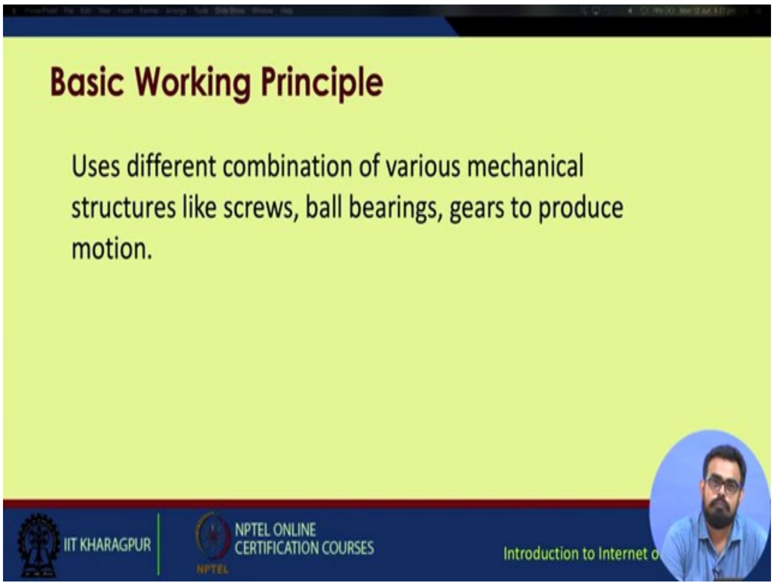
So in this lecture we will learn how to integrate this motors and make it perform according to our requirements. So, here we are going to cover the following topics, introduction to actuators, servo motors and interfacing of this servo motor with arduino. So, will first deal with hardware interface and then the actual sketch we are going to which you are going to upload on the hardware.

(Refer Slide Time: 01:58)



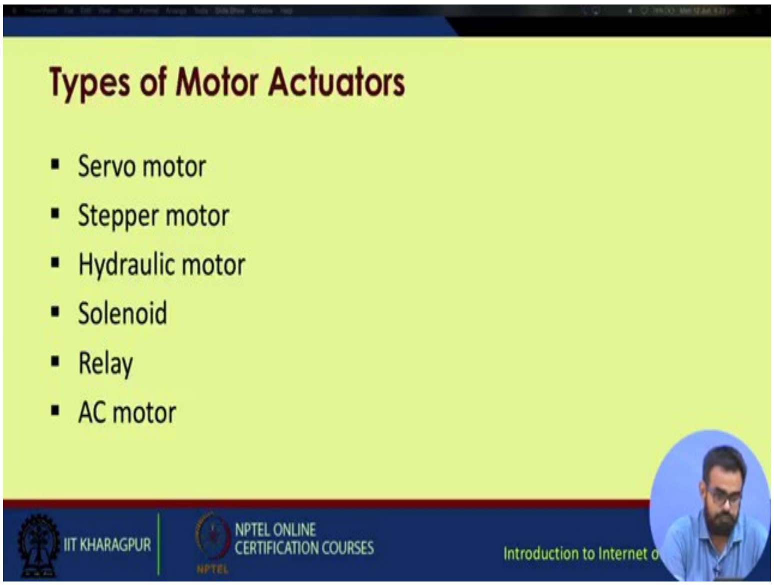
So, actuators are basically mechanical or electro mechanical devices. They convert energy or signals into motion. And mainly use to provide controlled motion to other components of various mechanical structures or devices.

(Refer Slide Time: 02:18)



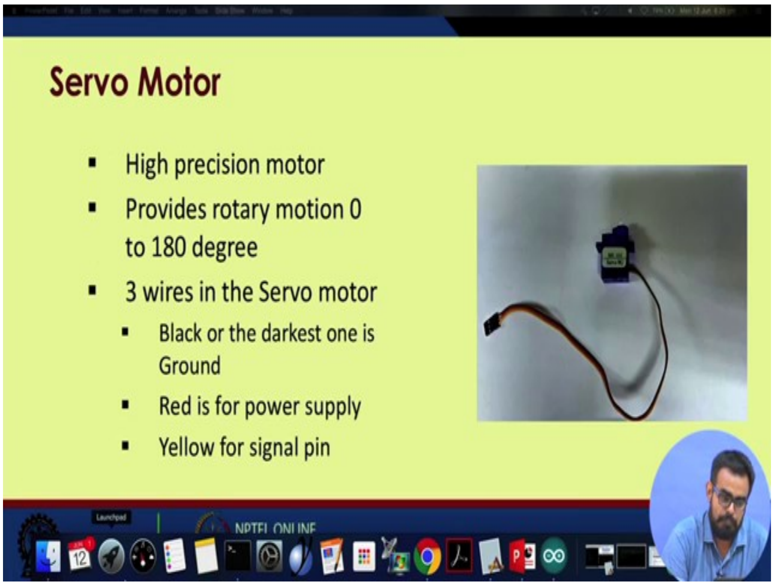
So, basic working principle is, in the servo motor you have various mechanical structures like gears and screws and ball bearings, which are interfaced with a small motor over here, and this produces very control motion, but is able to perform much more efficiently then this motor alone would have been able to. So, like generally for servers the top requirements are high as compared to normal dc motors. So, this is what is known as micro servo in the market. So, while purchasing you look for micro servo motors there are servo motors of various ranges and sizes. So, this one is this can be directly integrated with our arduino board without much interfacing or external circuitry.

(Refer Slide Time: 03:20)



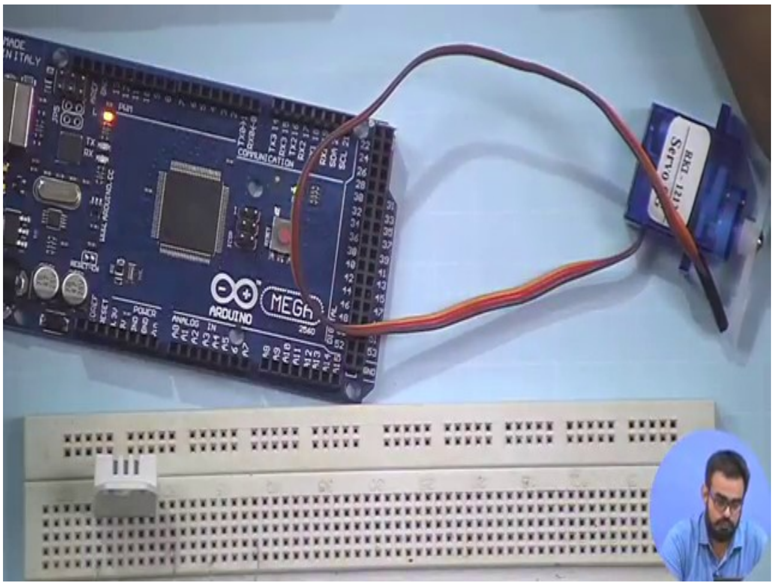
So we have various types of motor based actuators. Actually servo motor is just one of them. You have servo motors, stepper motors, hydraulic motors, solenoid relays AC motors. One point to note here is solenoid and relays are not actually motor based actuators, but sometimes solenoid may be used to drive motors and relays may be used to integrate various multiple motors with any kind of programmable circuit. So, relay is something like a electro mechanical switch, where as solenoid works on the principle of magnetism. Whenever you pass there is a coil there is a coil surrounding an iron coal whenever you pass current through the coil the whole set of magnetizes, you can use it as a magnet.

(Refer Slide Time: 04:30)



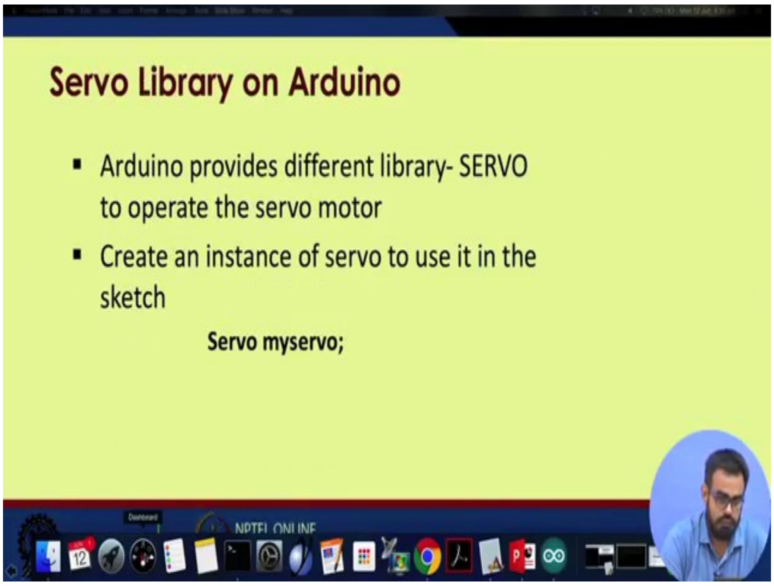
So, various uses of solenoid and solenoid walls for controlling water in pipes electronic locks and so on. So, we will focus only on the servo motor part. So, it is a high precision motor and it is able to provide a rotary motion between 0 and 180 degrees. And as you have seen it has got 3 wires one black, one red and one yellow. So, many a times you may have you may see that the black wire may be replace with brown ones also. So, the motor I have got does not have a black wire, but it has got a brown wire, but nothing to worry about this darkest wire is actually kept for browned. Then red one is for the power supply I am actually going to provide 5 volt power supply from the arduino board and the yellow one is the signal pin which is going to provide the signal for control motion to the motor, not from the motor to the device it is going to provide signals from the board to the motor.

(Refer Slide Time: 05:25)



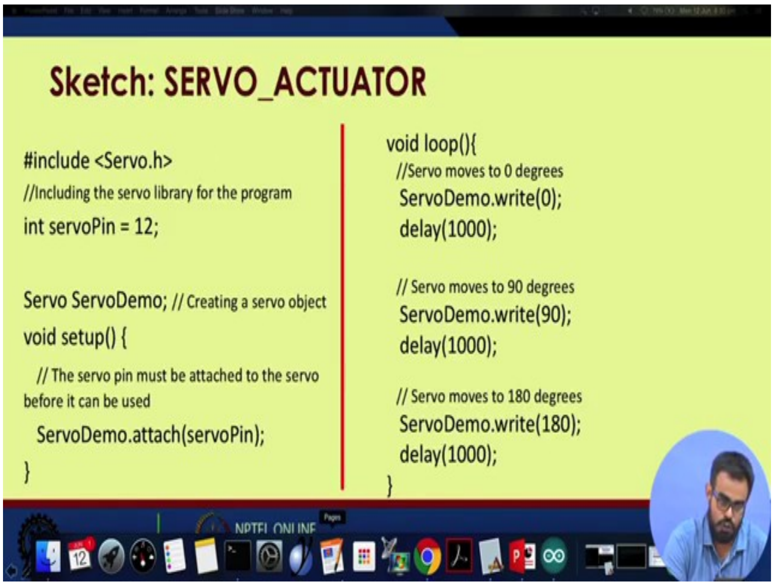
So, yet again we have to install a special library. So, following the process we follow during the GHT library installation. Just have to update a library.

(Refer Slide Time: 05:30)



If not already updated to include the servo library. And within the sketch we have to create instance called servo, Servo myservo for enabling this use of this particular servo.

(Refer Slide Time: 06:01)



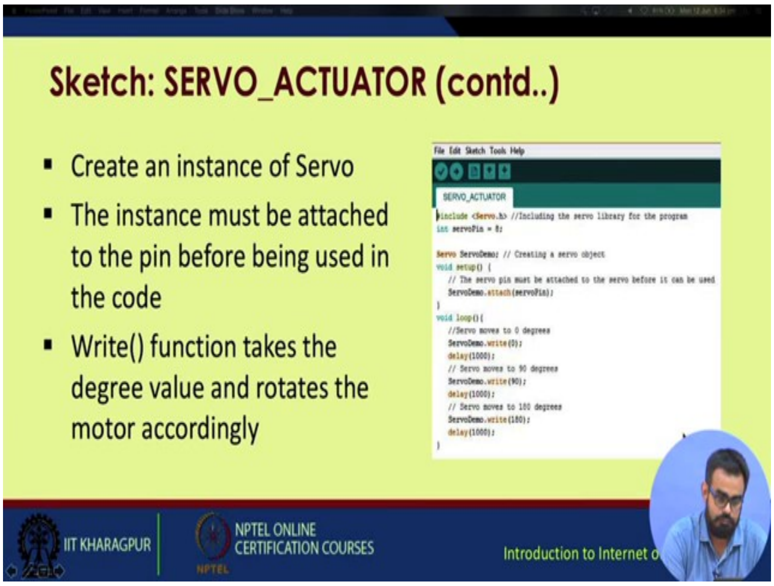
So, before moving any further let us just take a look in the library. Will just search for servo over in the library manager as you can see there are many options for servos, but I have just choosing the adafruit PWM servo driver library. So, it is already installed.

So, nothing else to worry about and one more thing, when you install a new library you can see whatever examples you had package with the normal ID when you first downloaded it. So, whatever library is you install you get some sample demo programs. So, for this adafruit PWM servo driver library. We have something called a PWM test and we are something called servo. So, we click on it a new sketch will appear. So, this is a what we called company provided sketch, just you check whether your code is working whether your hardware is working fine or not whether there is any problem with your board or whether there is any problem with your motor or other such things.

So it is a pretty big code. We actually will be doing something very simple not this complicated, so will take a look at the code. Now again we include the servo.h library function library file. So, once this has been included here we are choosing a servo pin as the pin number 12 on the at mega board. Then instance of a we create a instance of the servo as servo demo then within the setup we write servodemo.attach. These are some of the functions associated with servodemo. So, within attach it would expect the pin number to which the servo is being attached, the pin number of the processor board your using, or the arduino board you are using.

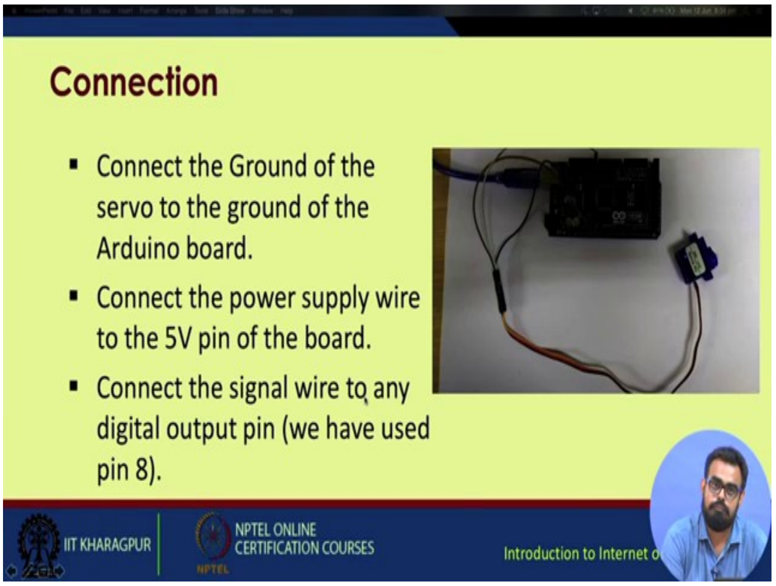
So once this setup is done we move on to the looping function. So, you have servodemo the instance of the servo servodemo.write if we write 0 it will move 0 degrees it reposition itself to 0 degrees then we put a delay for thousand milliseconds or one second then we again write value as 90 to move the servo 90 degrees again a delay of 1 second again after this we try to move the servo to 180 degrees. So, if you recall in the previous slides I have said the servo, the servo is able to move between 0 and 180 degree. So, this is the code out line.

(Refer Slide Time: 09:21)



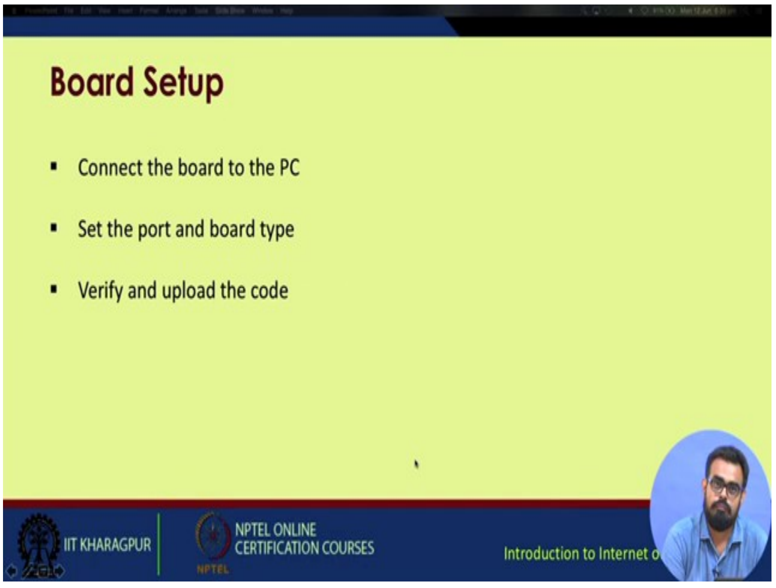
So, we have already covered these what will go through it. Create an instance of the servo the instance should be attached to the pin before it can be used in the code then; that means, within setup you write that Servoinstance.attach and the pin number. If you just call that Servoinstance.write it will not function you have to actually attach the servo with the coding part. Then the write function takes the degree values and rotates the motor accordingly.

(Refer Slide Time: 10:05)



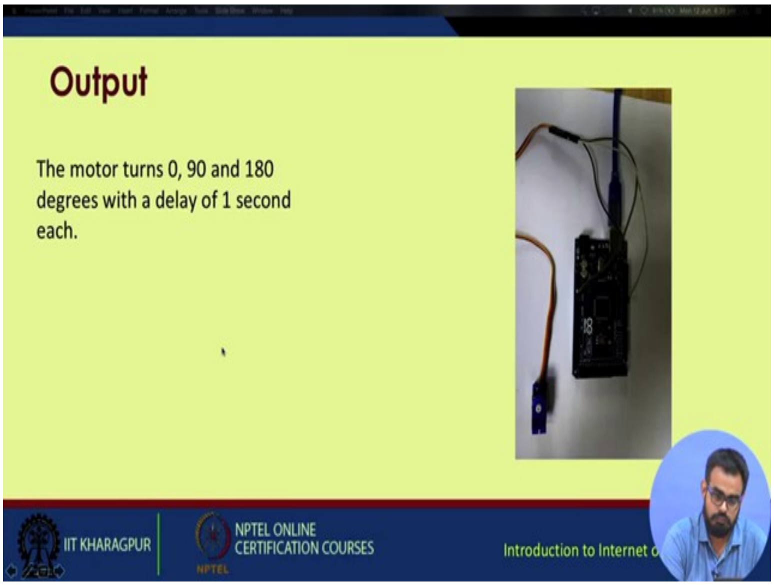
A connection is pretty simple, connect the ground of the servo that is the dark wire to the ground on the arduino board we connect the power supply wire that is generally the red wire to the 5 volt pin on the board and signal wire to anyone of the pins we may used pin 8 or pin 12 or any kind of digital input output pins.

(Refer Slide Time: 10:32)



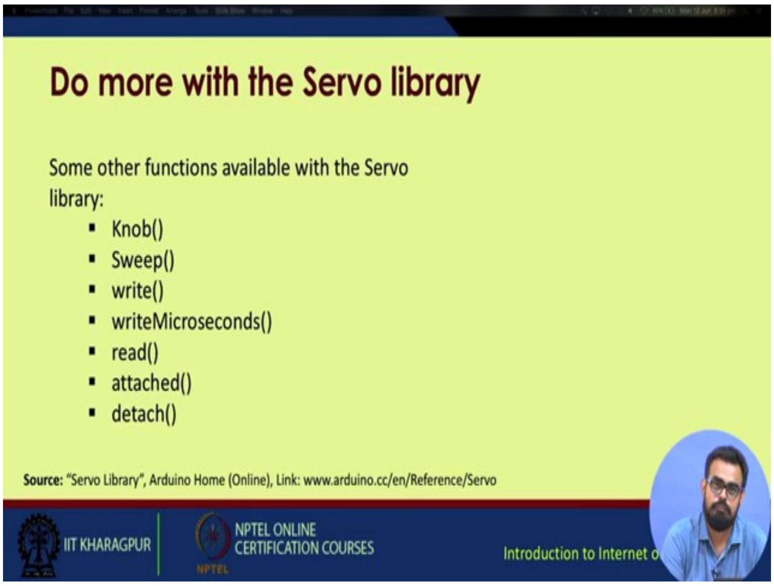
Now, try to using the board we connect the board to the PC we set the port number and the board type we verify and then upload the code.

(Refer Slide Time: 10:45)



So, the code we just discuss few slides back it will give you an output of first will turn 0 degree. It will a line itself to 0 degree then it will wait for 1 second then will go to 90 degrees, then wait for one second and finally, it will go to 180 degrees and this thing will keep on looping over and over again.

(Refer Slide Time: 11:12)



So, we will see a few variations of this code. So, there are lot more functions with the servo library we have we have a knob function, we have a sweep function write microseconds read attached detach and so on.

So, now, focusing back to the IDE. So, the code we discuss just now is already open. So, we have set the servo pin as pin 8. Or may be any one of the pins we can set let us say, we set it to pin 12 or pin 10, right. Now before we do anything will connect the servo. So, we connect the ground wire brown or black wire to the ground pin on the board. Then we connect the Vcc to the power supply pin on the board. And finally, will use a wire of another color yes. So, finally, we attach the signal the yellow wire. So, we are about to set it to pin 10, so will attach it to pin number 10. So, that is it, so this is the connection of the servo. We attached the board to the PC.

Now we check, our processor is at mega 2560, always verify. We have various variations of at mega board as you can see on the board over here. This is arduino mega 2560 if is zoom in on this region. This is at mega 2560 it is always better to be careful.

So, you see there are 2 variations at mega 2560 and at mega 1280. So, we are selected 2560 the port has been selected we verify our code. So, this seems to be no error in the code now we upload our code. Now if you focus on the motor I will reset it will first align itself to 0 then 90 then 180. Now we can try different variations of this code just take out the output signal pin. So, suppose the ID instead of 090 and 180 we give 45, 45 and 45. So, let see what it does. So, it does not seem to be doing anything. So, will try a different variation we give it 0, we give it 90, we give it 90.

So, it seems we have hit upon some error, as you can see it shows avdude time out, that is the compiler time out. So, will again check what is wrong with it. Let us reverse back to the original code - ports asset, board asset, this something wrong with this. This thing is permanently yellow will do one think we restart the code. So, we again compile the code and upload the code. So, there are various other functions we can try with the servo we have a knob, sweep, write. So, it is actually up to the user how you can manipulate these functions these libraries to build a new application. So, I hope you enjoy building IoT services with arduino boards just integrate simple senses and integrate them in various innovative ways.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 26
Introduction to Python Programming – I

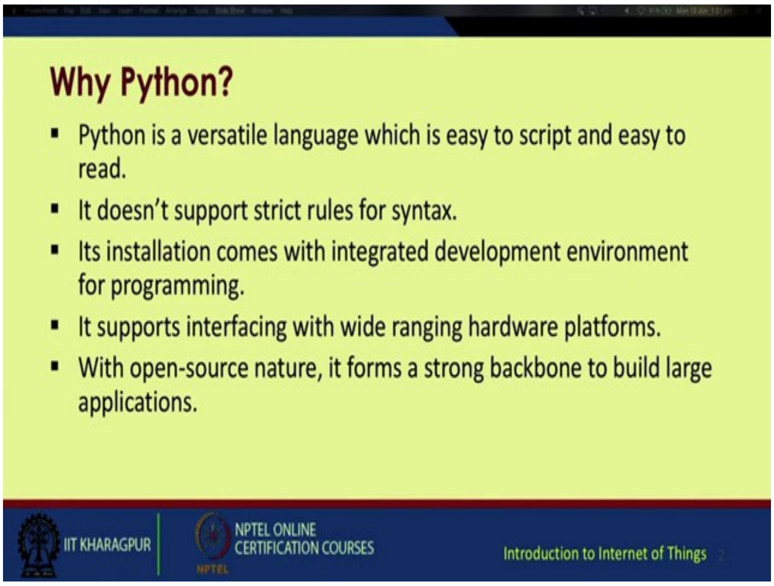
In this lecture we are going to introduce to you the language the python programming language. So, this python programming language lecture is divided into 2 parts. So, in both the parts again I will be assisted by your TA, Mister Anandarup Mukherjee. So, he is going to take you through the basics of the python programming language. So, before we start I just wanted to highlight upon that python is a very popular programming language at present. It is among other applications it is very much useful for embedded systems application development for example, IoT based application development python is very popular, there are several reasons for it one of the reasons is it is a lightweight programming language.

In the sense that from a programmer point of view first of all it is not very difficult to learn this language it is more like a scripting language it is of course, object oriented, but it is a scripting language and scripting like language, and you know it is very easy to learn this programming language. In the same way as matlab for instance is also very easy to learn python is also very easy to learn; and also you know python is supported by different embedded systems development platforms or IoT development platforms such as raspberry pi which you are going to learn in this course, but you know.

So, it supports different types of IoT devices and also you know you do not need to take help of complex libraries etcetera etcetera execution is faster and so, there were so many different advantages because of which python based programming is very important to learn particularly if you are interested in IoT based application development, and that is why you know in this course we are going to teach you a little bit of python programming to get you started and as before you know if you have your environment ready you can along with the lecture you can also code yourself. So, that the learning becomes better. So, that way it will become a enhance on experience for you. So, for all the lectures in module 2 of this course, you can do the same thing you can keep your respective environment ready. So, that you can do the do the you know the programming exercises while we teach you programming and enhance on exercises while we teach you the concepts.

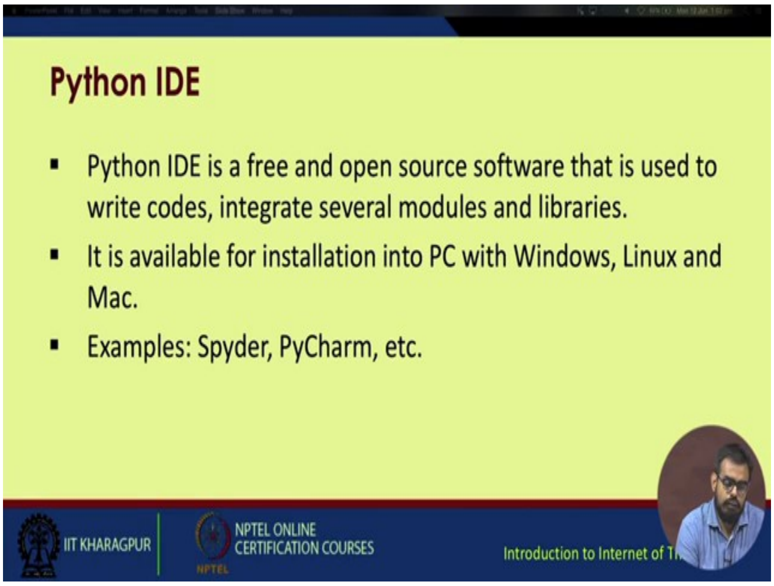
In this lecture I will be covering the basics of python programming. So, we will just talk about how to startup with the basic programming or scripting in python and the basic syntax and all those initial integrities.

(Refer Slide Time: 03:35)



So, first of all why python; now from my personal point of view python I have worked on matlab I have worked on C C++, but I find python to be a very versatile language the scripting is very easy it is very easy to write the code it is very easy to read the code and moreover it does not support strict rules for syntax. So, it is installation comes with an integrated IDE. So, the programming is actually very easy will come to that in the consecutive slides. So, and for IoT you must have seen in various online resources and lectures and courses people prefer python because it supports an interface with a wide range of hardware platforms and moreover since it is a open source platform. So, you have lots of libraries, lots of collaborative work, lots of examples available online on github on various repositories. So, it forms a strong backbone to build large applications.

(Refer Slide Time: 04:51)

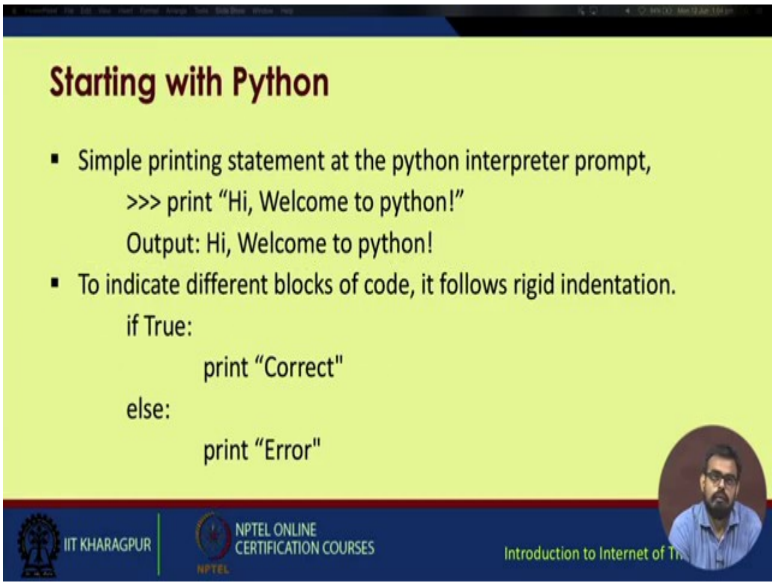


Now the python IDE is like arduino is a free and open source software. So, you can write various codes integrated integrate various modules libraries and so on. It can be easily integrated with windows, Linux and Mac machines. So, some examples of python IDE is are Spyder, PyCharm and so on.

So, my personal preference I as a personal preference I use Spyder to code my program I will show you a visual of Spyder. So, this is basically Spyder it is an editor for python as well as there is an output console over here, and for the python distribution I am using python 2.7 as you can see over here python 2.7, and I am using a python distribution using anacondas. Anaconda is a collection of various libraries and resources. So, I find it quite useful since lots and lots of library is very useful and commonly available as well as some uncommon libraries are also integrated with anaconda. So, that is also my personal preference. So, you can obviously, have normal idle ways systems. So, you have a IDE called idle idle and so on. So, this left hand side is the editor part this right hand side is the console part you can even write on the console. So, problem is you write one line and whenever you press enter it executes start line. So, that sometimes becomes bit problematic whereas, in the editor you write the whole code or the script and then collectively execute it.

So, for larger programs and systems this becomes much easier. Now to start off with python simple example is you write you want to print something some statement.

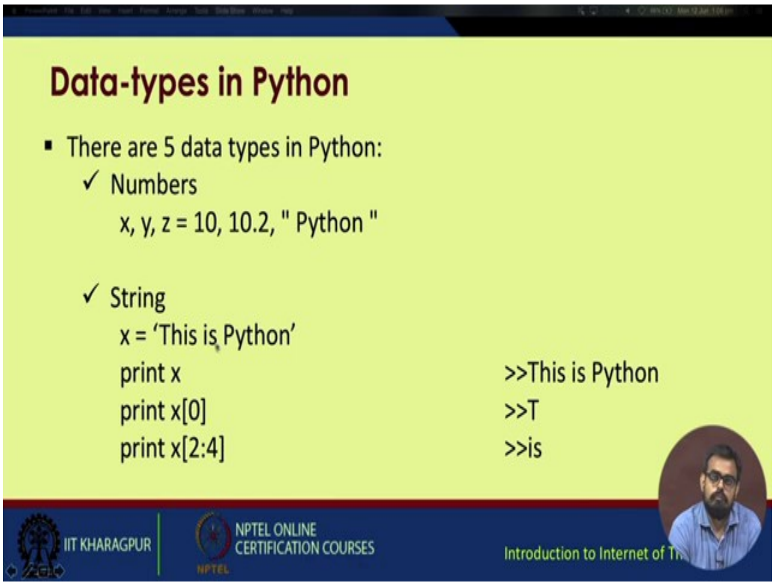
(Refer Slide Time: 07:23)



So, you just write print hi welcome to python or any other statement the output will be "Hi, welcome to python!" So, as you can see the syntax is pretty straight forward you do not need to call any libraries, you do not need any main function, you do not need other functions nothing. You just and remember whenever you encounter maybe online you encounter python codes or anything and you encounter these arrows basically means your code is being run on the console and otherwise it is for the editor you can interchange between the 2 no issues ok.

So, now to indicate different blocks of the code python however, follows a very rigid indentation policy right. So, suppose normal if else statement. So, if true then colon you have an indentation print correct else then again you go back else colon again indent print error. So, this indentation policy has to be followed whenever mainly whenever you enter into a loop. So, after one statement or this colon you have to give one tab space indentation.

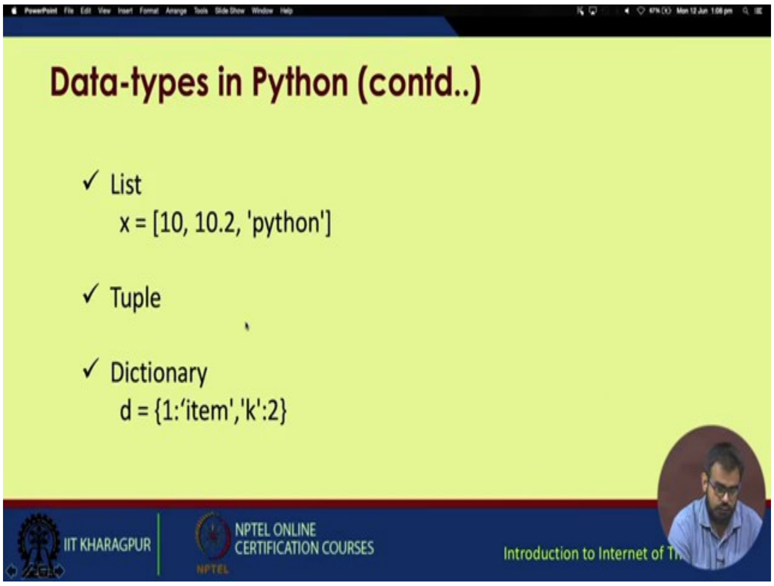
(Refer Slide Time: 09:00)



So, there are five data types in python, numbers you have x y z equal to you assigned 10, 10.2 then you write python. So, x will be assigned as 10, y will be assigned as 10.2 and z will be assigned as python. So, remember this x has been assigned with an integer value y has been assigned with a float floating type value and z has been assigned with a string right; again for the sake of toying around with how you manipulate strings. So, suppose you assign x equal to within quotes this is python; ok one more point single quotes and double quotes those actually do not matter too much you can use them interchangeably. So, over here you see the string python is within double quotes, over here it is within single quotes you can use either. So, string x equal to this is python. So, this string you are assigning to x now you print x.

So, your output will be this is python now you want to access, now this x is an array right. So, you want to access the zeroth element of x. So, you write x within bracket zero. So, this will give you the very first element that is the zeroth index element that is t, now suppose you want to access certain selected elements. So, you write x 2 colon 4; that means, select from index 2 up to index 4 and index 4 will be excluded. So, you have actually 2 and 3 right, so 0, 1, 2, 3. So, is right. So, is has been selected and this is the output of this third statement better still will take a look.

(Refer Slide Time: 11:12)



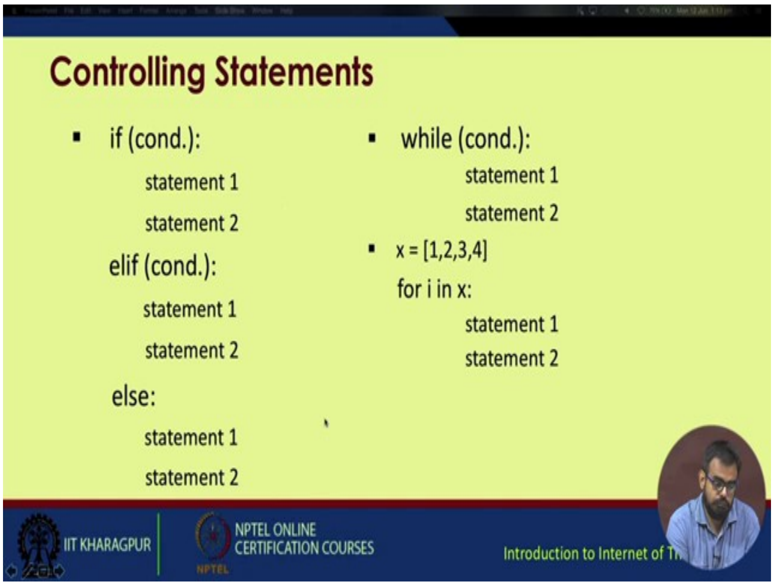
So, we will start off with a fresh console starting a new cornel. So, you can also write over here you write let us say print. So, I can execute this thing from the editor, see print this is a test message this was the line of the script and this in white is the output. So, this is a text message. Otherwise I can also write on the console itself maybe I right let us use single quotes I write hi there. So, you just get the output over here directly. So, as you can recall in C or C++ specially in C you had to call all those library functions using #include studio.h #include conio.h and so on and prior to printing you had to go to the main loop definition and all those things.

So, nothing is required for python you just start writing a script immediately. So, this was the first demo, now let us see let us assign x equal to let us assign string 2 x maybe this is a test right. So, this is a test this string has been assigned to x let us check. I just print x. So, perfect this is a test. Now I want to assign I want to select a specific element from the string let us say 0. So, x 0 it prints t which is the first character right now suppose I want to sell I want to print a specific range let us say 227 right. So, is space is right maybe we can change it to 629 right s space a right. So, it is fairly simple to understand.

Now, various other data types are you have a data type called list. So, list is an order sequence of items right you can see x equal to within the square brackets you have 10 comma 10.2 comma within quotes 'python'. So, you can assign a integers a float as well as well as a string type to this various elements of the list, then next data type is called the tuple.

So, tuple is an ordered sequence of items which once created cannot be changed or modified. Next is a dictionary; So, dictionary is an unordered collection of key value pairs used to contain a huge amount of data for example, this key is one colon, the value is item then again k, the value is 2 and so on.

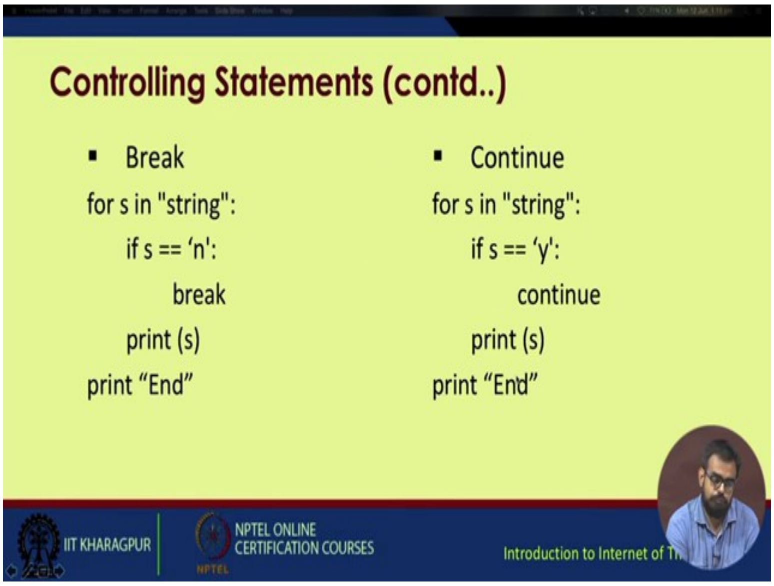
(Refer Slide Time: 16:03)



Now again similar to your Arduino programming or other languages, you have basic control statements. So, startup with if else statement. So, you have if then a condition then statement one, may be statement 2 you can have multiple statements, but remember if then the condition and then colon and since it follows a tabbing policy strict tabbing policy indentation policy. So, you need to have indentation while you enter a loop. So, statement 1 statement 2 have to be indented, then whenever you are using else if the syntax is elif, e l i f again a condition then again colon; then a post indentation you have 2 statements and finally, else which also has 2 statements post indentation

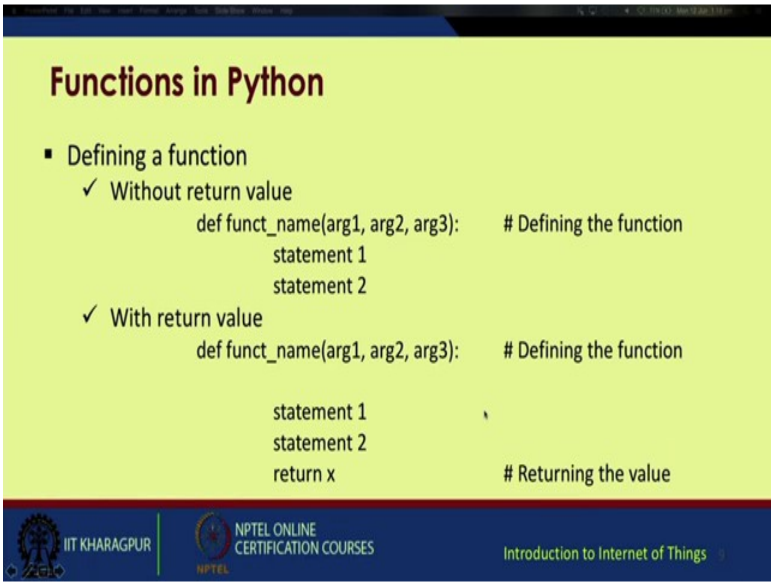
So, this is fairly simple to understand, another loop you consider is the while loop you have while condition colon after indentation you have statement one statement 2 that is it. Now for an simple example suppose x equal to 1 2 3 and 4 this is a list x is a list, now for i in x that is you iterate over the indexes one 0 1 2 3. So, for i in x you gave a statement you gave another statement.

(Refer Slide Time: 17:45)



So, you can modify it in various ways we will check it out later, then you have various other controlling statements like break. So, for s in string string may be anything. So, let us say this is the string then colon then indentation, if s equal to equal to n it compares if s is equal to n then it breaks it prints s and then prints end right and then continue. For s in string if s equal to y it continues then prints s and then end

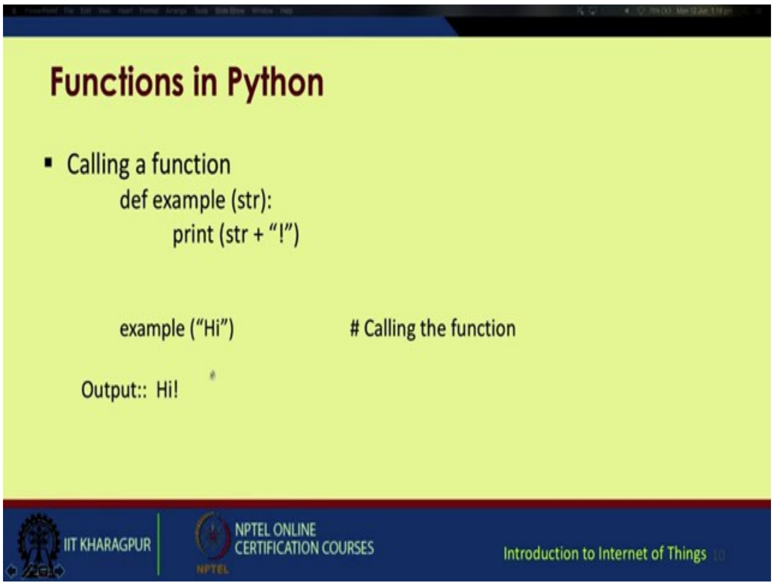
(Refer Slide Time: 18:28)



Now defining various functions in python you can for ease of your implementation for ease of your understanding whenever you are writing a very complicated function of very large program, it is always advisable to modularize your code as in suppose your code includes checking for a prime number, checking for a factorial or returning the factorial value of a function and so on like you have 20 to 30 different such functions.

So, and you need to include this functions multiple times within the complete code. So, it is always advisable you define that function once only, and just call that function again and again. So, this would not only save you lots of confusion, but also will make your code easy to understand. So, this definition of a function it can be either without a return value. So, you write as def a function name of your choice, then various arguments of your choice you can have n number of arguments depending on the function and then a colon then again an indentation statement one statement 2 that is it, right maybe statement 2 is a print statement. So, you give arguments 1 2 and 3 statement one does some operations on these 3 arguments and statement 2 prints the result of the arguments another type is with a return value. So, as you can see these things are the same, in the end there is a return function. So, maybe statement 2 is x equal to some operation and eventually it returns the value of x.

(Refer Slide Time: 20:41)



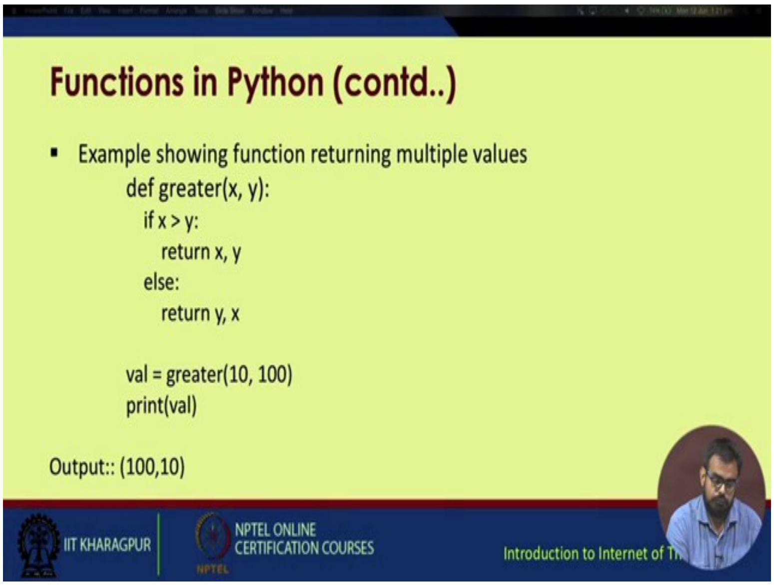
So, the function which calls this the point where this function has been called in the main code it will have x return to it right for example, whenever you are calling a function suppose def example("str"), then print str plus this not character. So, your example outside this function, you just call this function example hi and your output is hi it would be better.

If we do get to a little hands on let us say I define a function as capital IOT, give arguments as xy and z colon io statement as may be a equal to x plus y minus z right and it returns the value of x right. So, my function has been defined now outside this function maybe later on I just call this function IOT, it will require 3 arguments maybe I will right 5 4 3; right and since I will be expecting a return value I assign this function a variable sorry I assign this function to a variable. So, let the variable b b b equal to IoT 5 4 and 3 right let us see what happens. So, first we need to save this code now execute this code all at once ok.

So, this code has been executed, but I forgot to give a print statement let us print b now will execute this again, as you can see your arguments were 5 4 and 3. So, the first 2 will be added and the third will be subtracted from the result. So, your result will be 6 right. So, this is a result. So, this is pretty simple I guess.

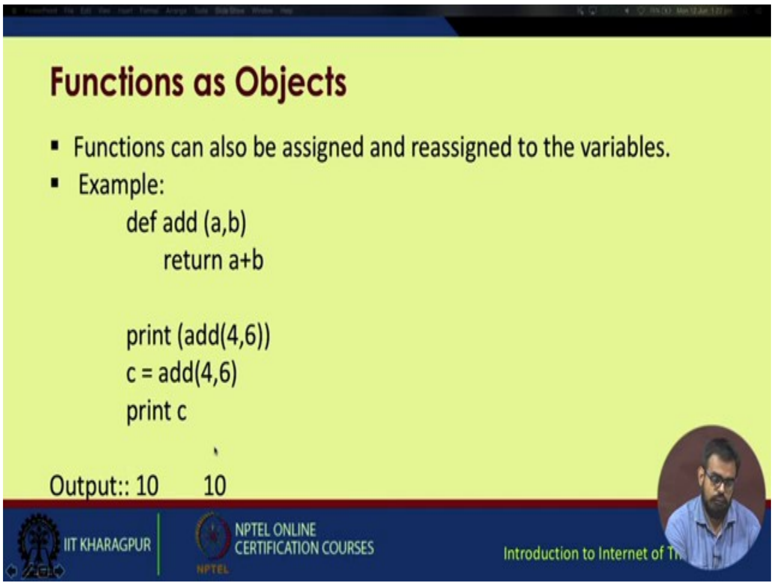
Now since defining a function has been covered. So, similarly you can define various other function suppose you take to arguments and define which one is greater or which one is lesser.

(Refer Slide Time: 24:17)



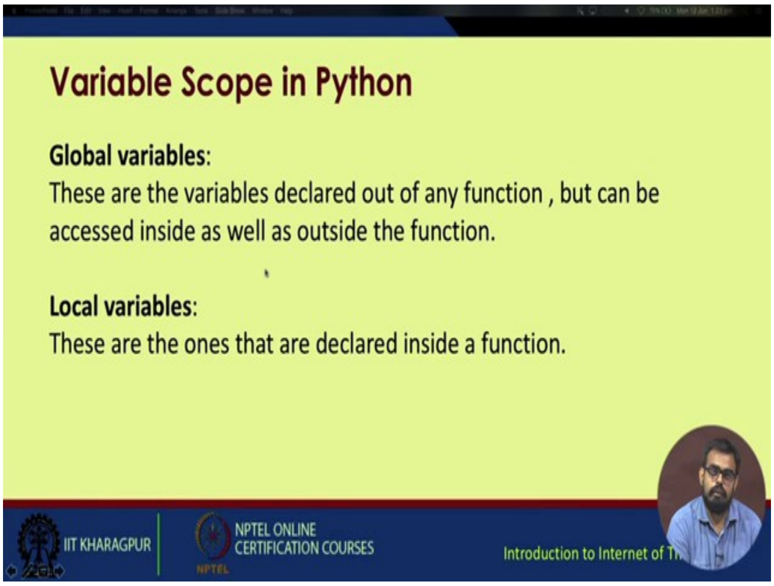
So, you check whether x is greater than y it will return x and y else it will return y and x. So, outside this function definition you assign you assign this function to a variable as greater 2 values as 10 and 100 print val. So, 100 is obviously, greater than 10. So, if this happens it will return this one y and x. So, your output is 100, 10.

(Refer Slide Time: 24:28)



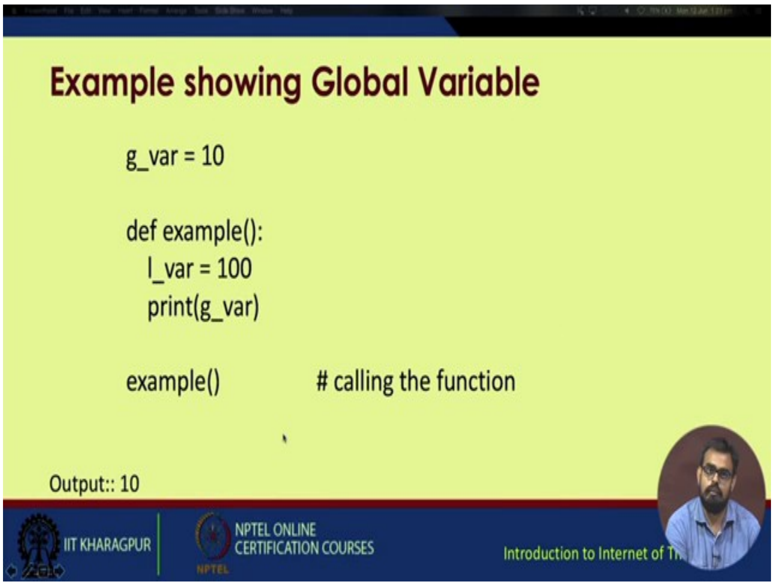
So, it is pretty straight forward now functions as objects. So, whenever you are these using these functions these can be assigned and reassigned to various variables. For example, you write a function for addition you can directly do the operation at the return statement itself, now you print(add(4,6)) and again you assign add(4, 6) to c and then print c, so for both the output will be 10 right.

(Refer Slide Time: 25:24)



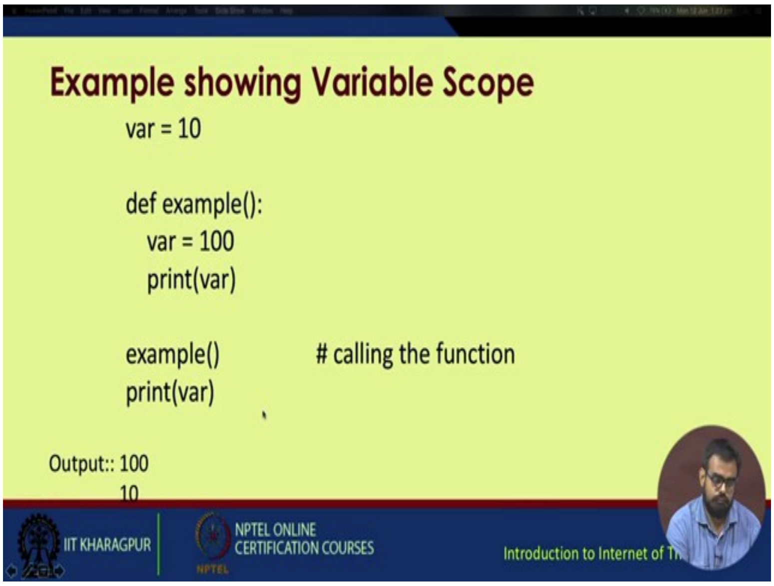
So, there are 2 types of variable scopes one is the global variable that is accessible those variables are accessible all across the your code, and these variables can be accessed outside as well as inside a function and local variables these are the once which are only declared inside a function and cannot be accessed from outside.

(Refer Slide Time: 25:46)



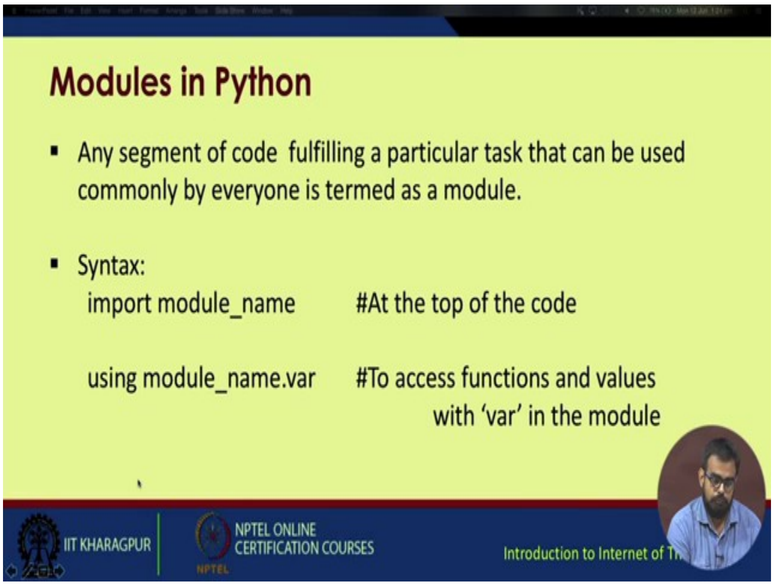
So, for example, before a function suppose the definition of a function def example these are some operations you define a variable as g_var = 10. So, this and another variable as i_var = 100. So, within example you can call g_var, but outside example you cannot call i_var.

(Refer Slide Time: 26:15)



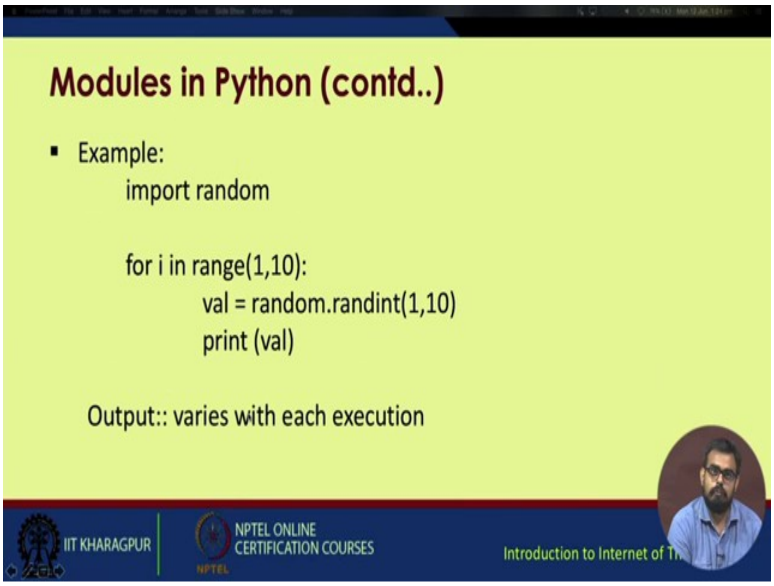
So, basic variation again you have a variable as 10 with an example variable equal to 100 you print this var and you call this example and again print var. So, what will happen is within this example it prints var. So, this var will be 100 which is locally assigned right. So, initially it was the global variable is 10, but this overrides that value and reassign hundred to it, but outside this function this is not valid.

(Refer Slide Time: 26:59)



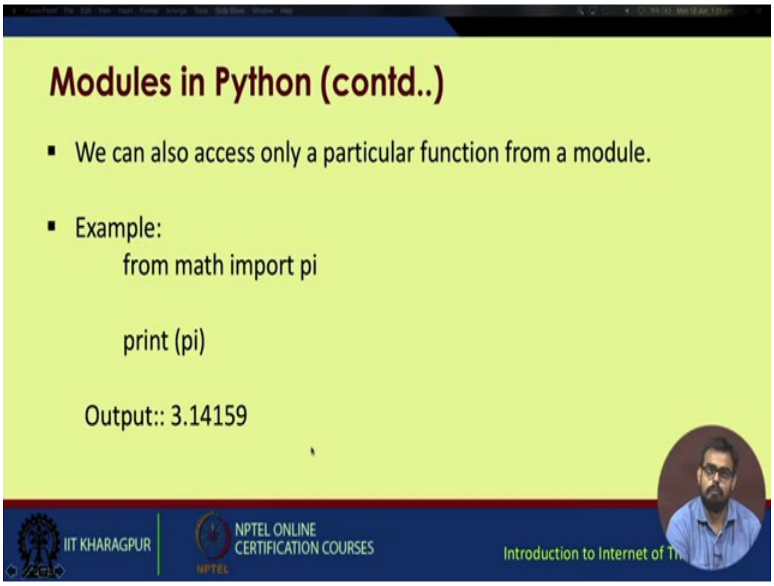
So, for the second print statement it will print the global variable 10. So, you have various modules in python. So, you import the module name now you can also call for the extension for example, you import random.

(Refer Slide Time: 27:11)



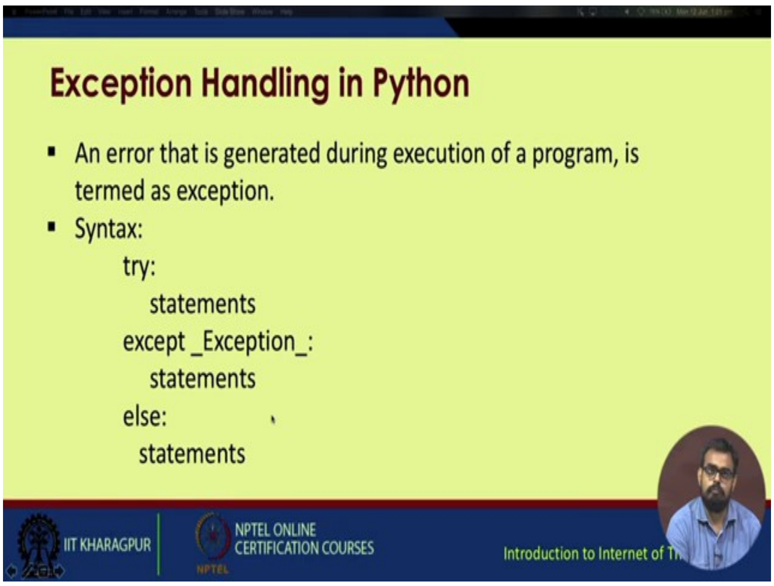
Now, the random has many such functions as random integer 1 to 10 and so on. So, for example, the script for I in range one to ten as when you have a list of 9 numbers 1, 2, 3, 4 up to 9 value is random.randint(1, 10) it will randomly generate numbers between one and 10 and print value. So, since this is random number generator it will the output will vary upon each execution. So, it is better you try this yourself.

(Refer Slide Time: 27:51)



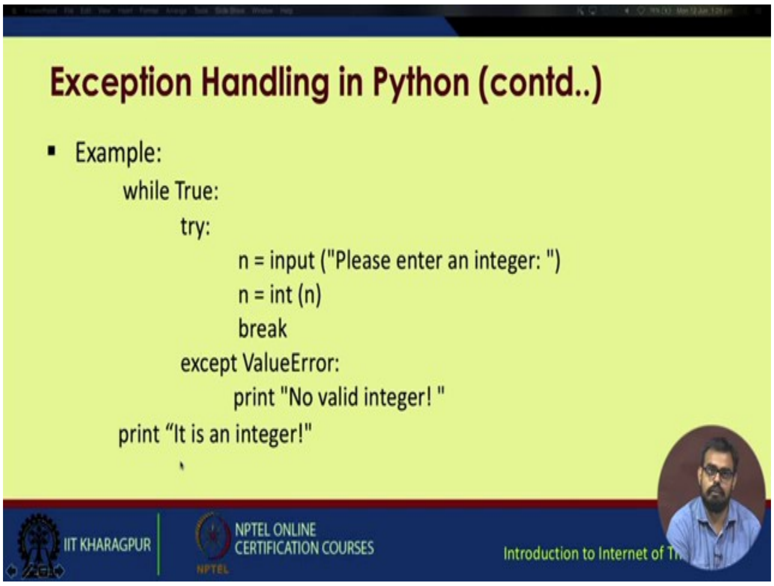
So, you can also try a particular function from within a module like from math import pi and then print pi it will just print the value of pi.

(Refer Slide Time: 28:06)



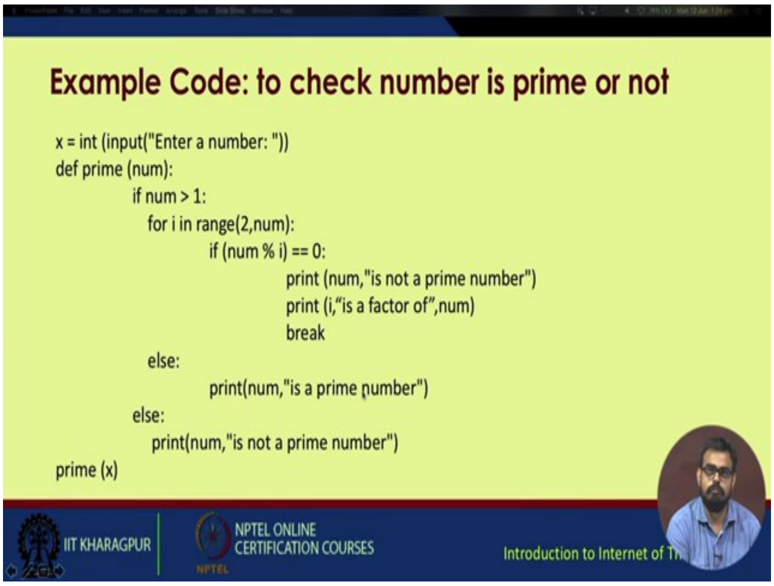
Now there are various exceptional handlers in python, these are mainly used for debugging or in case of errors in various complicated scripts they will give you the exceptions like try then statement except exception statements else statements one example is while true try.

(Refer Slide Time: 28:28)



So, within this type the function will execute this statements these statements will execute if it there is some error. So, it catches that error and accept the value error not a valid integer. So, whatever in number you are inputting it gets stored in n it is converted into integer and you break it and after that this print statement executes if you somehow erroneously input string number to it string or the character to it. So, it would not be converted to integer. So, it will print not a valid integer so, it is better you try this code also.

(Refer Slide Time: 29:12)



Another example code is to check whether a number is prime or not and so on. So, these kind of complication complications can be increased and you can have multiple nested loops you can have multiple functions, function within the function although it is not advisable, but still. So, this was it.

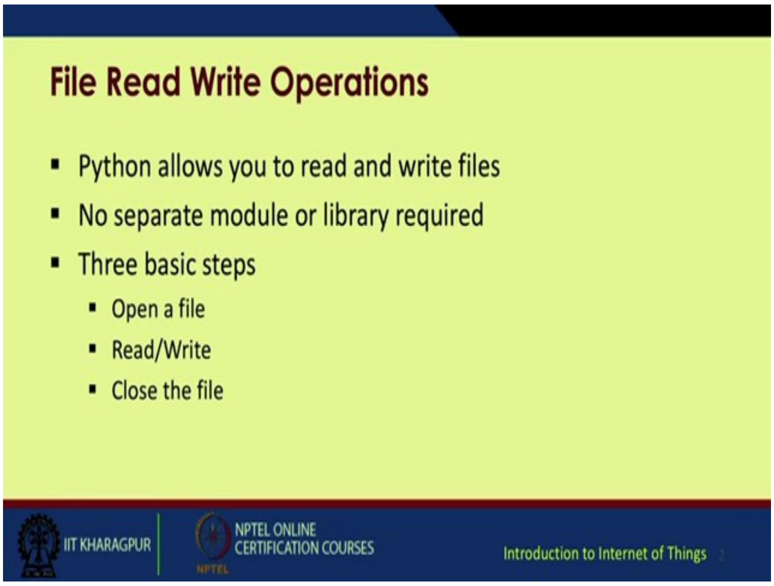
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 27
Introduction to Python Programming- II

Hello, in this lecture in Continuation to Python Programming, I will be covering a few interesting applications, you can develop using normal python programming.

(Refer Slide Time: 00:34)



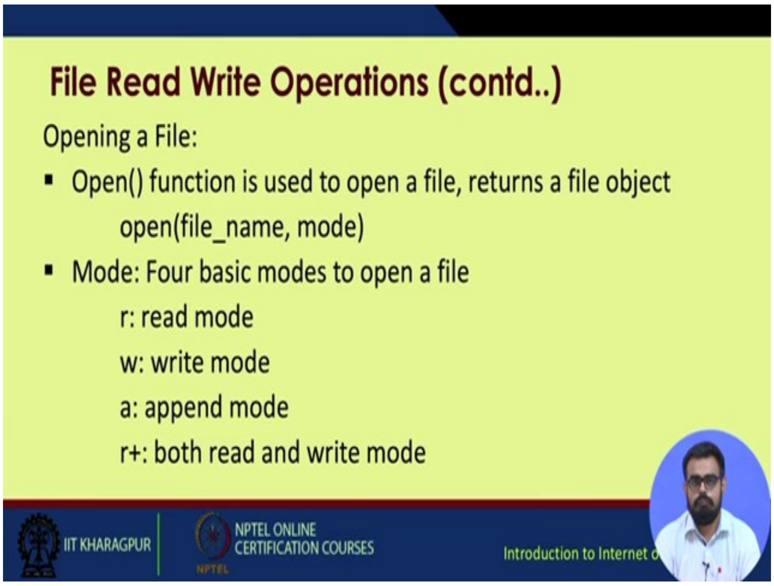
So, to start off with, we will be covering a few basic operations starting from file, read/write, operations, we will be dealing with normal text files as well as csv files. Csv are basically comma separated value files. So, each value in the file is separated by a comma.

Next we will move on to your developing a network socket using python scripting. So, we will develop two parts. First, we will develop a udp host or a server and a udp client and in the third part, we will be dealing with some basic image, read, write operations using python PIL library. So, to start off with the file read write operations as necessary in normal IoT based applications, imagine your sensors or lots and lots of sensors are uploading the data on a particular database or a file system.

So, the data is separated, separately stored or data is collectively stored using various time stamps or signatures or identifiers. It may be in a text file for small scale systems, it may be in a csv file, but larger scale systems and then, again for much larger implementations of IoT, people normally prefer using data bases like MySQL or Oracle ecetera. So, python allows us the functionality to read and write files.

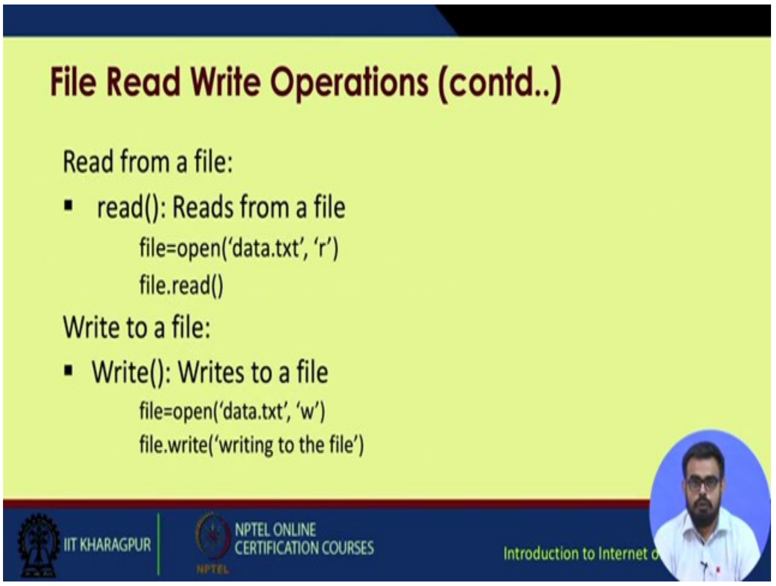
Generally no external module or library is required. It is available with the basic distribution of python itself and while reading or writing a file, three basic steps have to be followed. First and foremost is opening a file itself. Next is reading or writing operation and third one is closing the file. So, keeping these three in mind, we will dive into a bit more details about these.

(Refer Slide Time: 02:31)



So, the open function is used to open a file and return a file object. That means, whenever you give the syntax, open first argument is filename and the second argument is mode. There are the following four modes, r for read or w for write, a for append and r plus for both read as well as write modes. Through reading from a file as you can see the syntax is pretty simple.

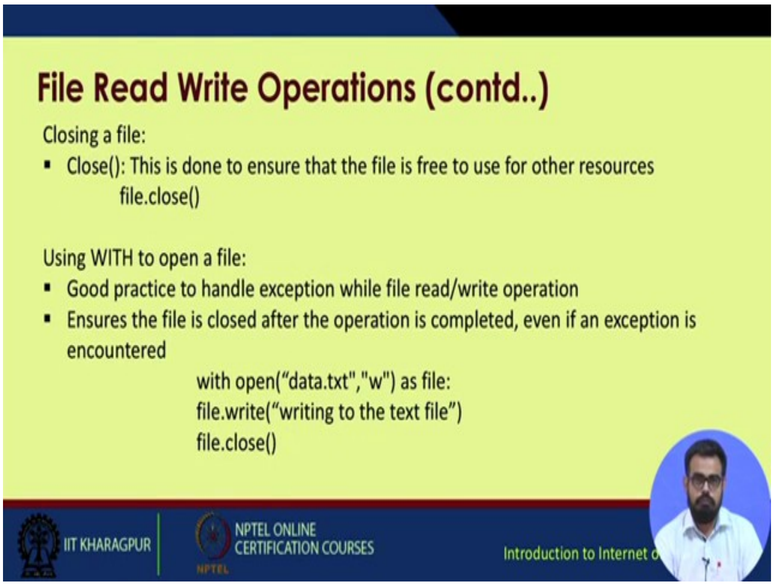
(Refer Slide Time: 03:01)



So, imagine you have a file text, file named data data.txt. So, we are going to attempt to open it using this line file equal to open('data.txt' , 'r') point to notice both the filename as well as the mode are within quotations because these are taken as strings and then, in the next line we have file dot read. So, this file equal to open function, the file is actually a variable. You can assign any other name to it. Next is the writing to a file part.

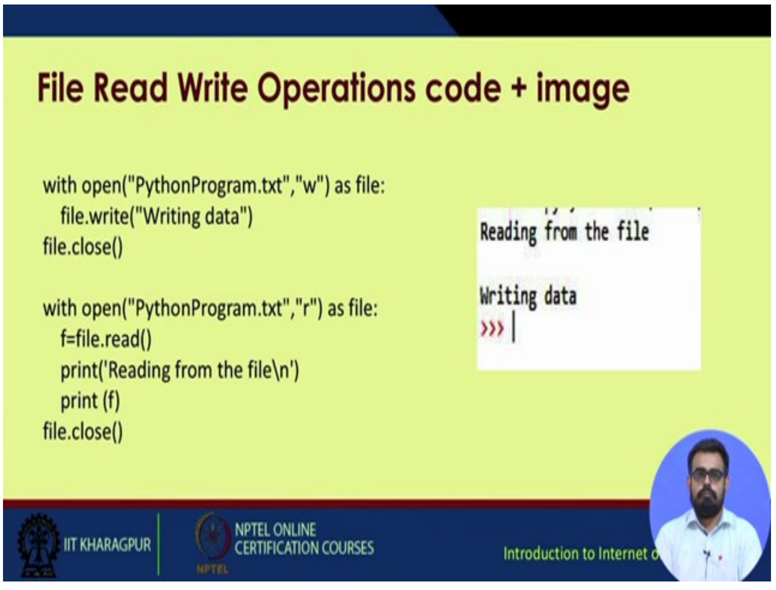
So, whenever we are writing to a file, again we have to open the file. Only the mode changes from r to w, then file.write and within arguments, you just put in the string here about to write to the file you can. Obviously, put various variables you can store your incoming sensor data and some variable and iteratively write those variables using the file.write function.

(Refer Slide Time: 04:14)



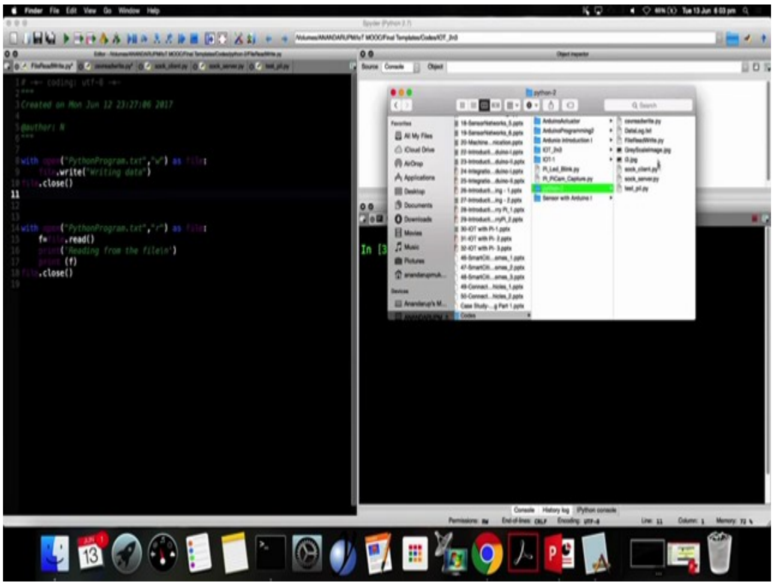
Now, at the end, once a file access has been done, you must ensure that your file handle is closed by using this function file dot close and whenever since in normal normal scenarios specially IoT based scenarios, there is a significant need to iteratively access the same file over and over again. So, using this script with open data.txt in write mode as file in file.write, we write the string which has to be written to the text file and then, we release the file handle by calling file.close().

(Refer Slide Time: 05:02)



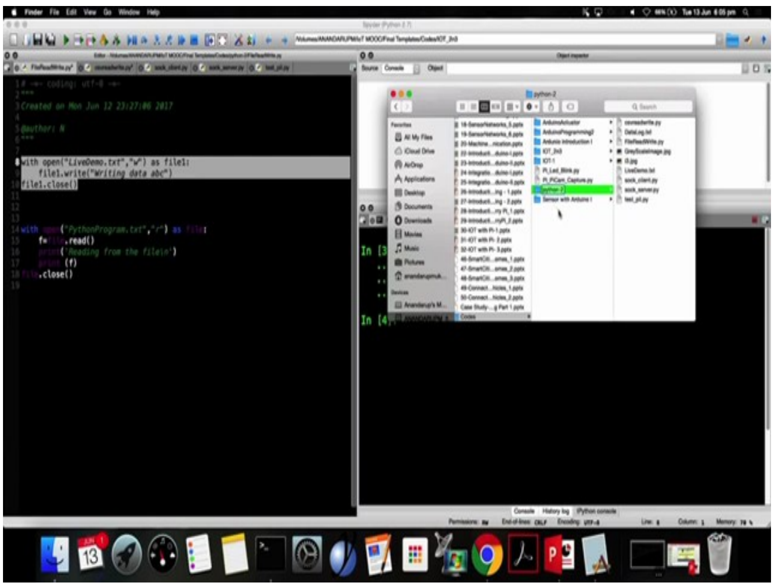
So, it would be better if we give a bit of hands on to this thing. So, as you can see I have already kept the program ready.

(Refer Slide Time: 05:29)



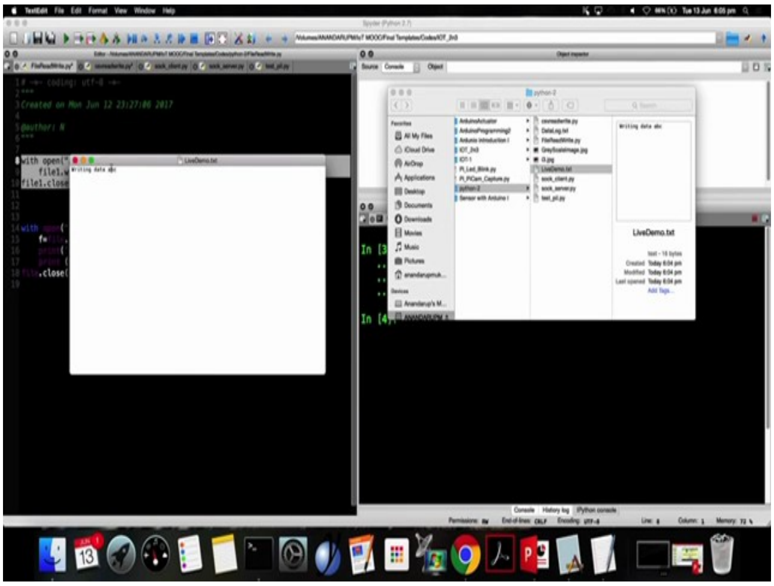
So, we just have to call a file, any file name we want to put over here. We have python program.txt. We can change it to something else also. So, my files and folders basically recite in this directory. So, as you can see there is no python program.txt file in this list. So, maybe we can just change the name to live demo.txt.

(Refer Slide Time: 06:26)



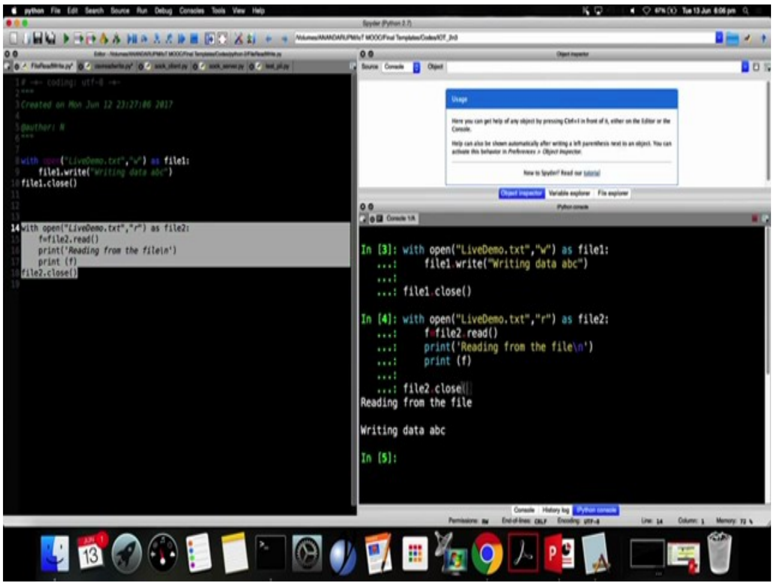
Then, in the next line for speed, iteratively we have to write something on it. So, with open live demo.txt as w or in write mode as file, let us call it by another name file1. Then, file1.write, we are writing this writing data abc and then, we release the file handle by calling file1.close(). So, once we run this thing, we have executed this thing, these three lines of code. Now again we will check the directory.

(Refer Slide Time: 07:40)



Here we have the file named as live demo.txt. We open it as you can see the intended data has been written to the text file. So, this was part one. Half of the job it is reading that is writing to the file. Next part comes that is reading from that file.

(Refer Slide Time: 07:56)



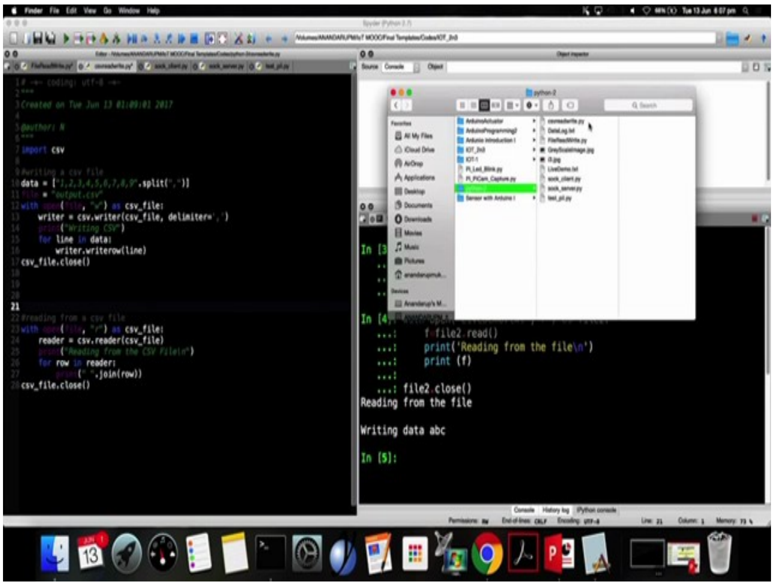
So, now I have a filename live demo.txt. So, in the same manner as before I will open the same text file, but in read mode. So, I will change the mode to r. Initial it was w, now changing it to r.

So, I am opening the file mode in read opening, the file in reading mode assigning the variable let us call file 1 or maybe just for the sake of it file2, f equal to file2.read. Then, I print reading from the file and then, again I print whatever has been read and again I release the file handle. I release this file 2 by calling file2.close(). So, once again I will execute these lines.

See once this execution is complete, the first line has been printed reading from the file. This was a first print statement and then, if you recall we had earlier written data to the text file like writing data abc. So, this has been extracted from the text file and put up and printed on the console. So, this was part one, reading and writing from normal text files. So, there can be multiple operations, we can consider while doing file read write operations.

So, not to go into that much details, you can easily avail various resources online to check those.

(Refer Slide Time: 09:50)

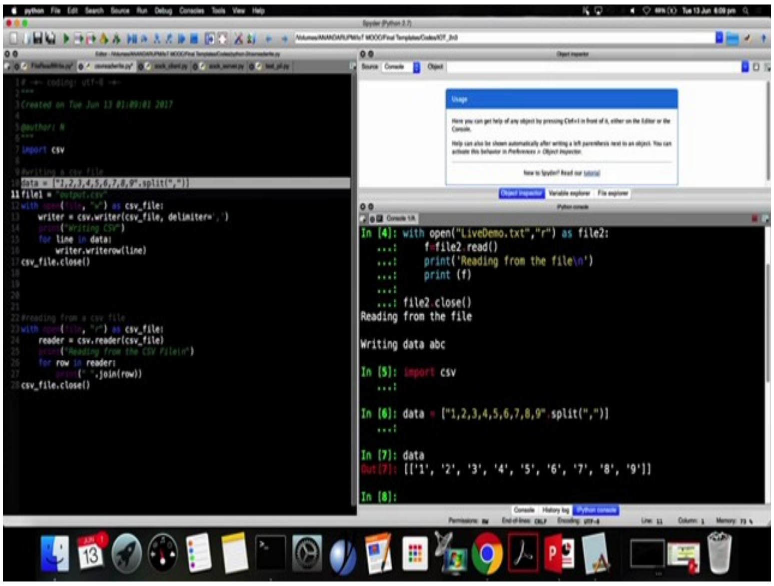


Another common thing being used is this csv file format or comma separated values. You can again check I do not have any csv file in my directory list. So, I am using this script csvreadwrite.py. So, once this has been executed, it will generate a file with the extension dot csv.

For this I have to import an external library or csv library. Once this library has been imported, I define the data. I want to write to the file. First I will write to the file, then once the file has been created and the data written to it, I will read from that same file. So, one point to remember is whenever I am trying to open a file in write mode, if the file does not already exist, the system will automatically create that file, that same file.

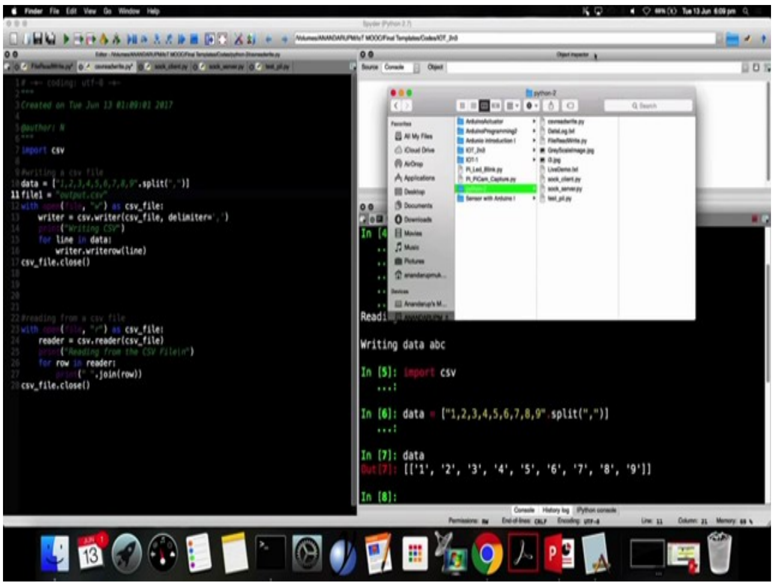
So, I am giving the file name as output.csv. Let us name the variable as file1. The data is within since we are putting up a string data. So, we are giving 1 2 3 4 upto 9 and we split it using the comma character, you can use other characters also like semicolon, colon so on, but for the sake of demonstration, I am just using a comma. Let us see what happens when I execute this line. So, this script has been executed and I will check what is stored in this.

(Refer Slide Time: 11:37)



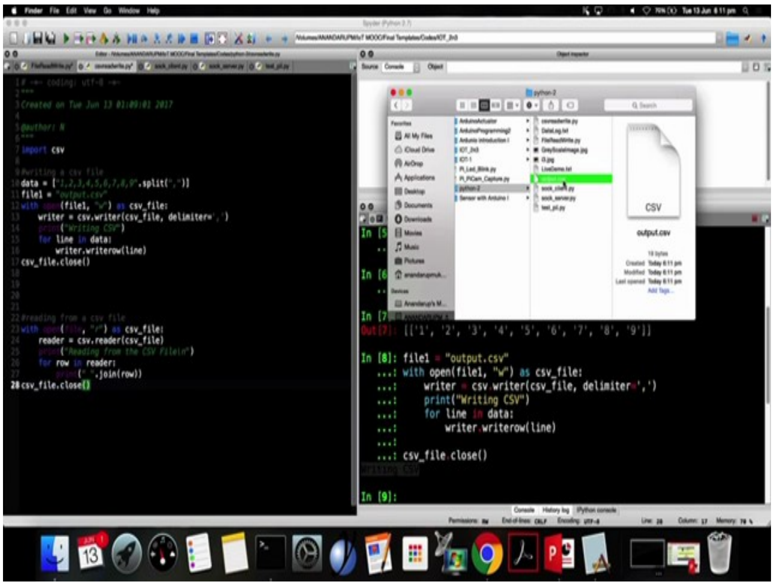
So, you can see individually you have various strings separated by comma. The first string is 1, second string is 2, and so on upto 9. So, whatever input you had given, it has been individually separated into substrings. Then, next I open a I create a variable file1 and try to open output.csv. So, in this directory, we have nothing called an output.csv file.

(Refer Slide Time: 12:16)



So, we are assigning this output.csv string to variable file1. Now, again using with open file1 in write mode as csv file, we call another variable writer equal to csv.writer .

(Refer Slide Time: 12:35)



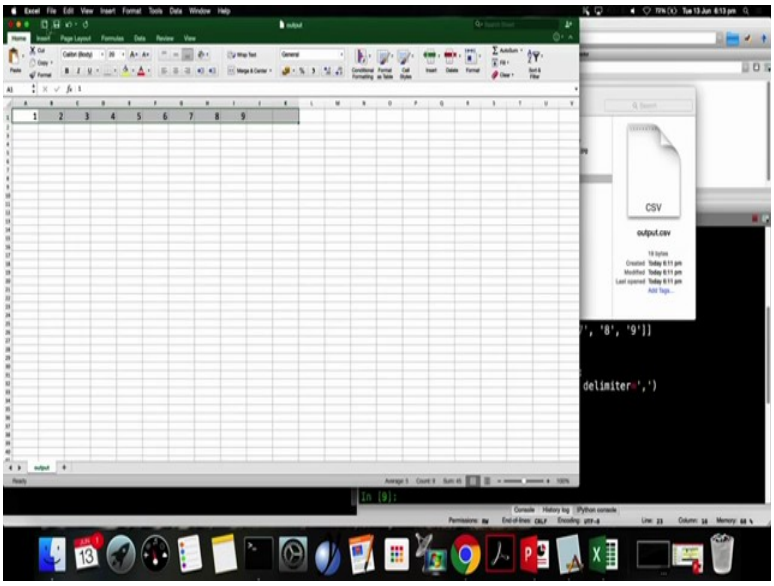
In csv file delimiter is comma. Suppose you had given a semicolon as delimiter, you could have replaced this comma by a semicolon and we print a normal statement to check whether it is working fine or not and then, whatever data is being written into the file.

So, we call the writer again and each row report in a separate value like 1 in the first row, 2 on the second row, 3 on the third row and so on. Then, eventually we call the close function file.close(). Now, let us see what happens when we run this collectively. So, my print statement writing csv has been executed. Let us check. So, the file name was output.csv . Yes we have a file called output.csv over here.

So, by default it is opening with microsoft excel. So, for my system, the default csv file viewer is microsoft excel. So, it is directly opening through excel. This will take some time. Let it load. In the meanwhile, we will look into this writing from a csv file part. Now, again we go on with open in a name variable file1 in read mode as csv file and reader equal to csv reader csv file.

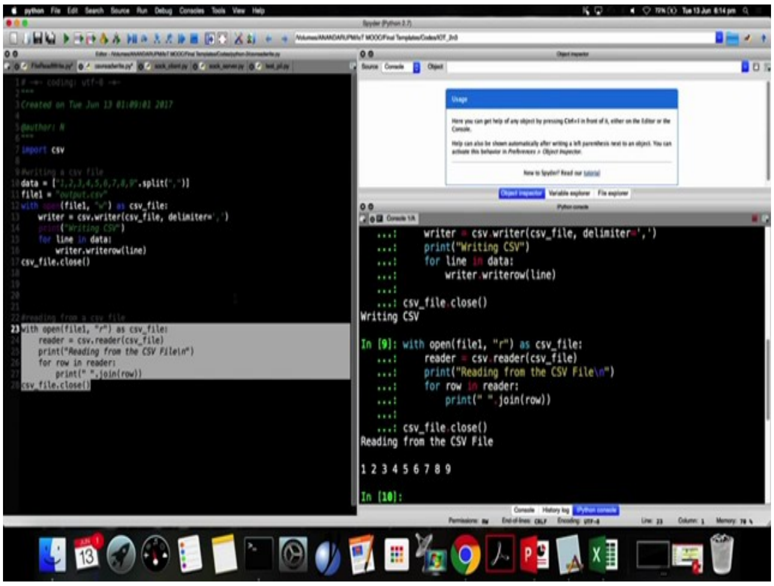
We print that it is reading from a file that is we will just give an indicator to the user that this script is executing and then, for each row being read by the reader, the value being read will be printed one at a time and eventually, we will release the handle by calling the filename.close() function.

(Refer Slide Time: 15:34)



So, I have finally managed to open my excel file. As you can see the values 1 2 3 4 have been written in separate columns. So, instead of these static values, we can acquire data from various sensors and we can keep on updating this csv file in a iterative manner. So, this will give me a database, a rudimentary database, ok.

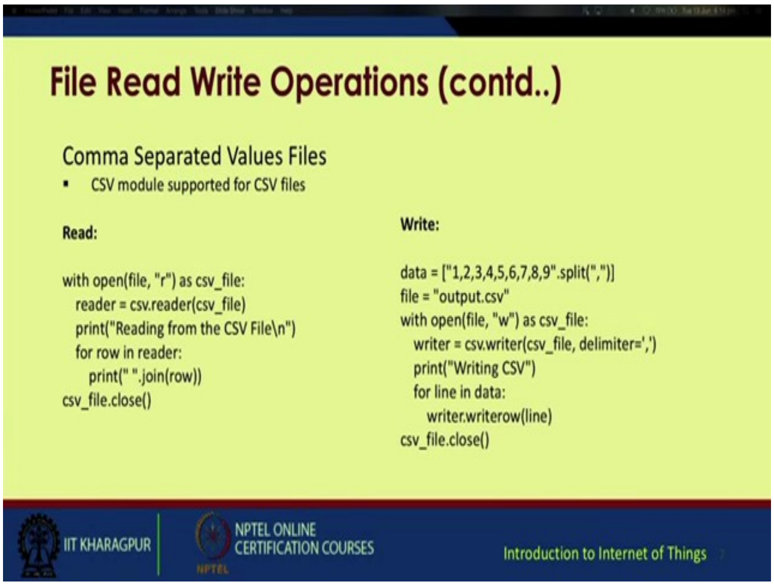
(Refer Slide Time: 16:28)



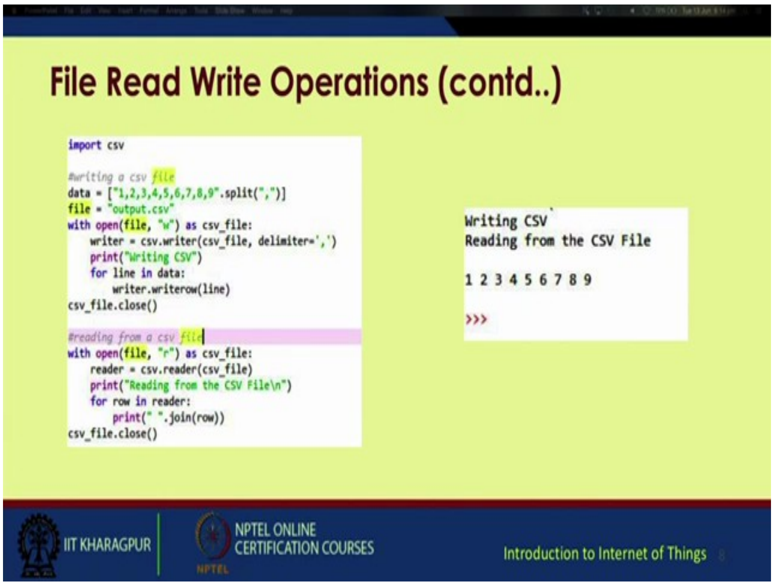
Now, I know my output dot csv file is in place. I will try reading from that file. Now, the first after the script has finished executing, the first print statement was reading from the csv file and it has read the values individually like 1 to 9. So, I hope this was quite easy. We will move on to the next part.

So, we have already completed these. Now, the next part is a, but interesting since it will deal with various images.

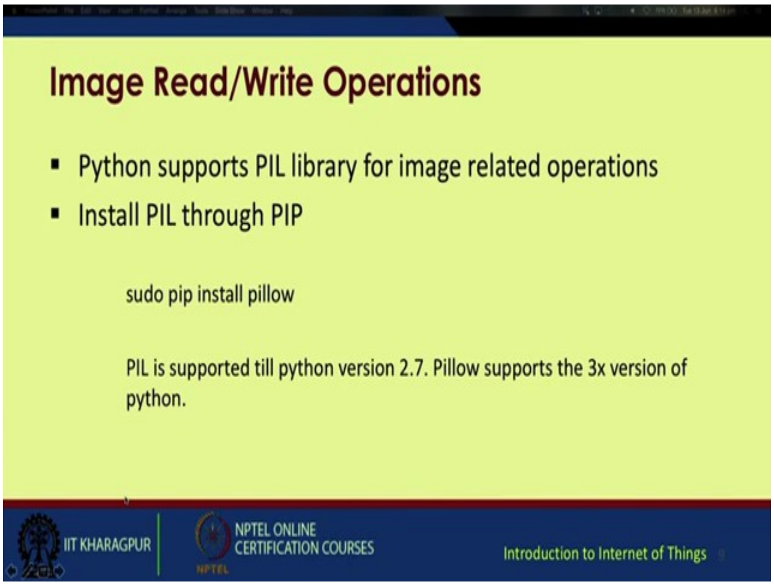
(Refer Slide Time: 17:05)



(Refer Slide Time: 17:07)



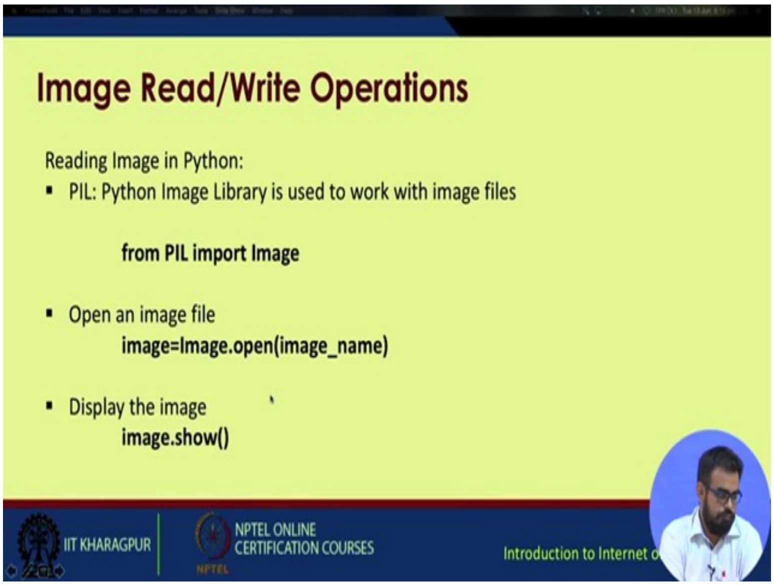
(Refer Slide Time: 17:10)



So, we will functionally work with image read write operations. Now, python supports this library called PIL or python imaging library. This is generally used for image related operations. So, if by default your PIL is not on the system, we use PIL or we acquire PIL using sudo pip install pillow.

So, normally PIL is supported in the python version 2.7 till 2.7, otherwise for higher versions PIL needs to be installed to get this working.

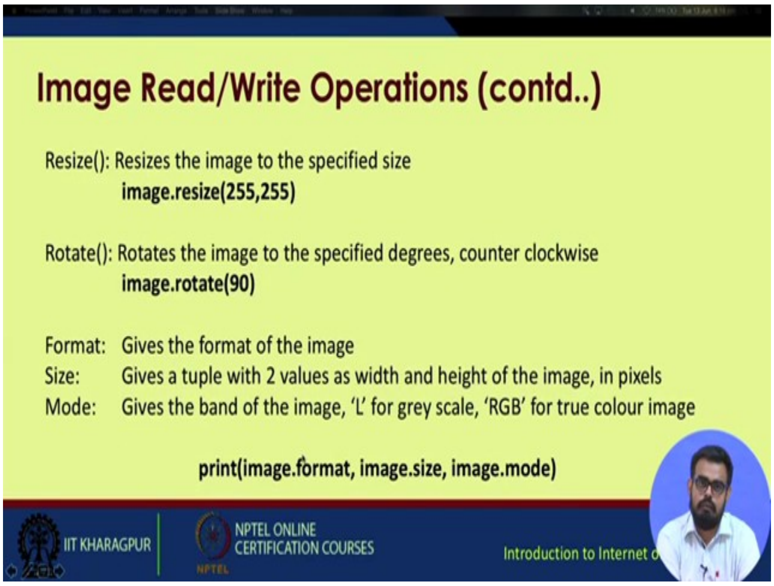
(Refer Slide Time: 18:02)



So, for image read write operations, first of all we have to call this PIL library either we import PIL directly or if we have any particular function in mind like the function image, we just import that particular function.

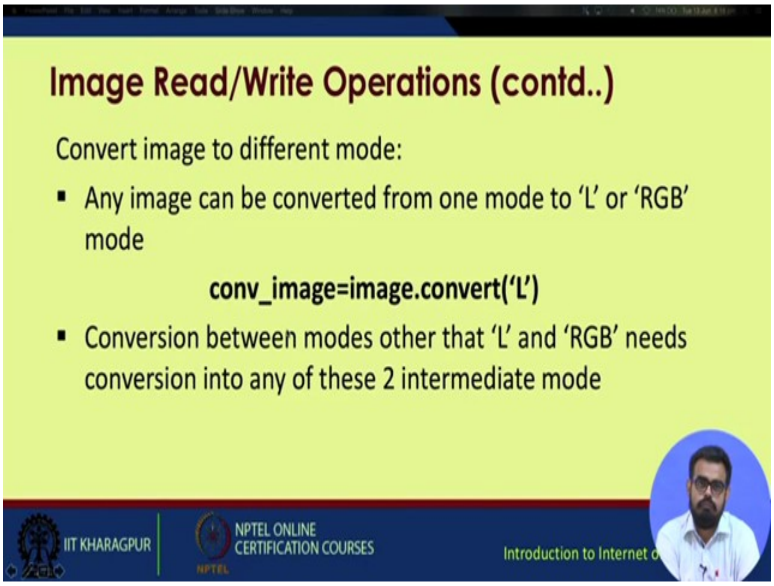
So, for that we have from PIL import image, then opening that image file, image equal to image.open name of the image and for displaying the image, we just write image.show()

(Refer Slide Time: 18:36)



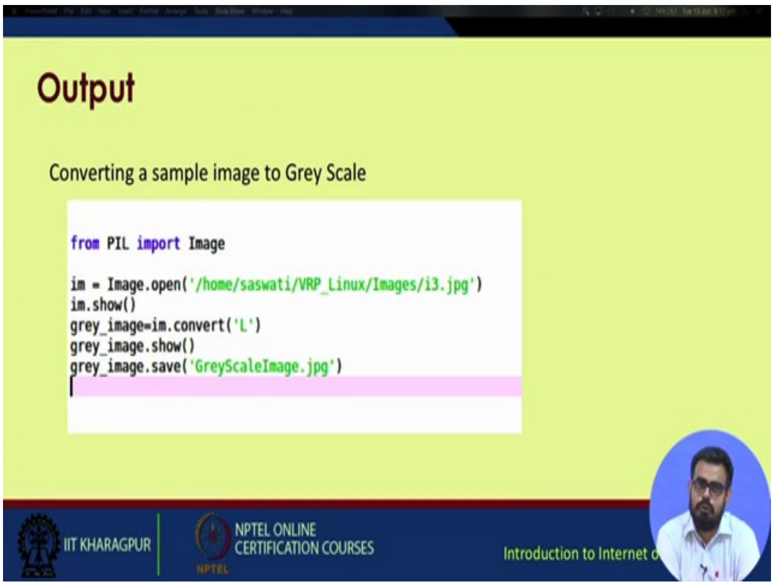
So, you have multiple functions related to images. You want to resize your image, you call the resize function and within arguments you give the number of rows and columns you want to rotate your image.

(Refer Slide Time: 18:59)

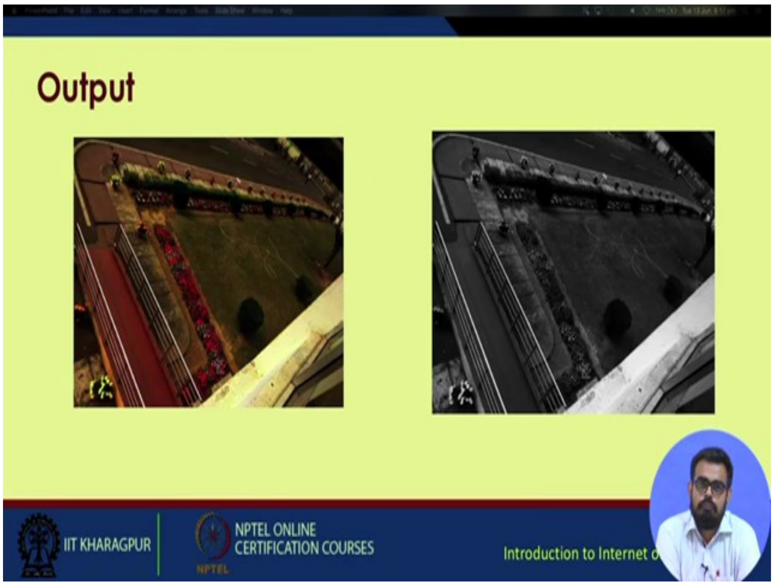


You call rotate and within arguments, the degrees you want to rotate your image, also you can convert between various color maps. So, for example you can convert your normal images acquired from standard cameras. We call them as RGB images because of the presence of three channels red, green and blue. We can convert this into gray scale also. So, the conversion function is pretty simple, image.convert and within the arguments within quotes, you write that mode. "L" stands for pay scale and RGB stands for the normal RGB mode. So, you can alternatively convert between these two.

(Refer Slide Time: 19:40)

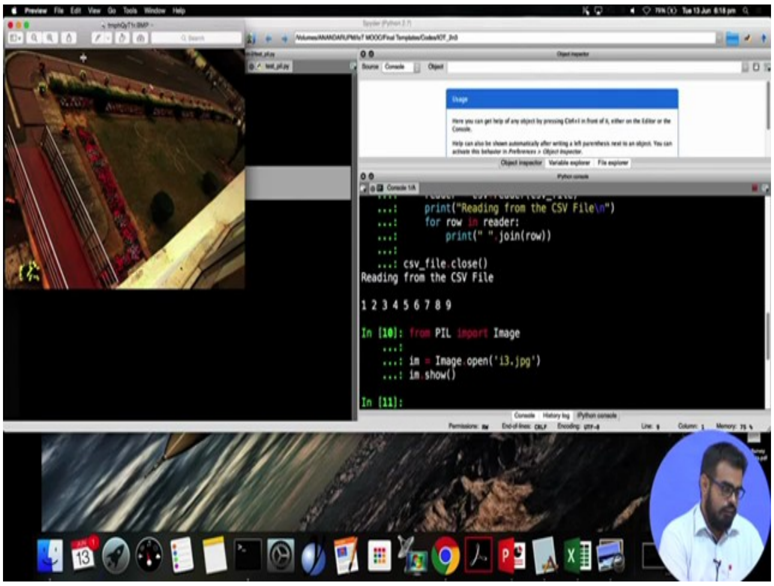


(Refer Slide Time: 19:45)



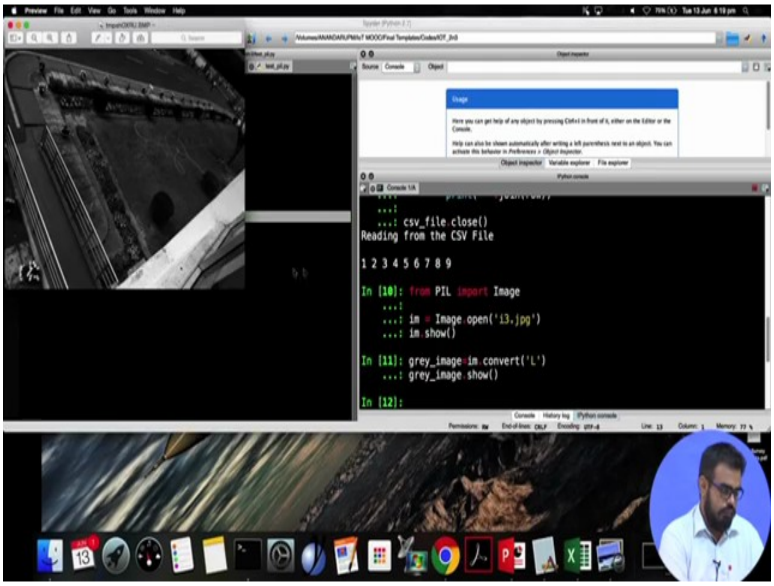
So, this is just for the sake of demonstration. See for example, once we execute, this script will come to that in the hands on part. Once we execute the script, it will give you the following output. The left hand side, this image was taken as the input image and after conversion using image.convert function, it has converted to your grey scale. So, we will check out this function.

(Refer Slide Time: 20:24)



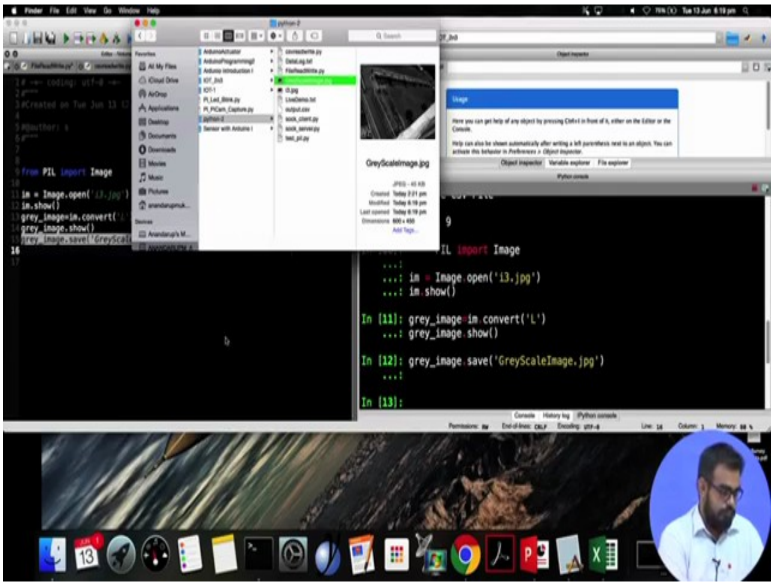
So, now I have from PIL import image and assigning a variable to the function image.open. So, I have a input image, I3.jpeg in my folders, same folder as the script, then I execute this im dot show. I will just execute these three lines you see. Once the im dot show has been executed, the default image viewer application of your system opens up and this was this is the input image null convert it to grey scale.

(Refer Slide Time: 21:31)



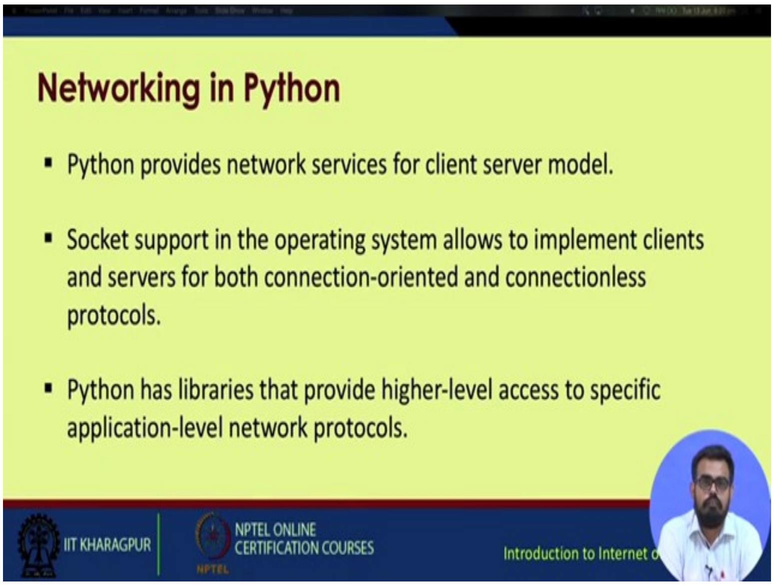
So, im dot convert and within quotes l and again, I will ask the system to show the image. So, as you can see again on the default image doing application, the image has been converted to grey scale from RGB. Now, I need to save this image. So, since the converted color map of the grey scale image is stored in a variable grey_image, I need to save this grey_image.save and the name I want to save it as.

(Refer Slide Time: 22:07)



So, once save function has executed, I get the required file in my directory. These are just some of the very basic functions I can work with.

(Refer Slide Time: 22:29)

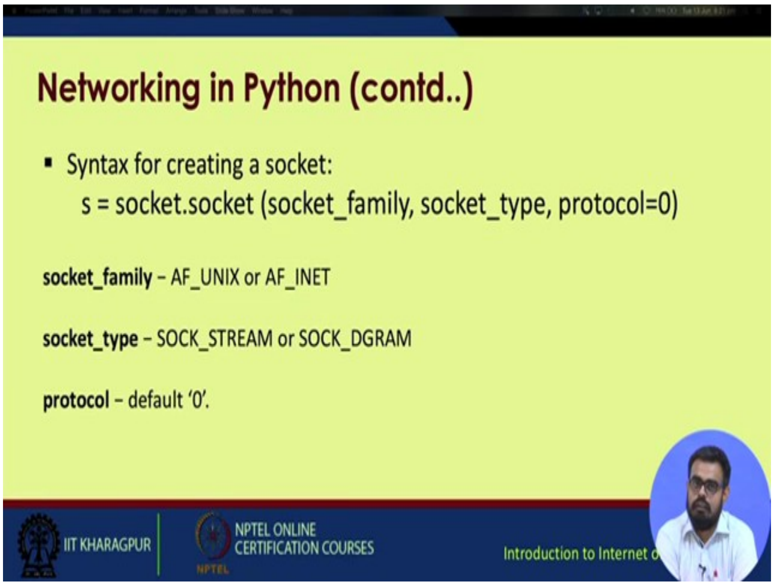


Next we will move on to basic networking in python. So, for this we will create udp sockets. So, we will try to simulate two systems like you will have a client and then, you will have a server. So, server will expect data from the client. Later on you can actually now itself you can actually imagine your client to be deployed IoT devices which read various sensorial data and transmit it over the network to the server. It works in a same principle.

So, for starters we will just see how this networking part happens. So, maybe your server is located far apart, but connected to the network using this same code, same principle. With a bit of modifications, you can get your field deployed IoT devices to send data to a remotely located server. So, python provides this network services using the client server model and then, this socket support in operating system, it allows the clients to implement servers.

It allows the implementation of clients and servers for both TCP IP that is connection oriented as well as UDP protocols which are mainly connectionless protocol and python has additionally libraries which allow higher access to specific application level network protocols.

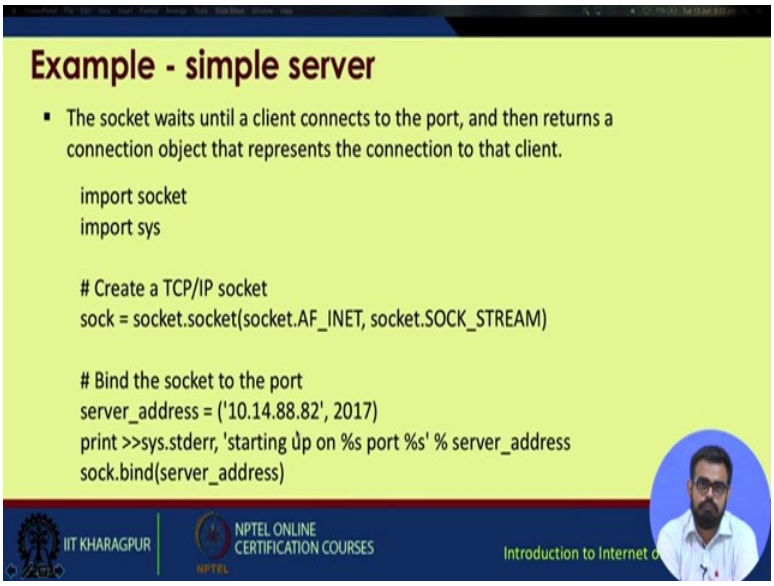
(Refer Slide Time: 23:57)



So, general syntax is locating the socket a variable which is equal to socket dot socket then socket_family, socket_type, protocol. By default the protocol is 0. So, within socket family you have AF_UNIX or AF_INET.

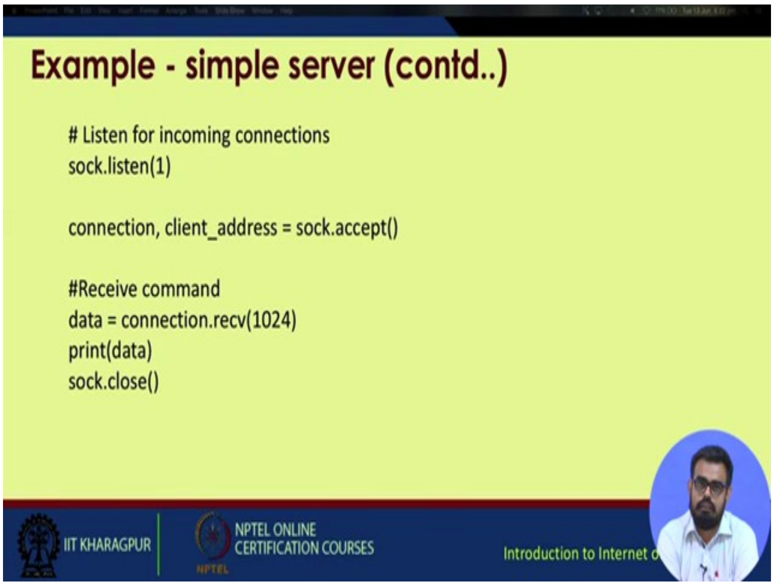
So, generally UNIX option is only available for UNIX base systems, where as INET stand for all internet protocols. Socket type is SOCK_STREAM or sock datagram and protocol by default is 0.

(Refer Slide Time: 24:35)



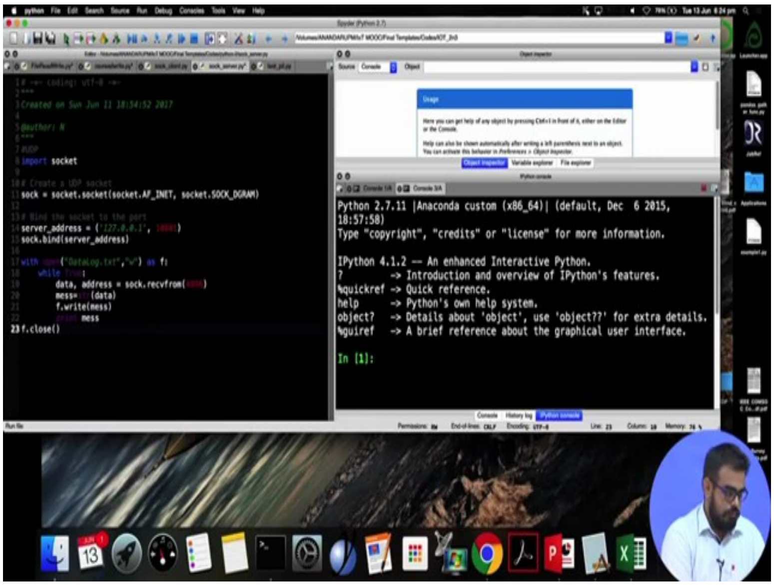
So, we have created a TCP/IP socket, we give the server address as this is a particular IP address, then we give a particular port to which server your client will bind and just some print statements and eventually, the main functions sock dot bind and server address, so that this will be listening for connections and then, we have sock.listen this initializes the listening part that the server is expecting connections from client.

(Refer Slide Time: 25:04)



So, it would be better if I give a demonstration of this thing. So, I will need two consoles for this. From 1, I will run the server and from another, I will run the client.

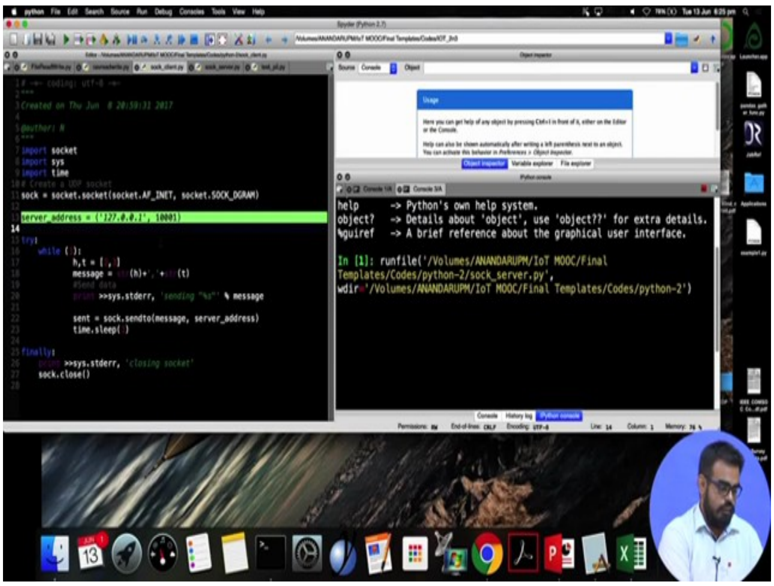
(Refer Slide Time: 25:30)



So, this is my socket server. For the server address, I have given a normal loopback address that is 127.0.0.1

I given a random port 10000 and one and we intend to write the data which is being generated into a text file. So, data log.txt in write mode and this data socket will be expecting the data which it receives from the client in junks of 4096 bytes and whenever this data is received, it will convert the data to string and write the data to the file and eventually once the transaction has finished, it will close the file.

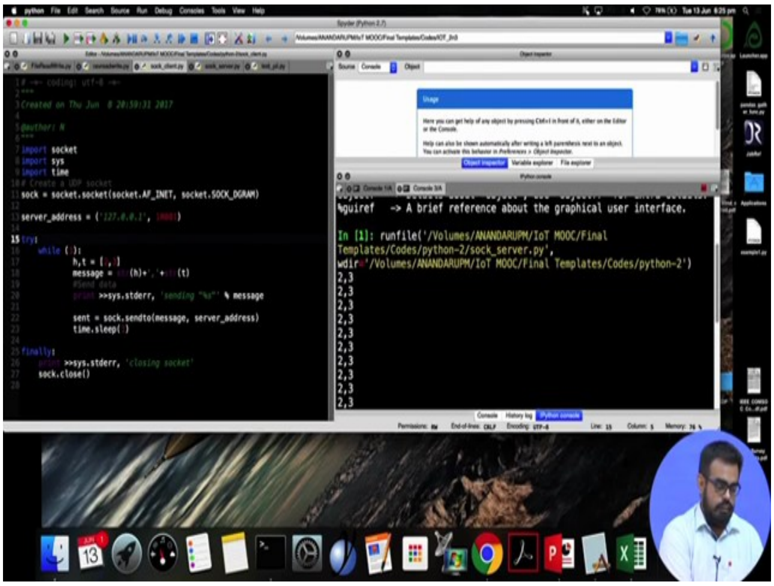
(Refer Slide Time: 26:51)



So, till this part the socket operations take place and within this the data read write operation take place, similarly for start I will get the server running. So, it does not show anything because it is expecting data from a client. On the client side, I give the same loopback address as the server, then the same port number. It is very important to have the same port numbers.

Now, with try and finally we just iteratively loop again and again and send two values h and t. I have fixed it to 2 and 3 and this will keep on sending these values over the socket. You see this sent equal to this sock dot sent to message, the message that is 2, 3 to the server address that was this loopback address.

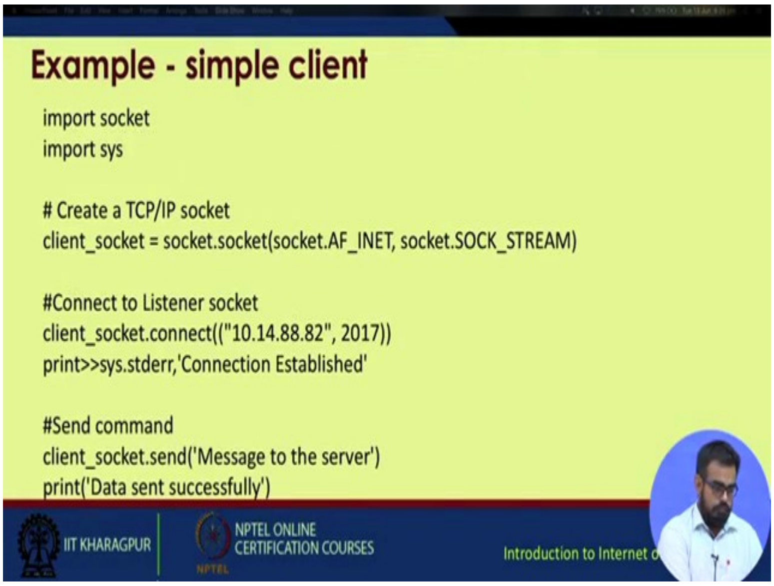
(Refer Slide Time: 27:42)



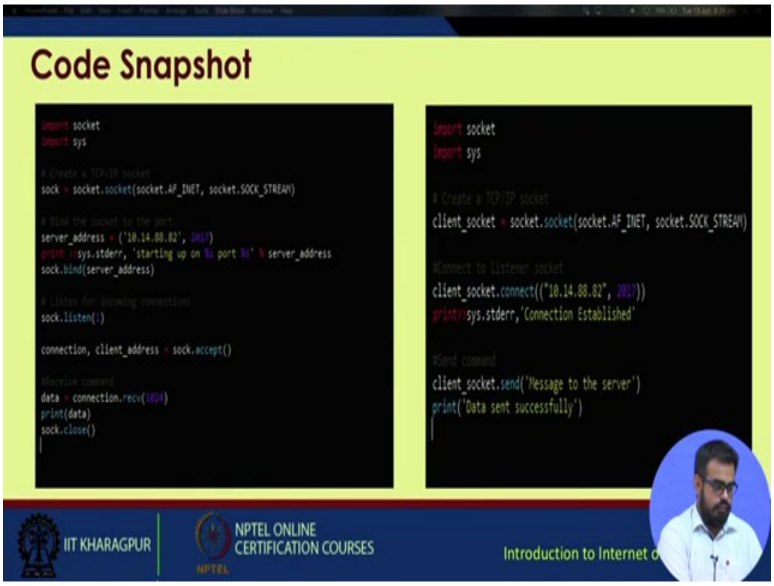
So, in the second console, I will run the client. You see the client is sending 2 3 2 3. It will keep on sending this until I terminate the execution and at the server side, you are receiving this 2 and 3.

So, this thing you can implement on two different machines connected to the network. It may be in the same room, it may be in different cities, it may be in different countries, but your server, your IP and port needs to be the same.

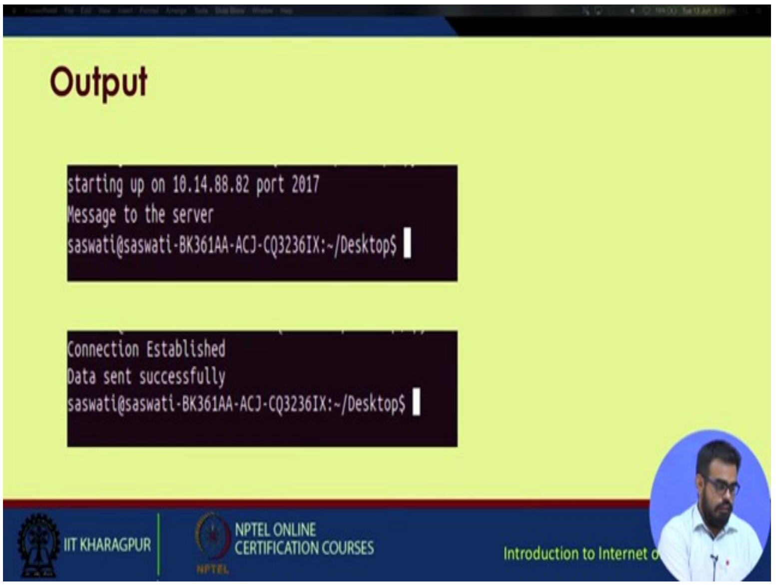
(Refer Slide Time: 28:19)



(Refer Slide Time: 28:22)



(Refer Slide Time: 28:25)



So, we have covered this client. You have seen the code for stand and outputs you have seen. So, I hope you can now use this knowledge to generate some interesting applications on python.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 28
Introduction to Raspberry Pi– 1

In this lecture on the introduction to Raspberry Pi, you will learn about what Raspberry pi is what are the different functions of Raspberry pi and more importantly about why Raspberry pi is so important in the development of IoT.

So, Raspberry pi compared to Arduino is more powerful, it is more powerful in terms of the computation or processing power. Additionally it has better memory capacity and also it can integrate different types of sensors and actuators and this part is more attractive than compared to the similar kind of feature of Arduino. So, we can do different types of sensors integration in Raspberry pi and due to the feature that it can process more compared to Arduino it has better processing capabilities and more features and so on. This is particularly attractive for sensors which have which require more processing for example, imaging sensors multimedia different types of multimedia sensors which require more processing you know this sort of device becomes more useful.

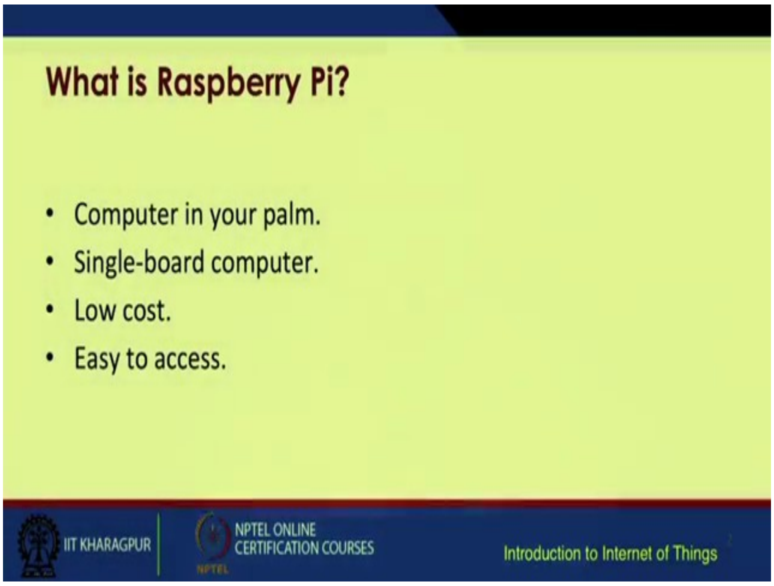
So, in the same way as we can have an Arduino based IOT node here also we can have using Raspberry pi, we can have a Raspberry pi enabled IOT node and this IOT node would be more powerful compared to the Arduino based node. Additionally we have to keep in mind that although it has better capabilities, but it comes at more cost the cost of purchasing Raspberry pi is more than the cost of Arduino in general. So, there is a trade off of course; however, it all depends on the requirements if the requirement of the particular IOT application that is being developed is to have some nodes which you know which should act as a server then Raspberry pi would be a better option than Arduino.

Second thing is that you know with Raspberry pi you can configure Raspberry pi as a web server you can even configure Raspberry pi as an edge device and so on. So, there are different capabilities that are there, but at the same time you know more computation means more power consumption. So, if you have the same kind of you know application with a more power consumption requirements, etcetera, etcetera and if that is not a problem then you know one can go for raspberry pi; however, this particular issue is a little bit you know tricky because there are certain scenarios where Arduino can also come to be beneficial with respect to this.

So, we are going to go through the different aspects of Raspberry pi and try to understand how Raspberry pi can be used. So, I said before you know if you have a Raspberry pi module along with you can practice as we explain to you the different steps the different features and. So, on in this lecture and the subsequent one the next one in both of these we are going to teach you about raspberry pi. So, I have along with me; my TA for this course Mr. Anandroop Mukherjee; like the previous few lectures you know he is going to take you through the hands on aspects of Raspberry pi.

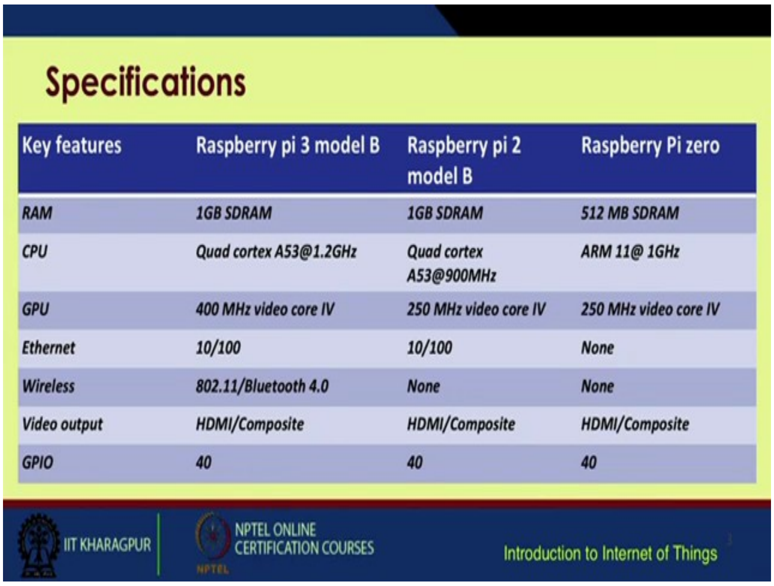
Hello, today this lecture will cover an introduction to Raspberry pi. So, this will be again a 2 part lecture and the part first part will cover the basic introduction to what is Raspberry pi the hardware system and how you go about installing basic operating system on the Raspberry pi and how to access that device. So, what exactly is Raspberry pi?

(Refer Slide Time: 04:36)



It is basically micro sized computer or commonly in common terms it is said as a computer in your palm more specifically it is a single board computer which is very low cost device and which is very easy to access. So, these are one of the main reasons these are some of the main reasons why Raspberry pi has become. So, popular with respect to IOT as well as hobby electronics people.

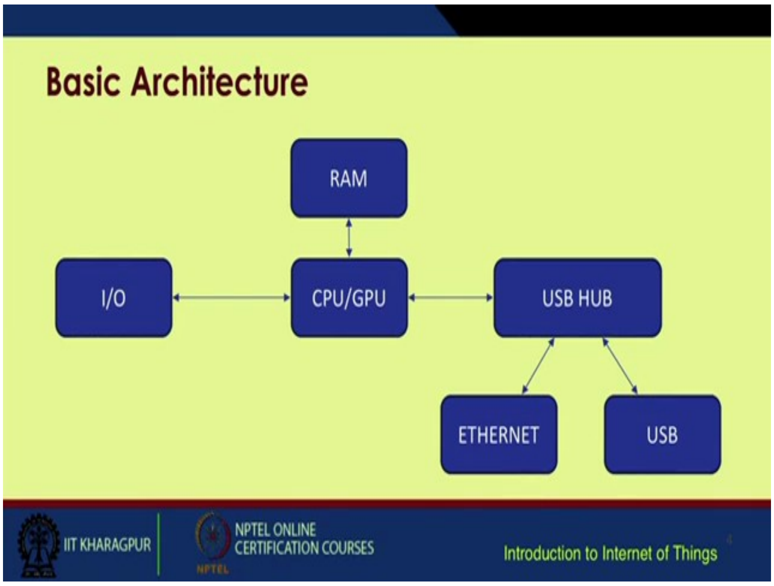
(Refer Slide Time: 05:03)



Key features	Raspberry pi 3 model B	Raspberry pi 2 model B	Raspberry Pi zero
RAM	1GB SDRAM	1GB SDRAM	512 MB SDRAM
CPU	Quad cortex A53@1.2GHz	Quad cortex A53@900MHz	ARM 11@ 1GHz
GPU	400 MHz video core IV	250 MHz video core IV	250 MHz video core IV
Ethernet	10/100	10/100	None
Wireless	802.11/Bluetooth 4.0	None	None
Video output	HDMI/Composite	HDMI/Composite	HDMI/Composite
GPIO	40	40	40

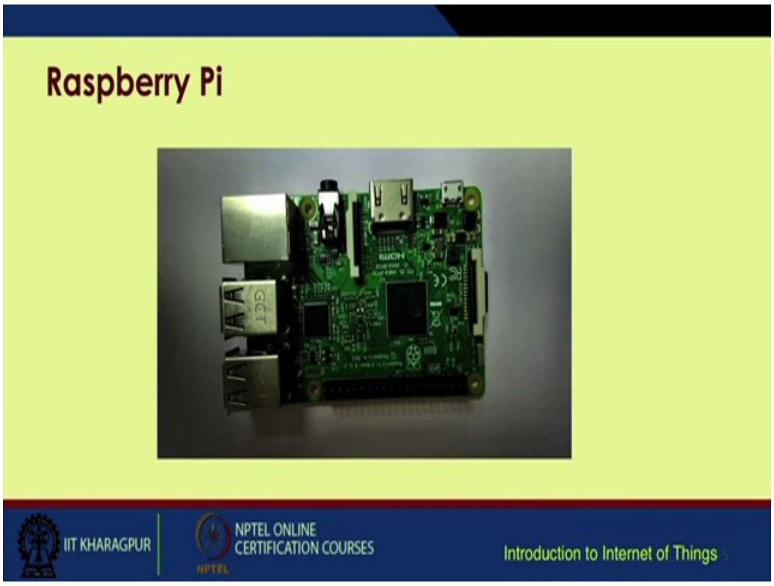
So, there are various variants of raspberry pi. So, some common variants are you have the newest Raspberry pi 3 model b then pi 2 model b pi 0. So, these are the once most commonly being used. So, there are other variants also, but these 3 can be considered as the main market holders. So, as you can see the RAM requirements for pi 3, pi 2 and pi 0 for pi 3 it is 1 GB, pi 2 it is 1 GB whereas, for pi 0 it is bit lesser at 512 MB. The CPU is a quad core cortex a 53 processor processing speed is approximately 1.2 Gigahertz whereas, for pi 2 it is 900 megahertz. GPU requirements you have on pi 3 400 megahertz of video core 250 megahertz video core for pi 2 and 250 megahertz again for pi 0 you have provision for Ethernet on pi 3 and pi 2 whereas, there is no provision for either Ethernet or Wi-Fi on pi 0. Yes, there is a provision for Wi-Fi and Bluetooth only on mod pi 3. Generally video output is from HDMI port and there are 40 GPIO pins. So, these GPIO pins are mainly known as general purpose input output pins.

(Refer Slide Time: 06:39)



So, this is the basic functional architecture of a raspberry pi. So, at the center you have a CPU or GPU you have various input output ports connected to it you have a RAM you have a USB hub from which you can connect an Ethernet as well as you have various USB ports to which you can connect regular USB devices. So, in short this thing is as similar to your normal PC, right.

(Refer Slide Time: 07:11)



So, this is the picture of a raspberry pi. So, I have one Raspberry pi with me right now. So, if you can see this is a Raspberry pi 3 model b.

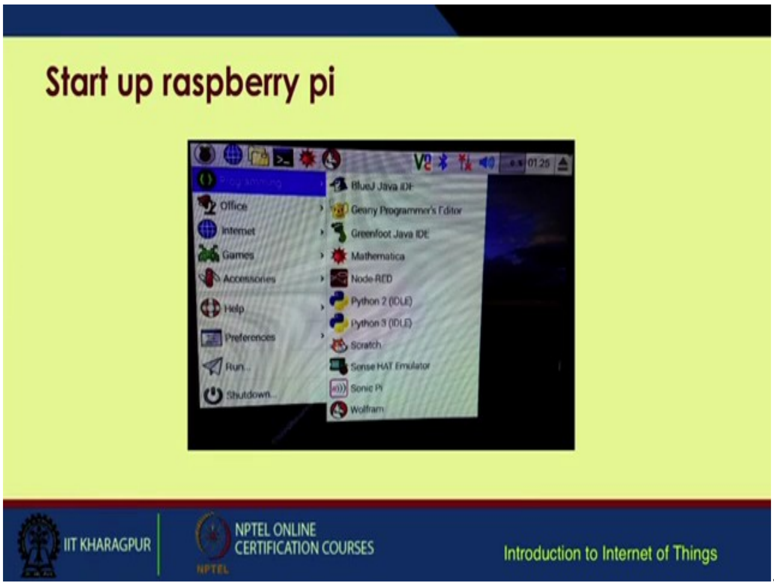
(Refer Slide Time: 07:22)

So, over here you have one HDMI port this small port is for the power adapter these are the GPIO pins interlaced with some power pins like 5 volt 3.3 volt in ground and you have this processors this is the ARM base processor you have four USB ports you have one Ethernet port. So, and you have one sound card output also and turning it over to the other side you can see there is a small memory card attached. So, if you take it out. So, we are using a 32 GB memory card, but generally 8 to 16 GB memory cards are sufficient. So, the main function of this memory card is it actually holds the OS of the raspberry pi.

So, first step towards initializing Raspberry pi is you download the OS available on freely online you load the OS on the memory card and you just plug this thing into your memory card slot on the raspberry pi. So, in goes like this and your system is ready then we need some basic configurations to get this up and running and available on the network.

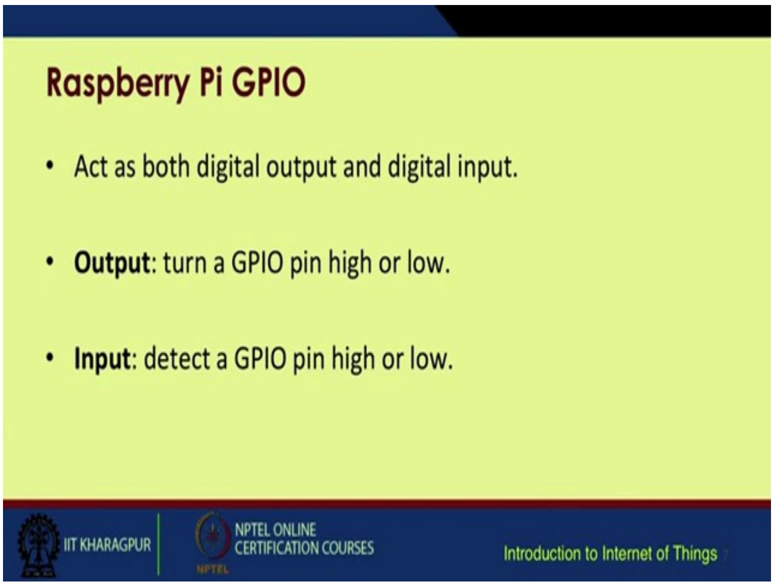
So, once your system is up and running you can see will you may access the Raspberry pi based OS which is primarily a GUI based system.

(Refer Slide Time: 09:05)



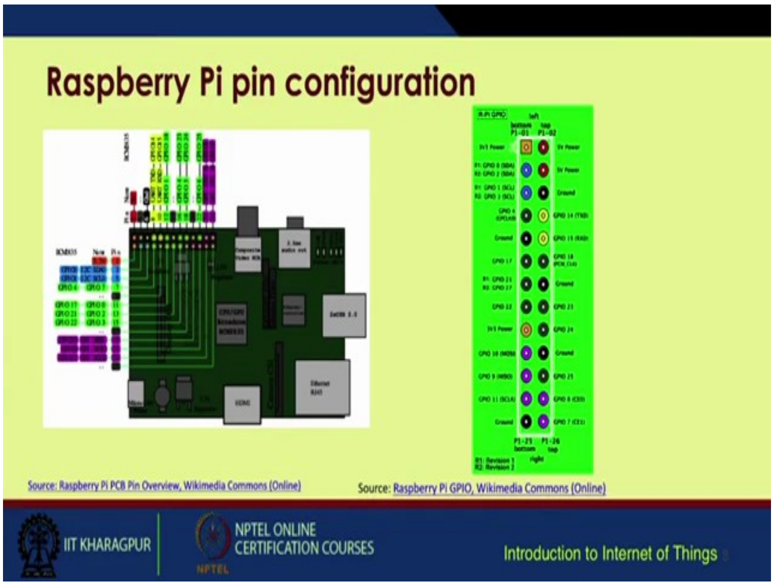
So, it is quite similar to your normal Ubuntu base systems. So, you can see you have various programming languages which are already available within this you do not need to externally install it you see your Python 2, Python 3, Scratch, BlueJ which is a desktop for java and various other options you have some office options also so on. So, basically you get the idea there is one symbol for Bluetooth the symbol for increasing decreasing the sound this one shows the ram usage time and so on. So, it is quite similar to your normal Ubuntu based systems.

(Refer Slide Time: 09:59)



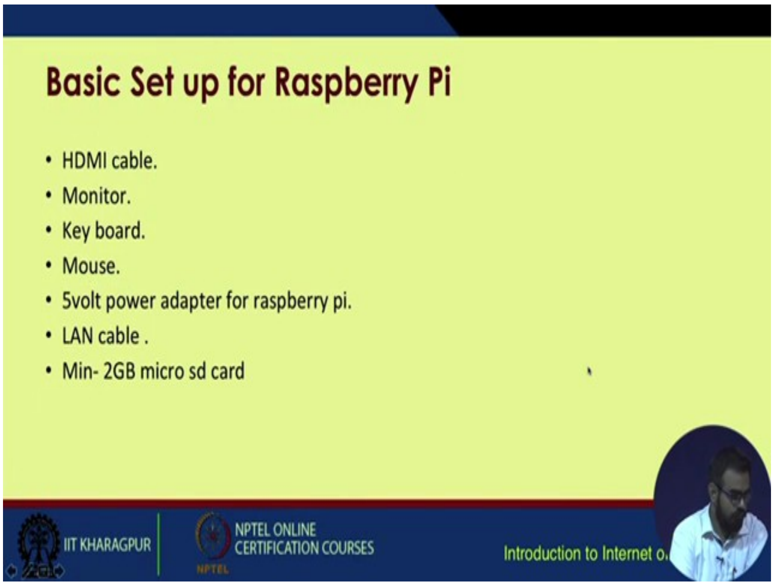
So, these Raspberry pi GPIOs or the general purpose input outputs they can act as both digital output as well as digital input it is quite similar to your input output digital input output pins on the Arduino boards we covered previously. So, if you pay attention to this thing.

(Refer Slide Time: 10:24)



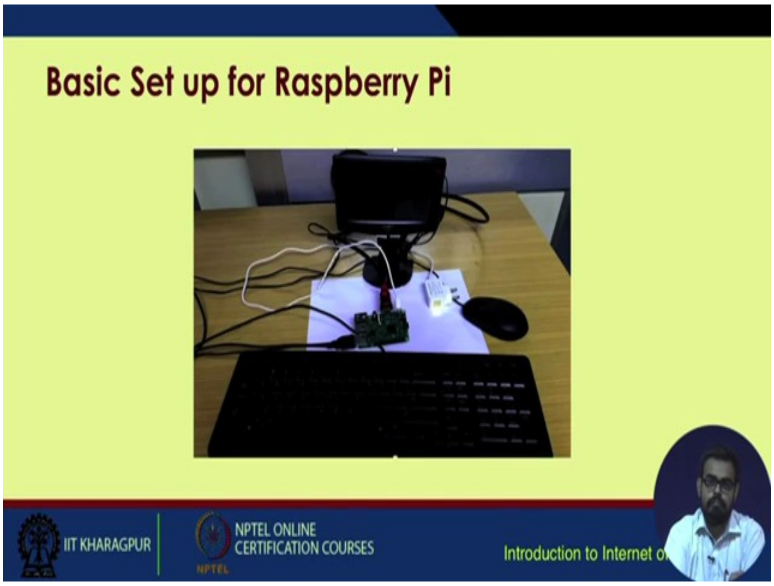
So, these GPIO pins these are a bit confusing. So, I have included one chart descript describing the pin configurations over here these 2 red pins are the five volt power pins the black ones over here are the ground pins and the remaining are GPIO pins. So, you have certain GPIO pins which act as you know your qart txt and rxt; that means, transmission and for reception there are normal GPIO pins and this chart or this configuration is very easily available online.

(Refer Slide Time: 11:14)

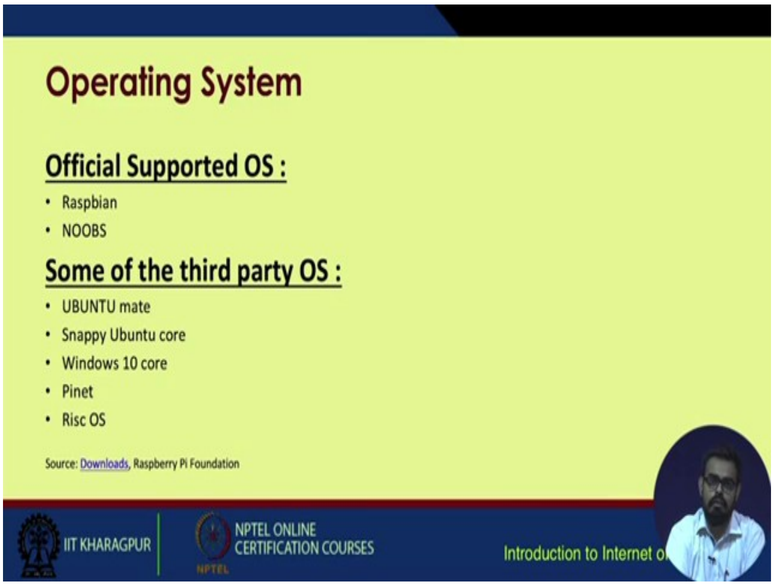


So, the basic setup for this Raspberry pi will require a few components first and foremost when you are setting up the Raspberry pi for the very first time you will require a external monitor you will require an HDMI cable to connect the monitor and the Raspberry pi you will require a keyboard and mouse a basic 5 volt adapter to power up the pi LAN cable and your memory card which will include the operating system on it.

(Refer Slide Time: 11:47)

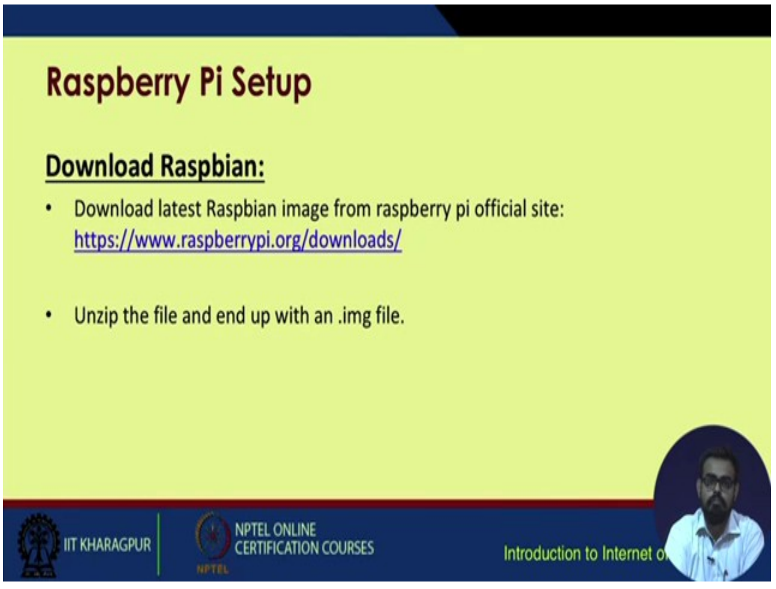


(Refer Slide Time: 11:56)



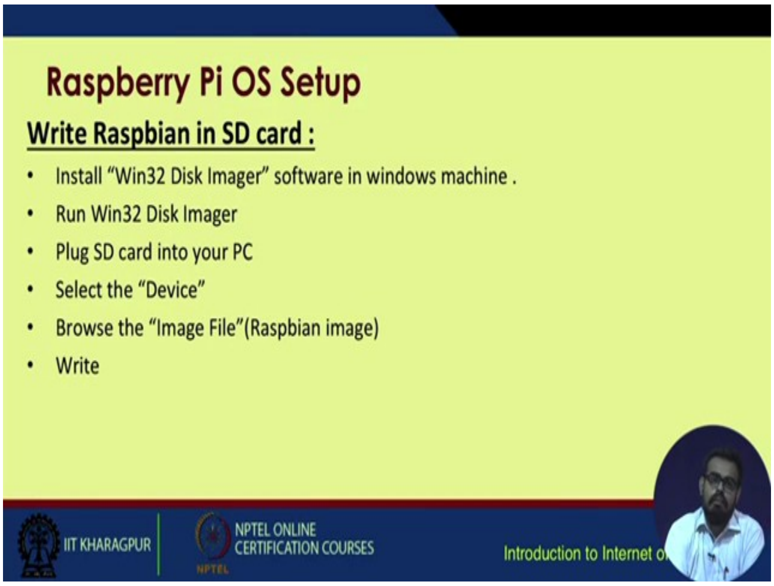
So, we will come to the set up a bit later will I will give a demonstration of how to set up the whole system. So, regarding the operating system certain official bestows for Raspberry pi or Raspbian and Noobs and some third party OSs which can also be installed on the Raspberry pi are this UBUNTU mate, Snappy Ubuntu core, you even have nowadays Windows 10 core for Raspberry pi is finite and so on.

(Refer Slide Time: 12:21)



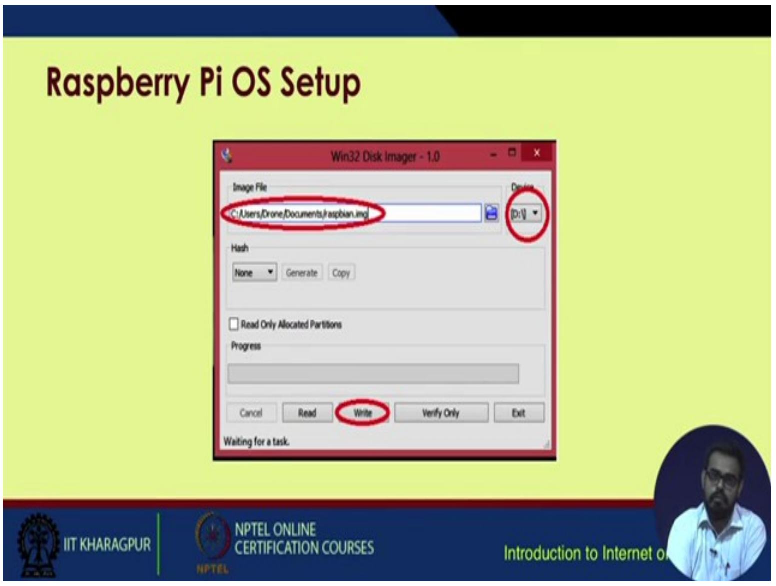
So, you can download your Raspberry pi normal Raspbian image distribution from this link you otherwise you go on to this site you search for Raspbian distribution there are various versions of various releases you select the most appropriate one and that is it. And once the download is finished you will end up with a zip file you unzip it you will get a image file and you just write that image onto the memory card.

(Refer Slide Time: 12:54)



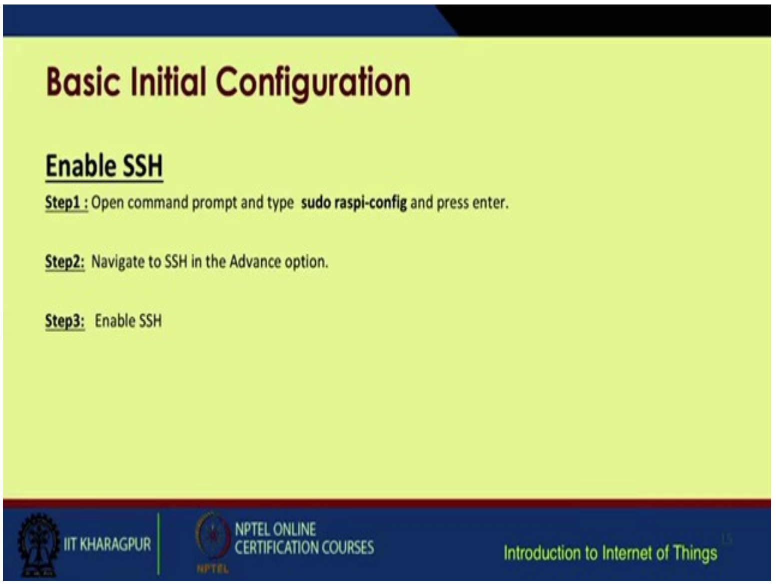
So, for windows based systems since most of the people use a windows based system; the installation for this image is quite easy you require a software called Win32 Disk Imager. It is freely available online you run this disc imager software plug in the SD card into your PC you will need an USB adapter for the a SD card you select the device browse for the image file which contains that Raspbian image and you just select write. So, it will take around anything between 15 minutes to half an hour. So, once your writing is finished your memory card is ready to be integrated with the Raspberry pi.

(Refer Slide Time: 13:39)



So, you can see you just select the distribution or the image the location of the image on your PC on the right hand side you can see you select the device onto which you want to write and after both of these have been done you just click on the right button that is it.

(Refer Slide Time: 14:00)



So, now, before coming to this step let me give you a demo of how to start off with the basic Raspberry pi installation.

(Refer Slide Time: 14:15)

So, over here first of all I have a keyboard and mouse I will just connect them to the USB ports choose any USB port I have a LAN cable ready I am connecting it to the Ethernet port this is an a small monitor portable monitor. So, it is being powered by a external power supply and it is connected it will be connected to the Raspberry pi via this HDMI cable on this HDMI port. So, once all of these have been done you just plug in your power supply for the Raspberry pi you already check whether you already have the memory card in place. So, it is there you just plug it in.

So, now if you pay attention on the screen you are booting starts. So, once the boot is finished you get a GUI based interface. So, just like the screen shot in the previous light. So, you have got one terminal you have got a start menu option you can access various programming languages. You can access internet options have got options for mail you have got options for other things you can also set up a VNC server or VNC viewer on raspberry pi so that you can remotely access the user interface on the network.

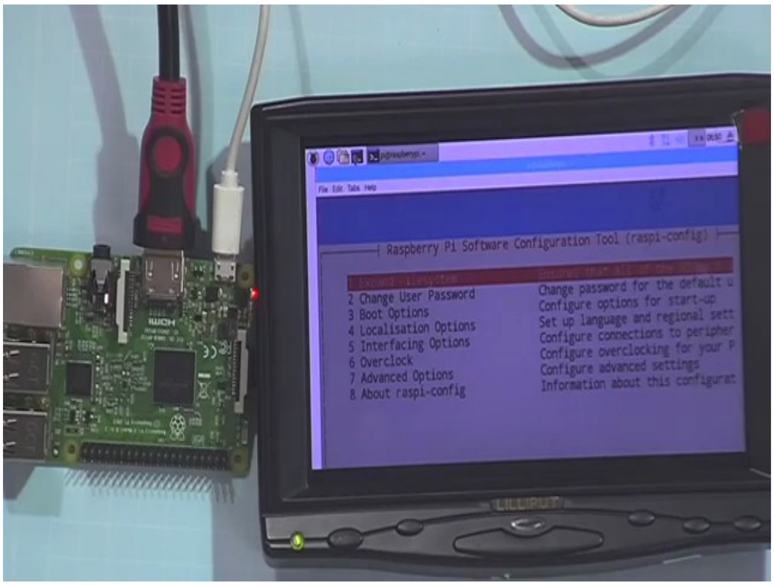
So, once the Ethernet cable has been plugged see this Ethernet has been plugged. So, it is showing one IP. So, this IP will be required to remotely access your PC Raspberry pi from your PC. So, best practice is you go to terminal right.

(Refer Slide Time: 16:38)

One more thing; the default name for the Raspberry pi distribution is pi p I and the password is Raspberry; r a s p b e r r y. So, whenever you are remotely logging into the system you give the; I username as pi and the password as raspberry. So, first of all I will check for the IP of the system. So, I give the command IP config. So, you see various interfaces have been located. So, I am more interested in the first part. So, this is going to be my required IP. So, now, I will store this IP and I can remotely login to the system using this IP. So, now, my Raspberry pi is ready to be accessed remotely. So, now, I do not need to use the monitor anymore. So, the main function of the monitor is to initially get the IP address for your system and for basic configurations.

So, coming back to the presentation; so, initial configuration we have done now enabling this SSH option SSH as you know is stands for secure shell login. So, just check on your Raspberry pi; go to the go again to the terminal you give the command pseudo raspi-config and press enter. So, you will get something like this, right.

(Refer Slide Time: 18:19)



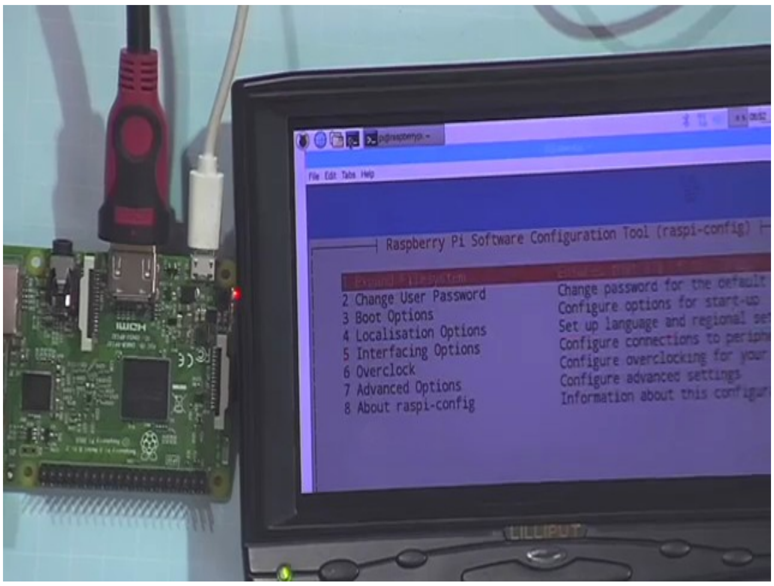
Since I am already using this Raspberry pi for quite some time this is not a fresh install. So, all the operations have already been performed, but post first time installation of your Raspberry pi you need to expand your file system because these images are more or less compressed and if you expand the file system it will cover your entire memory card. So, your entire memory card; suppose I am using a 32 GB memory card, but the image was 2 GB approximately. So, it will now expand to cover the maximum of the memory card.

So, you will have lots of space for additional functions installing new softwares putting on files etcetera. So, once you expand the file system after this operation is done you reboot the system. So, I will go to advanced options.

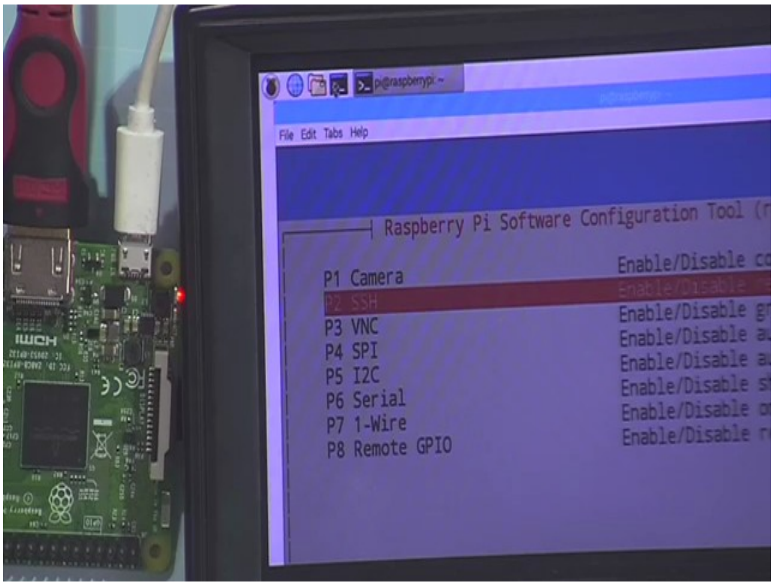
(Refer Slide Time: 19:45)

Sorry, I will go to advanced options as you can see there are various options for overscan resolution, audio driver and so on and there should be one option for ok I will go to interfacing options for this distribution you have your enable SSH in the interface options under Raspberry config.

(Refer Slide Time: 20:23)

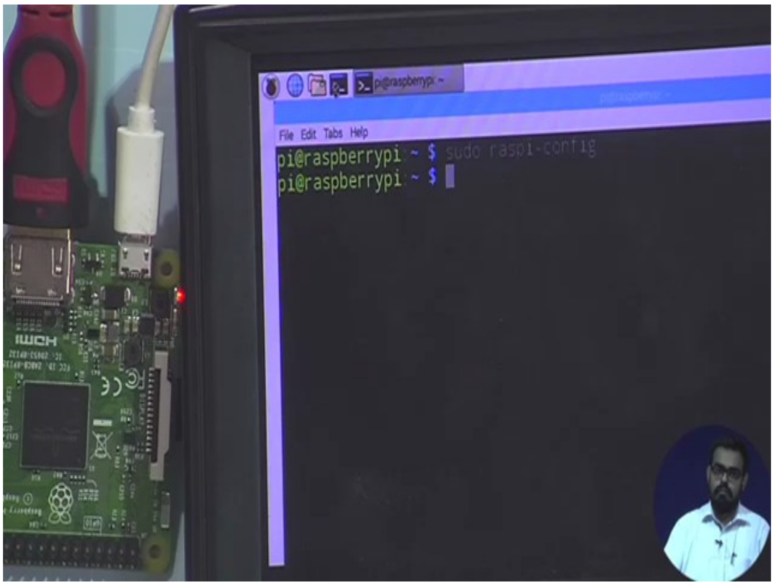


(Refer Slide Time: 20:27)

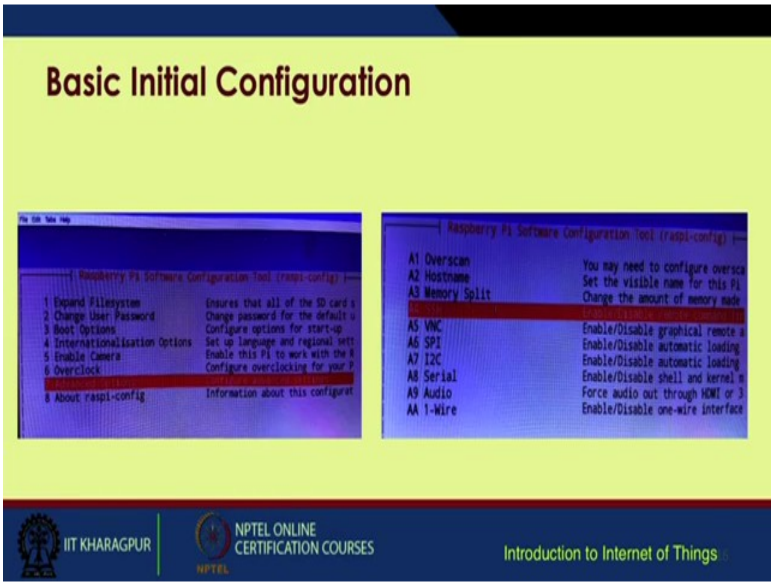


So, you select SSH and press enter and once your SSH is enabled you reboot your system. So, this will allow you to access your Raspberry pi over the network from any remote PC from windows based systems you can use software such as putty or any SSH client from Ubuntu based systems or MAC based systems you can only use the terminal to perform this SSH operation. So, my SSH is already enabled you can also enable your additional options like if you have a Raspberry pi camera there are these are special cameras which can be integrated to as Raspberry pi. You can obviously, integrate USB cameras to wireless USB ports and there are as you can see there are various other options if you need to use the VNC server you enable this VNC option and so on.

(Refer Slide Time: 21:39)

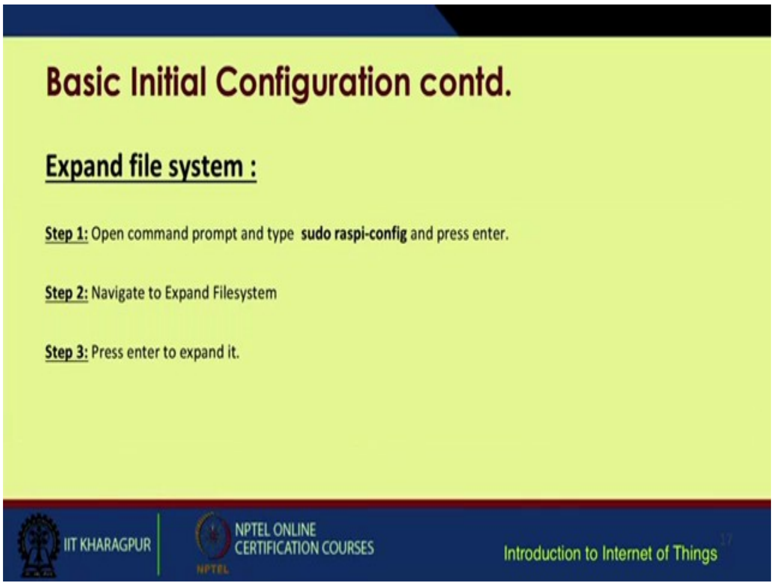


(Refer Slide Time: 21:45)

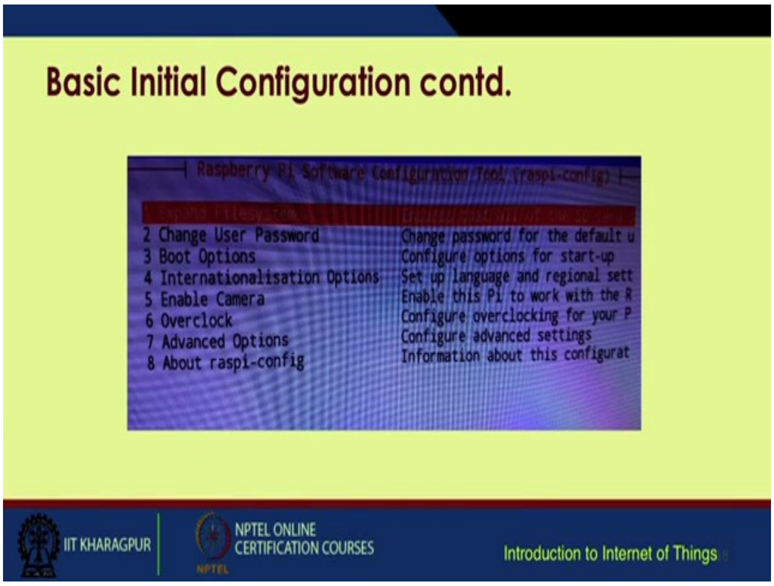


So, I hope you get the idea. So, I will escape this thing now coming back to the presentation once the SSH has been enabled. So, we have covered this thing.

(Refer Slide Time: 21:51)

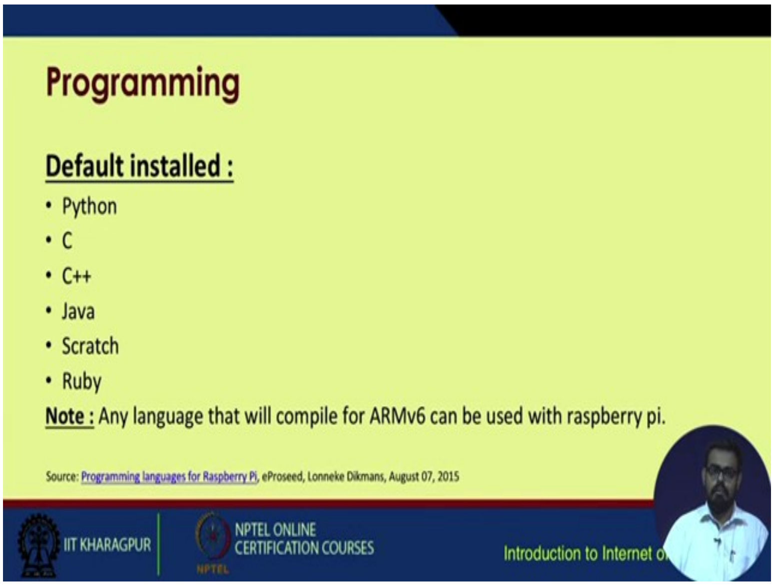


(Refer Slide Time: 21:57)



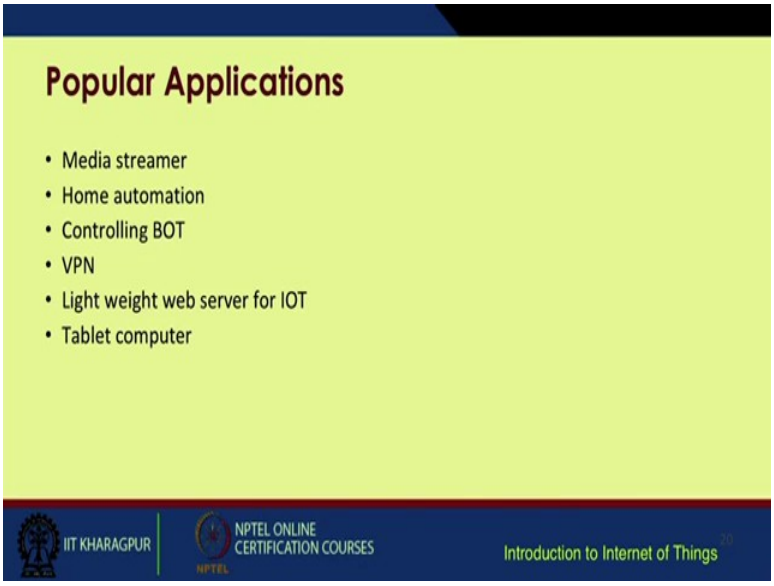
Then file system expansion we have explained. So, as you remember from the live demo this option was there the first option expand file system.

(Refer Slide Time: 22:06)



So, post this as I have already told you the basic default programming languages which are installed are Python, Java, C, C++, Scratch and Ruby. So, more or less any language that will compile for arm version six can be used easily with Raspberry pi.

(Refer Slide Time: 22:29)



So, some basic and very popular applications you will come across on the internet for Raspberry pi based systems mostly they are media streamers home automation systems controlling a BOT, virtual private networks, a lightweight web server for IOT. So, like instead of having a dedicated big server for running IOT based applications suppose you want to install a small IOT network in your home maybe for home automation or home monitoring you can; obviously, go for a Raspberry pi base system. So, this system will act as a server whereas, your devices will start uploading data to the server you can even run various analytics on the Raspberry pi based server and then you; obviously, have a tablet computer based system. So, this Raspberry pi is already a computer just interface a monitor and some external peripheral devices any other and you are ready to go.

(Refer Slide Time: 23:38)

So, coming back once again to the system; so, I do not require this anymore I just close it now I will do one thing let me access this pi base system from my PC I already have the IP. So, here it is so I will write for my since my PC is running a MAC based system I will write the command ssh -y then space pi at the rate the IP address for your raspberry pi. So, once I press enter it will start it will ask for the address as I have told you; the default sorry it will ask for the password the default password is raspberry once you enter the password you are ready to go first it will give some basic information about the system and then you will see a prompt which will say pi at the rate Raspberry pi.

So; that means, you are ready to go. So, you can just see your file system what exactly are there you can give a basic ls command or list file. So, these are some of the directories or files put in your Raspberry pi you can even remotely start restart your PC or raspberry pi. So, for the end of this lecture I will just reboot my raspberry pi. So, I write pseudo reboot, press enter ok. So, as you can see over the monitor my Raspberry pi has gone into reboot again it is starting up. So, this was the end of our part one lecture.

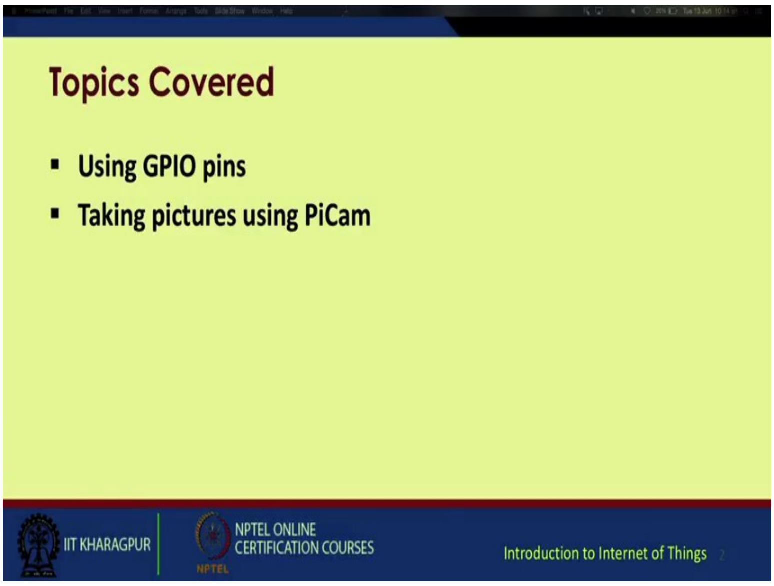
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 29
Introduction to Raspberry Pi- II

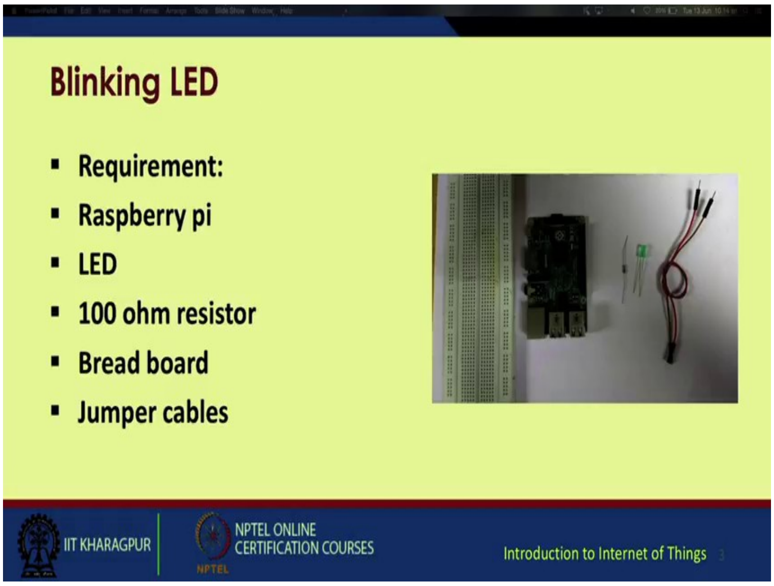
In this lecture, we will cover the bit more detailed introduction to raspberry pi, so that you will get a concise idea about how you can go about integrating various sensors and devices with a raspberry pi base system, and maybe programmatically access and manipulate them.

(Refer Slide Time: 00:41)



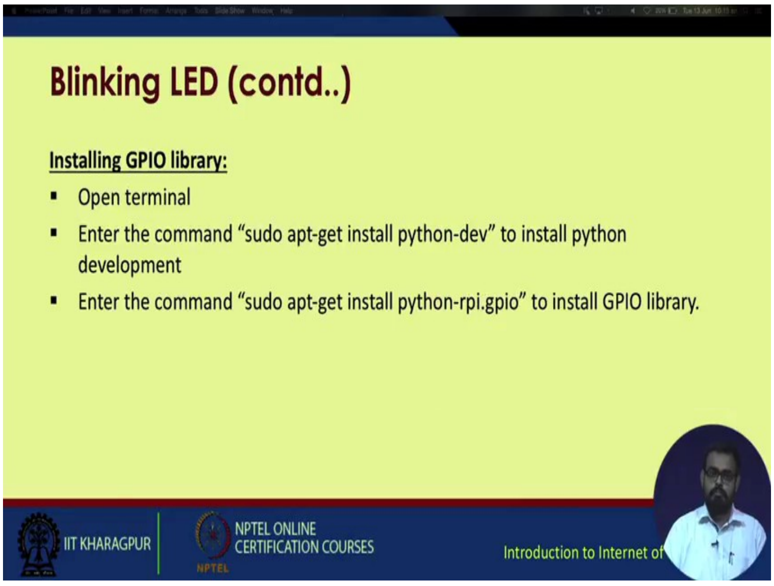
So, first of all we are going to cover how to use that basic GPIO pins and then you are going to cover how to integrate a pi camera with the raspberry pi for taking images.

(Refer Slide Time: 00:56)



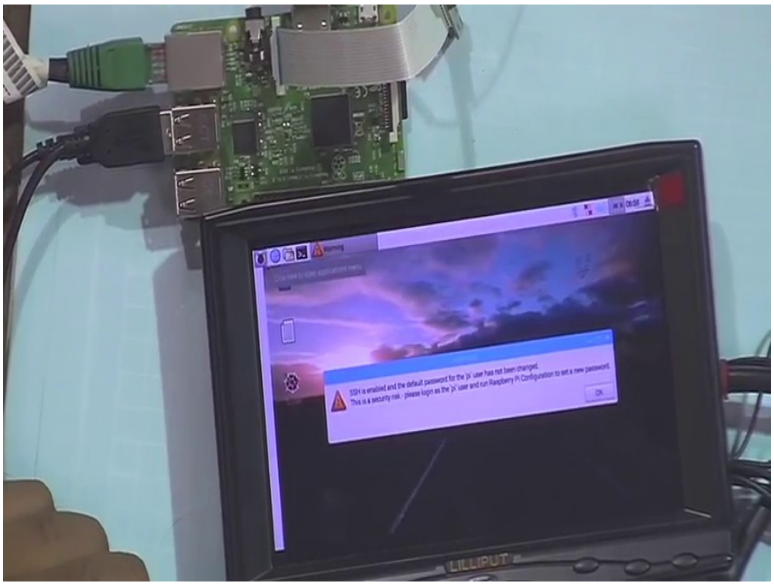
Point to note is we will be covering both of these things on python. So, the programming language will be python. So, since it is quite easy and easy to integrate with raspberry pi also, we will be preferring python So, first thing we are going to go about doing is a blinking LED based project. So, basic requirements are you are going to require a raspberry pi connected to the network, you are going to require an LED, a basic 100 ohm register breadboard and a few jumper cables.

(Refer Slide Time: 01:37)



So, before we go into this any further let us come back to the raspberry pi as we remember from the last lecture. As you can see I have not yet powered on this device yet, but I have attached a pi camera. So, this module is known as a pi camera and it goes over this side. So, you will see this is called a ribbon wire. So, it is already available with the pi cam and the blue sided should be pointed towards the Ethernet port, this is one point to remember. You take this white jack out plug this ribbon and push the white jack in and that is your that will attach your pi camera to your raspberry pi.

(Refer Slide Time: 01:45)



So, now we are going to power up this system. Now, since my device is booted up. I will check whether we have network access or not. Now, we have got a functional Ethernet configuration ready for operation. We have got the same IP as the previous example. Now, in the last example, in the last lecture, I showed you how to connect your raspberry pi over SSH from any PC. So, using SSH you can mainly execute and run various programs suppose you want to transfer some file this would not be this operation you would not be able to do using SSH. You can, but it is quite tiresome. So, the easier way out is using a ftp client. So, one I prefer is Filezilla it is available freely online.

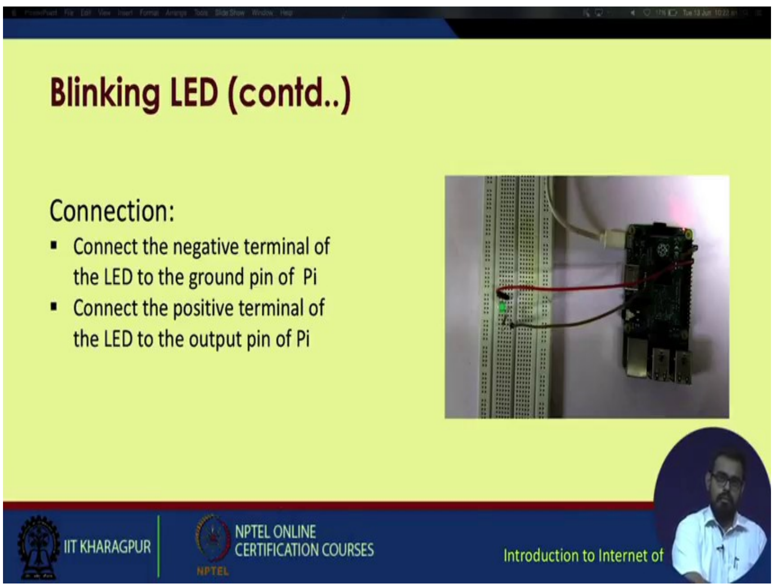
So, once I open the Filezilla, the left hand panel generally shows my local PC contents and the right hand side will be my remote PC contents. So, I am connecting to the host the IP address was I put in the IP user name was pi password was raspberry, and under ports it give 22. So, this is fixed for ftp, to give port 22 and then quick connect. So, it will ask you will get a security confirmation message, you click ok. Now, you are connect to the raspberry pi. You can just drag drop between the two file systems.

Suppose, you want to copy this folder I created this folder name IoT lets see what is inside it has three files two python files and one image file. So, just as an example I will transfer this to my desktop or better still I will transfer one file from a desktop to raspberry pi. Suppose I have got this one example1.py on my local machine and I want to transfer this to my raspberry pi. I just drag drop between the two interfaces, see file transfer was done, and now this example1.py is on my raspberry pi base system.

So, if you check again on the raspberry pi screen, now there is a folder name iot you click on it and there you have this example1.py on your raspberry pi base system. So, it is quite easy many a times programming bigger things on raspberry pi is quite cumbersome. So, I my preference is I basically program everything on my local PC and then transfer the eventual files into the raspberry pi and just do some minor configurations and changes.

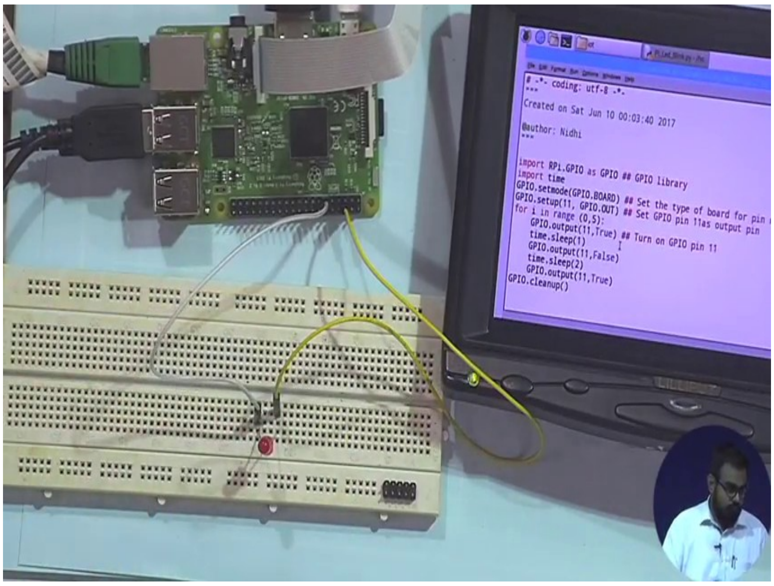
So, now coming back to the raspberry pi. So, for the blinking LED project since you are going to connected to the GPIO terminal, you will require two things first is the python-dev library and the other is the python-rpi.gpio library. So, you can easily access these two libraries over the net. So, once your pi is configured and ready to go on the terminal, you just type the commands sudo apt-get install python-dev. Once this operation is over, you type the commands sudo apt get install python-rpi.gpio.

(Refer Slide Time: 08:09)



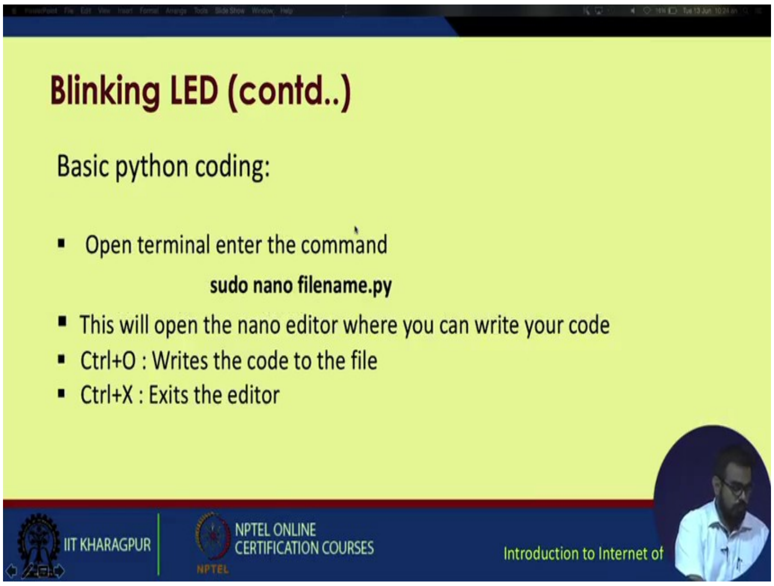
So, once these two files are installed on your raspberry pi base system, you are ready to go. So, for initial connection, I am taking an LED, I will check for the positive and negative terminals the larger one is the positive terminal and the smaller one is the negative one.

(Refer Slide Time: 08:36)



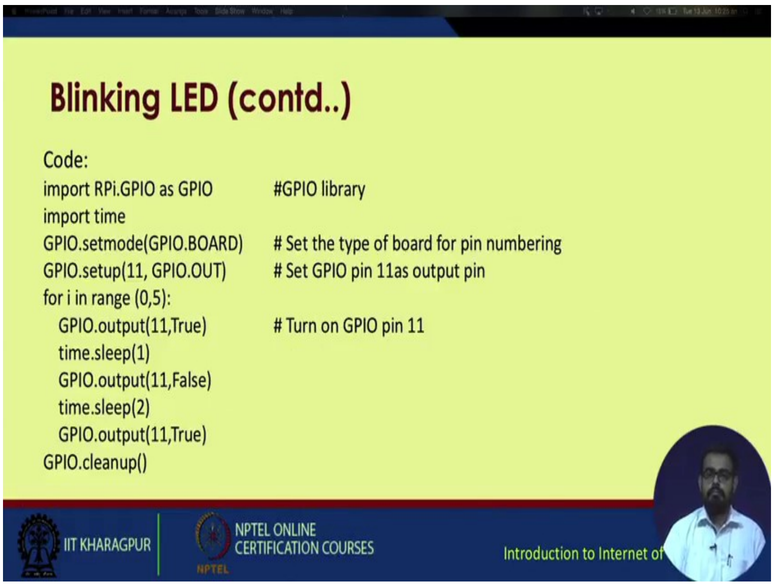
So, the white wire is connected to the positive terminal, the yellow wire is connected to the negative terminal. So, this negative terminal I will put to ground and the positive terminal for this I will have to check which port I have assigned. So, I have assigned port 11 GPIO pin 11. So, it is not quite straight forward as arduino boards for this you need to have that a reference table shown in the previous lecture, so that will give you a good reference for which pin is which GPIO pin. So, for GPIO pin 11, so actually 1, 2, 3, 4, 5, the 5th pin on the inner side no sorry is the 6th pin. So, now I have connected this. So, my connections are ready.

(Refer Slide Time: 10:07)



On the terminal I can; obviously, write my code on the terminal. So, best practice is there is in built editor on the raspberry pi in nano. So, you write sudo nano and then filename.py. So, if I want to name my file as LED blink I write LED blink.py. So, this will open a new terminal on your system on which you can write your code, python code since your file name is in the extension of your file name is dot py you have to write your code in python. And once your code is ready you press control plus O this will write the code to the file and you exit the nano editor by control pressing control plus X.

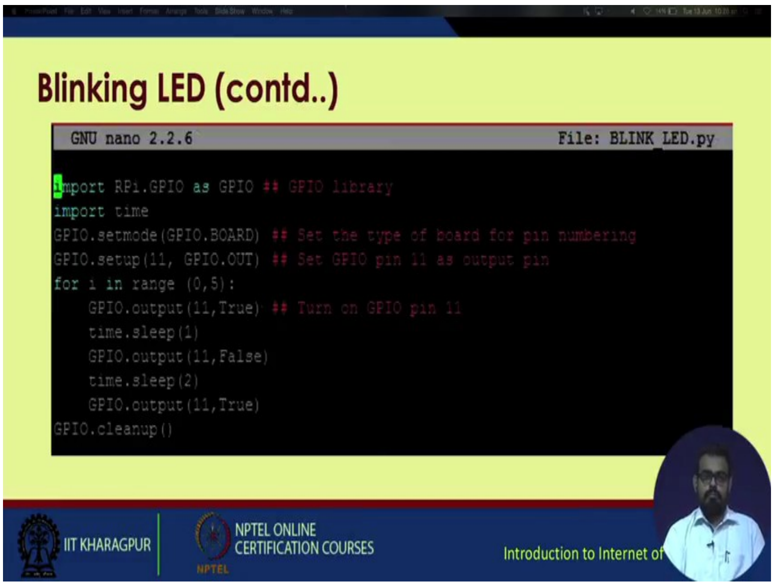
(Refer Slide Time: 11:00)



So, this is the code. So, first line is import RPi.GPIO as GPIO. So, this actually calls the GPIO library second one is import time, since you will be using a delay function on python this delay function is denoted by sleep. So, we use a time.sleep third line is GPIO.setmode. So, you put GPIO.BOARD. So, there are two options you can use it as a board mode and there is another option which we are not going to use now. So, you are going to strict to this board option in GPIO pin 11 is setup as the output pin. Then the main looping part just a simple loop for i in range 0 to 5 that means, it will iterate between 0, 1, 2, 3 and 4, 5 is because it is excluded we covered at this in the python programming part.

Now, GPIO.output pin 11 is true that means it will send a high bit to the output pin, it will sleep for 1 second and again it will send a low bit to the output pin. So, the physical output will be your once the high bit is reached, your LED will glow then it will wait for one second then once the lower bit is reached it will turn off. And again it will sleep for 2 seconds and then turn off. At the end you do this cleanup operation to release the GPIO pin.

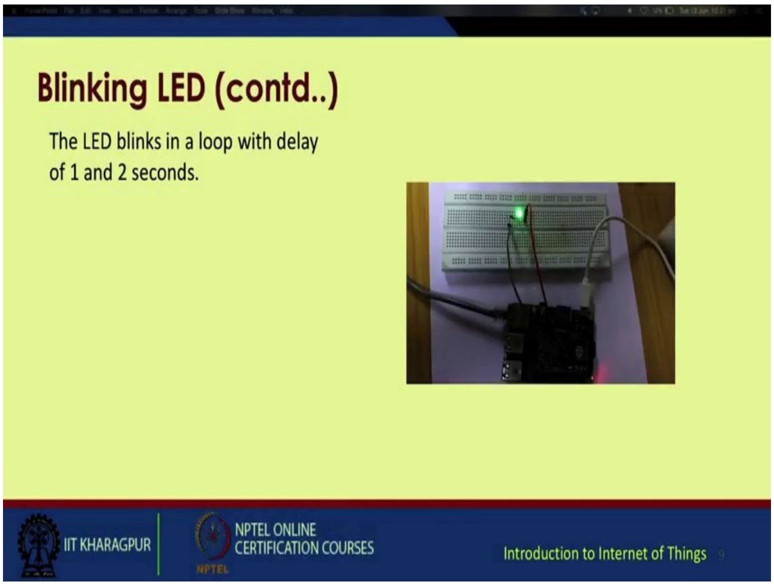
(Refer Slide Time: 12:51)



So, you have already seen on the console this operation. So, these are the codes. So, one more thing since the inbuilt python installation on raspberry pi OS are very rudimentary you would not be able to access advanced options without installing advance libraries. So, the very basic python idle interface and editor you will be able to access on raspberry pi. So, once you double click on this file this is my file of interest pi LED blink dot py, it opens up this code right. So, let us suppose you do not have a visual display anymore let us try accessing this thing over the terminal.

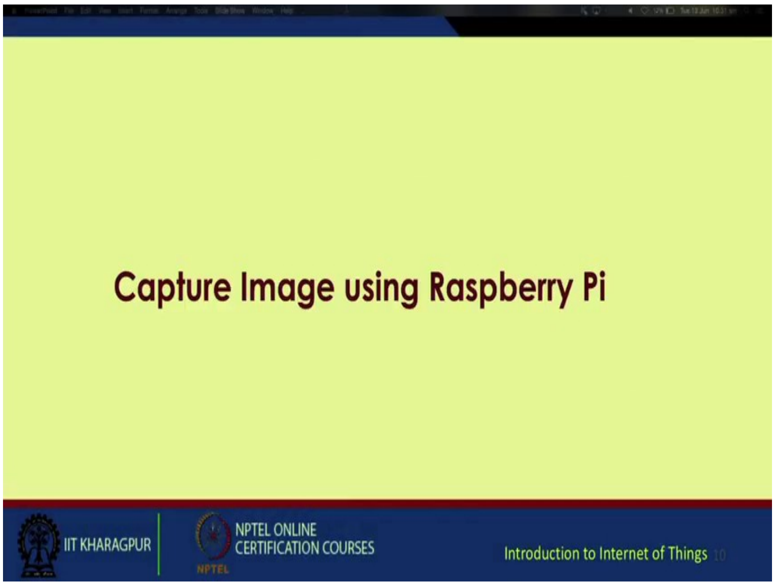
So, you login into my raspberry pi, I go to the directory IoT I am inside the directory I will check what are the files and folders inside the directory by writing ls it will list all the files and folders inside this iot directory. So, my code of interest is pi LED blink dot py. So, first let us see what is exactly inside this file I write sudo nano pi LED blink dot py. So, it opens up the editor this is the same code we showed on the slides it has already been saved. We exit this. Now, when I want to run this code I write python Pi Led_blink.py this was my Led blinking program you press enter as you can see the LED has started blinking so and it will keep on blinking. So, again run this program, I run this module, you can see LED blinks, program is executing. Now, once you get this triple arrow symbol for the console that means your program execution has finished. So, this was the basic integration and usage of GPIO pins on the raspberry pi.

(Refer Slide Time: 17:00)



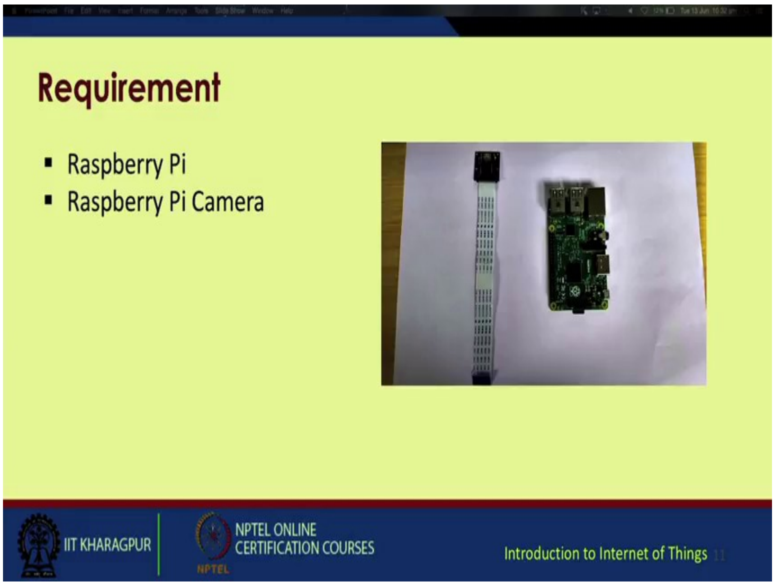
The next interesting topic you are going to cover is integration of the camera or the raspberry pi camera.

(Refer Slide Time: 17:03)



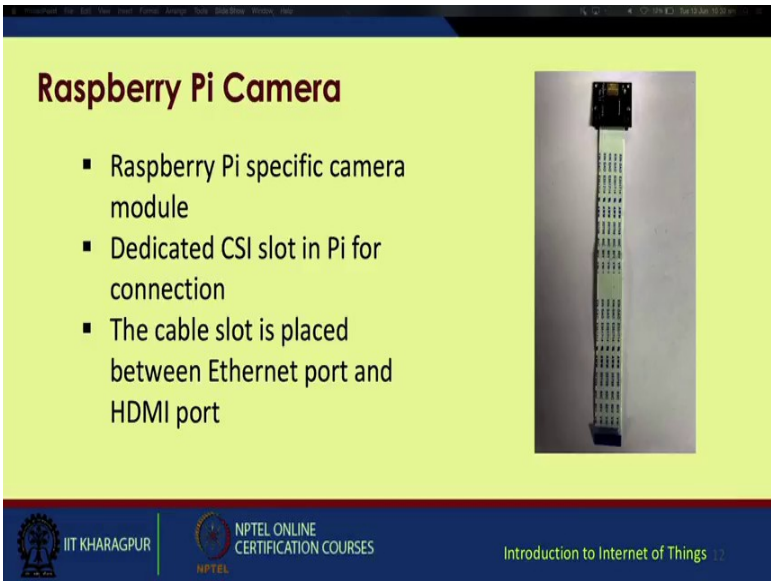
Here we are just going to show integration of raspberry pi camera.

(Refer Slide Time: 18:03)



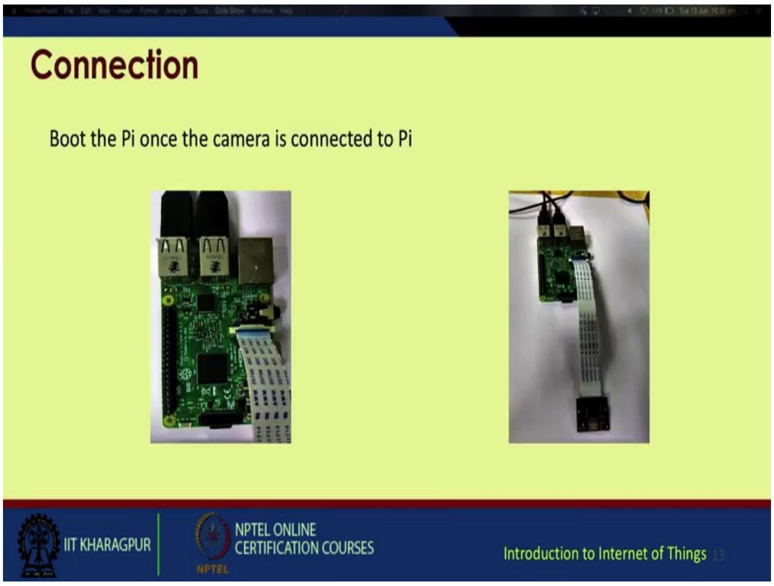
I am going to place my camera over here, my pi is booting up. Prior to this, we will cover the basics of the camera. So, you will need a pi cam and a raspberry pi.

(Refer Slide Time: 18:08)



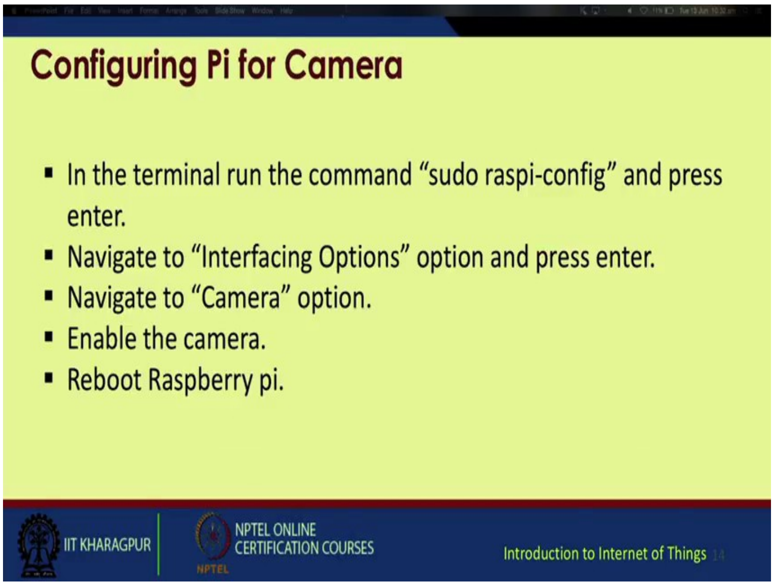
So, your raspberry pi specific camera module for on the raspberry pi you have a dedicated CSI slot for the connection and the cable slot is placed between the Ethernet port and the HDMI port told you before. The end of the ribbon cable you will find a blue tag and that has to be placed toward facing towards the Ethernet port.

(Refer Slide Time: 18:34)



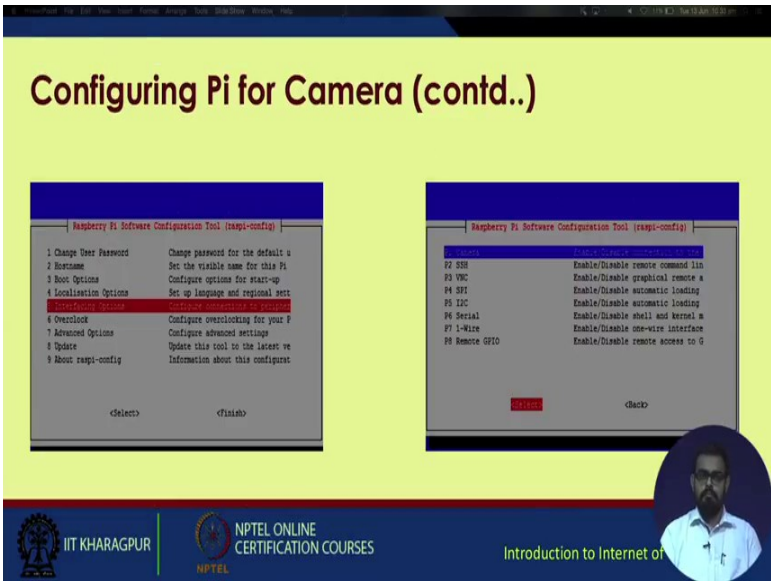
So, once the camera is connected we reboot the system. So, this reboot operation has already been done.

(Refer Slide Time: 18:43)



Now, in the terminal we run the command sudo raspi-config and press enter. So, this was covered in the first lecture on introduction to raspberry pi. I showed you there were various options one for enabling the camera another for enabling the SSH and so on. So, over there you enable the camera option and reboot your raspberry pi.

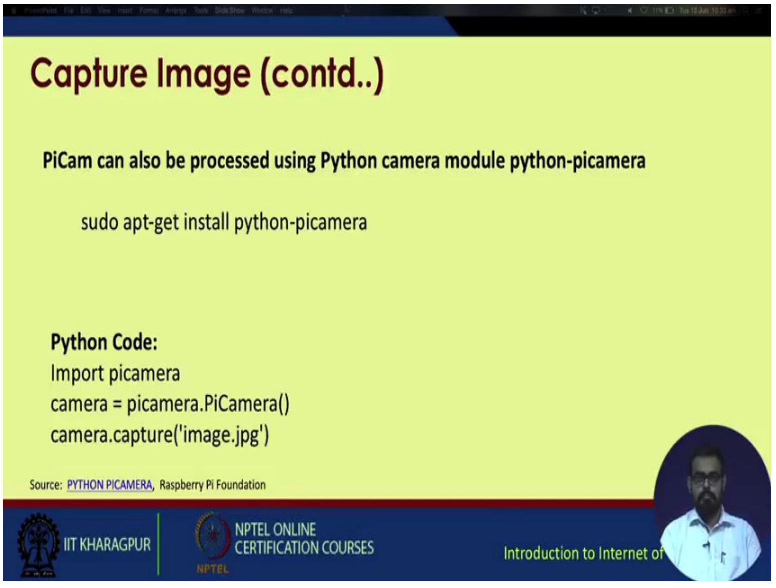
(Refer Slide Time: 19:08)



(Refer Slide Time: 19:11)

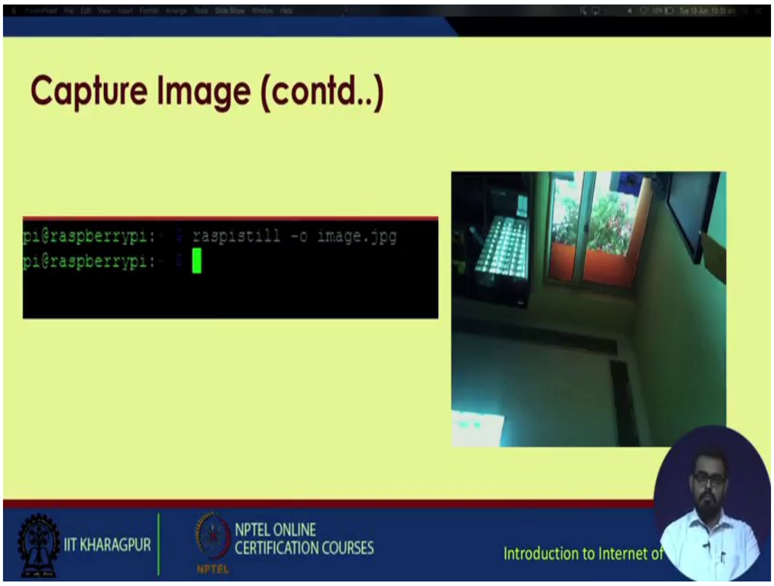
Now, once this has been done you can directly capture your images using the pi cam by writing on this terminal on this particular line of code raspistill -o space any image name.jpeg. So, this will click an image and store it as that "image name.jpg".

(Refer Slide Time: 19:40)



Now, this pi cam can also be integrated with python and the module particular module is known as python-picamera. So, again you will need to install this library because none of these libraries are by default available on your raspberry pi system. So, you write sudo apt-get install python-picamera. And this is the small code snippet for capturing your images from the pi camera using a python code, it is a very short script. So, first of all you import this library import pi camera then you initiate an instance of camera by this name camera = picamera.PiCamera(). So, you must pay special attention to the way it has been written you see the first pi camera is all small then dot PiCamera P and C are capital. Once this has been initialized within camera you write camera.capture then filename.jpg. So, these tutorials are commonly available online, you can go for advanced versions options also. So, these things are commonly available on any online resource.

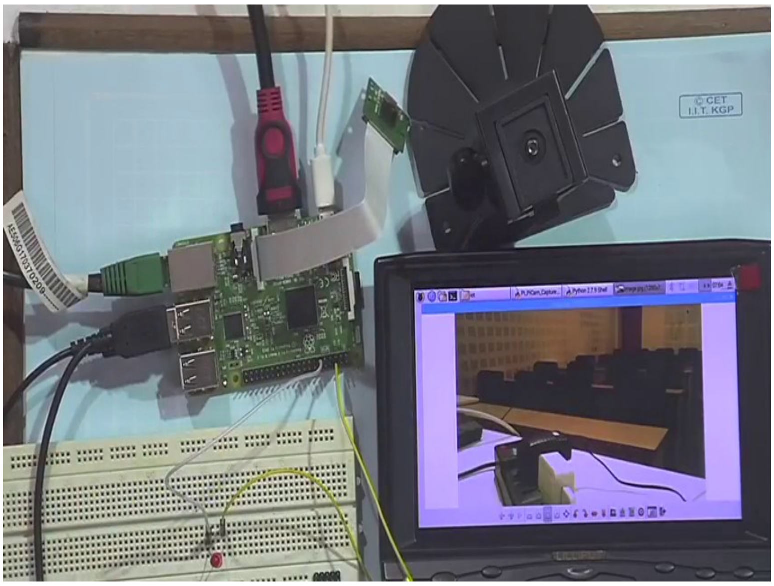
(Refer Slide Time: 21:03)



So, this is one screenshot. You write raspistill -o image.jpeg. So, your system will capture an image. So, coming back to the hardware part, so we have our camera ready. We have connected it to the network your raspberry pi to the network and it is connected to the monitor via HDMI port. Let us open the IoT folder. Now, we already have this code ready the three line snippet you saw earlier. So, this is the part of the code we are interested in. We simply run this code. Pay attention to the pi camera module, when it clicks an image then we have LED indicator going on. So, I run this module, you see this small LED indicator went off.

So, let us finish taking the image see it has taken the image of the roof. Let us try another image. We may delete this image also. Let us point the camera forward and run this code again. So, the code has executed, you see it has captured an image of the studio. So, this is just one of the basic examples of how you go about using GPIO based pins for integrating various small sensors. And actuators with your raspberry pi as well as IO integrate larger systems with your raspberry pi more complicated devices like cameras, you can integrate keyboards mouse and so on.

(Refer Slide Time: 23:48)



I have already put up interfaced a keyboard and a mouse over here through which I am actually controlling raspberry pi interface, you can see the cursor move and using the mouse to move it. So, this is as good as a computer its additionally it is very low on power requirements as well as it is quite cheap as compared to regular computers available on the market. So, I hope you will be able to go for more complicated projects using this basic idea.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 30
Implementation of IoT with Raspberry Pi- I

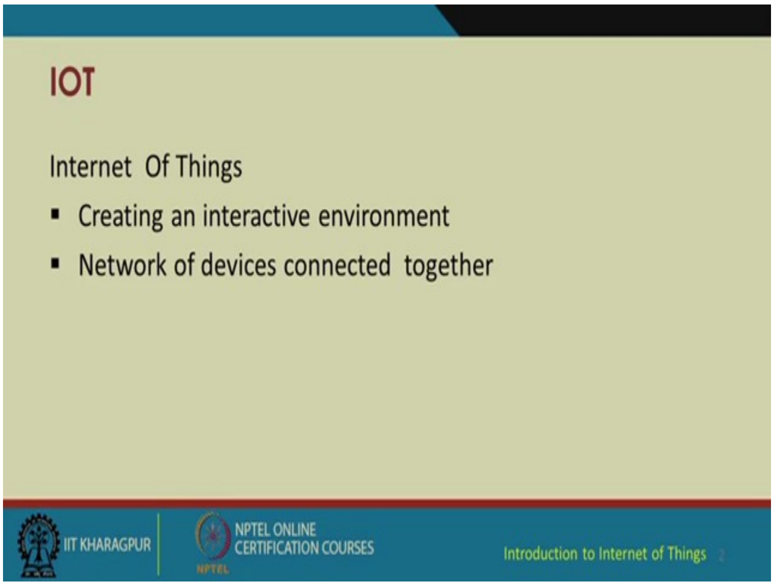
In the previous lectures on introduction to Raspberry pi, we have learned about how to configure Raspberry pi and how to use it along with 2 bear basic sensors on is killer sensor and the other one a camera sensor. So, 2 sensors were used and the basic interfacing was introduced to you in the previous 2 lectures. In this lecture you are going to learn about how to integrate Raspberry pi for for enabling IoT development.

So, here you are going to learn about you know these things in more detail. So, not only this lecture but the next 3 lecture I mean this one and the next 2 lectures you are going to learn about how to integrate the sensors, how to integrate the sensors different types of sensors not just one or two, but different types of sensors at the same time then after these sensors have collected this data then how to send the data how to disseminate the data through some kind of creation of socket to a remote server for that processing using in the UDP protocol which is a transport layer protocols. So, using UDP how to do particular this particular thing you are going to learn and there after you are also going to learn in this and the next 2 lectures about you know about how to visualize the data at the server.

So, the data is received then we have to visualize the data is received at the server at the server how to visualize the data this is what we are going to learn. So, I and Mr. Anandroop Mukharjee; your TA is going to taking through these few steps for achieving these things; that means, the data acquisition through these different types of sensors then sending through the network and there after you know visualizing the data at the server.

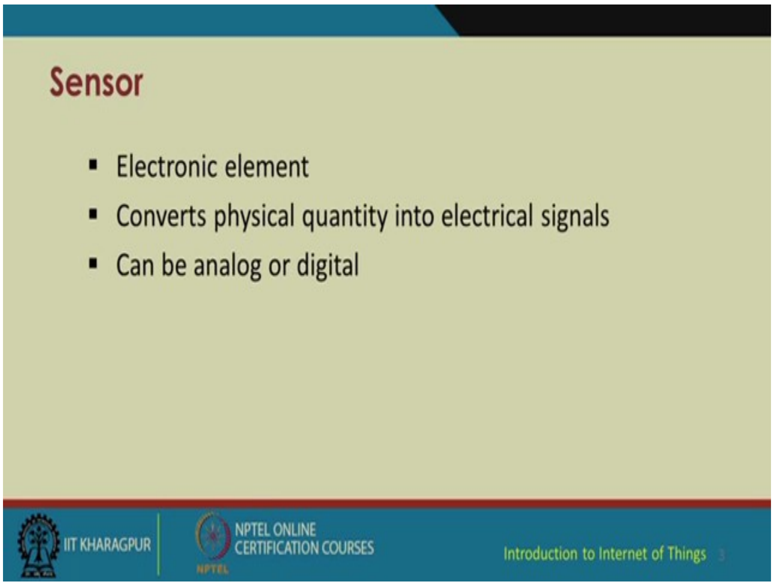
Hello, in this lecture this lecture will be covering 3 different parts of implementation of IoT with Raspberry pi. So, in part one will be discussing about using Raspberry pi to capture data from sensors and making a basic decision on the basis of capture data to actuate some device.

(Refer Slide Time: 02:55)



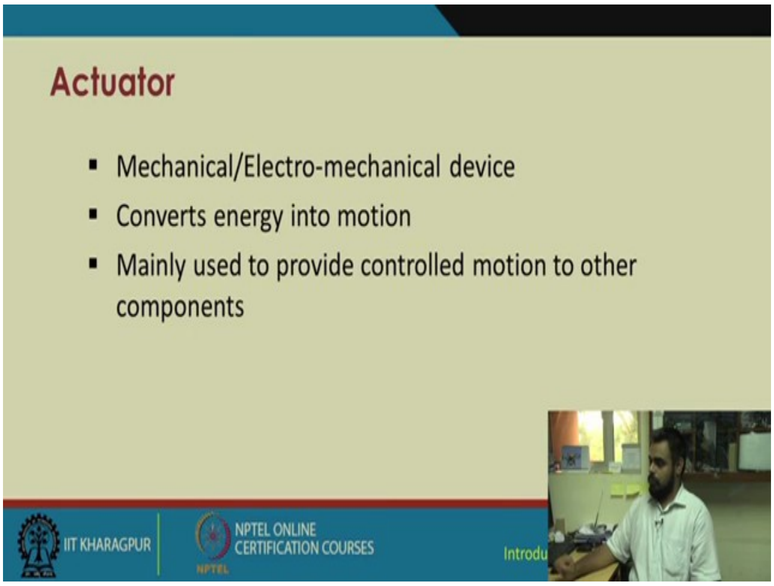
So, first of all 2 recapitulate internet of things basically needs to create an interactive environment and additionally it has a network of devices which are connected together. So, bringing these 2 together for this particular topic will get into the hands on.

(Refer Slide Time: 03:16)



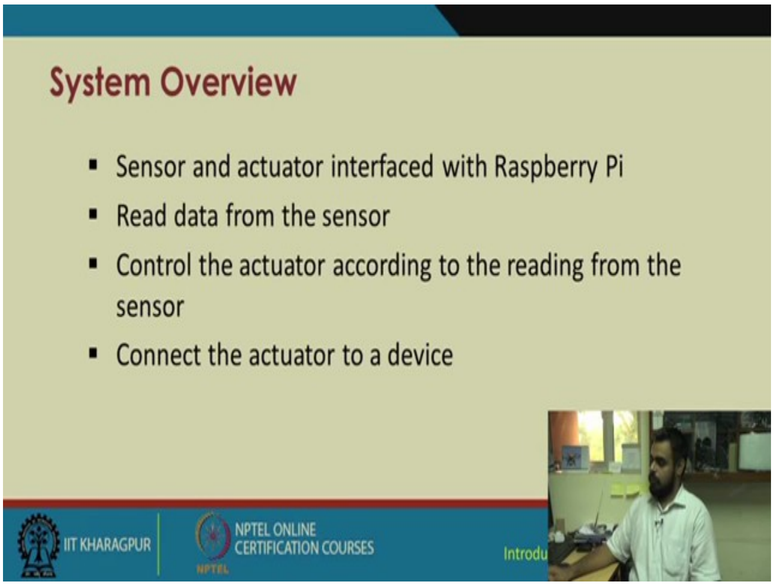
So, another thing regarding sensors as of already learnt by now and it has been discussed many times, sensors are electronic elements which convert physical quantity into electrical signals or any measurable quantity into electrical signals and sensors can be primarily analog or digital.

(Refer Slide Time: 03:37)



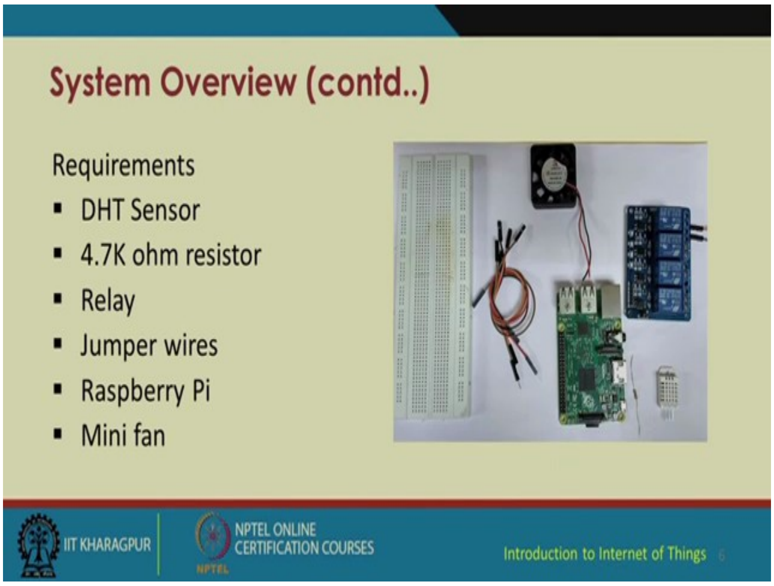
Similarly Actuators; Actuators are electro mechanical devices or they can be standalone mechanical devices also and generally they actuate or convert energy into motion. So, mainly they are used for providing control motion to other components in a big system.

(Refer Slide Time: 03:59)



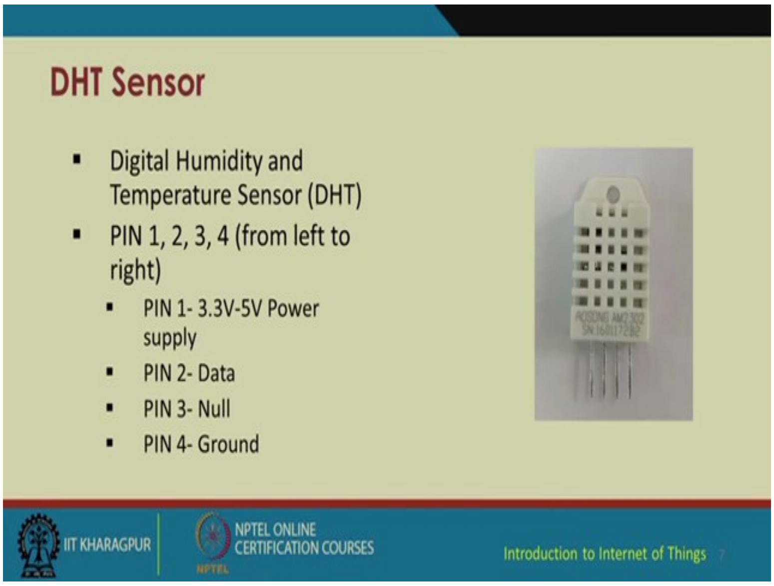
So, in this a system overview is is as follows sensor and actuator are interfaced with Raspberry pi, data is read from the sensor the actuator is controlled according to the readings from the sensor and the actuator basically which is connected to the sensor is being controlled from the readings and this control mechanism will be showing a brief decision making loop which can be replaced by additional much higher inversion like machine learning statistical learning or even deep learning based methods.

(Refer Slide Time: 04:42)



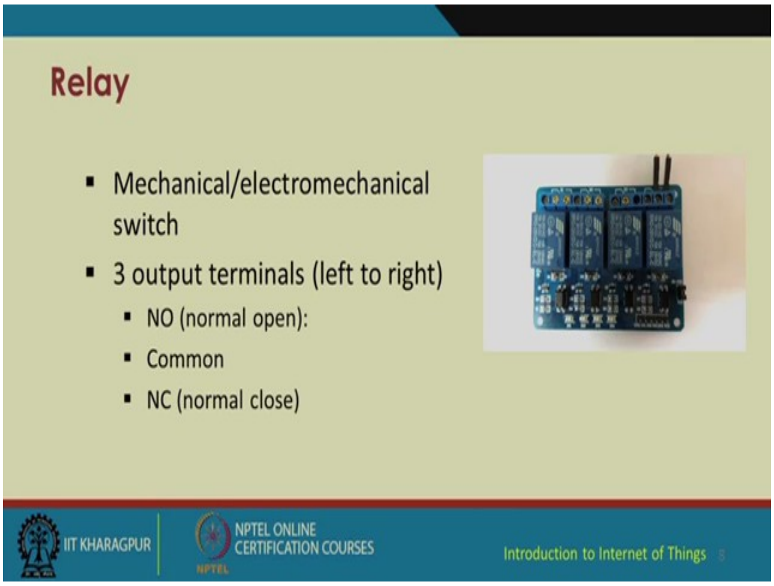
So, for this, the following are the system requirements we are again using a DHT sensor which as a digital humidity and temperature sensor we are using a 4.7 kilo ohm resistor relay some jumper wires Raspberry pi and mini fan which we have going to connect to the relay to show the effectiveness of our decision making approach.

(Refer Slide Time: 05:05)



So, as you already know this digital humidity and temperature sensor it has got 4 pins. So, generally when you keep it like it is shown in the slide from left to right you number the pins 1 up to 4 and pin one is generally use for power supply rangers from 3.3 to 5 volt pin 2 supplies the data to the process a board to which this sensor is connected, pin 3 is generally kept open and pin 4 is connected to the ground.

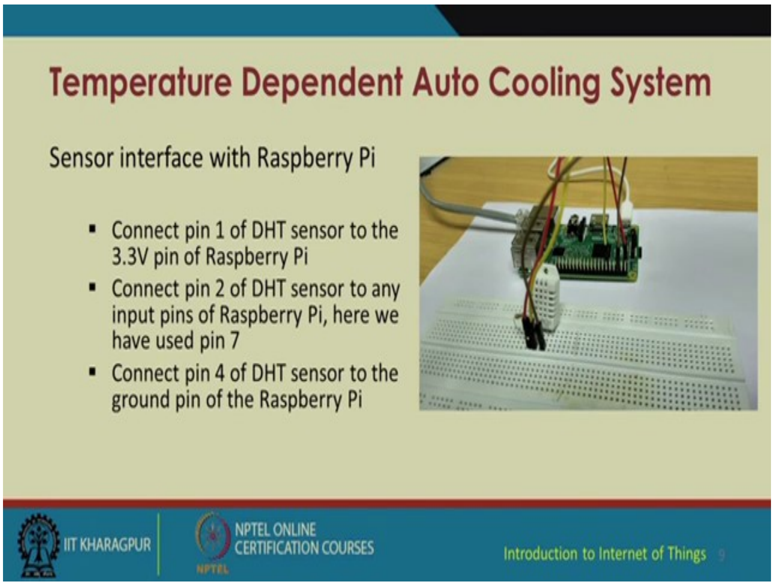
(Refer Slide Time: 05:39)



And this one is called the relay board it is an electromechanical switch. So, it has got 3 output terminals starting from left to right. So, in this particular board you can see there are actually four relays this is a composite board consisting of four different relays. So, you can connect four different devices to it this single entity is known as one relay and in electronic we call this a sugar cube relay generally you can find sugar cube relays ranging from operating voltage as of 6 volts up to 12 volts.

So, as you can see there are 3 terminals corresponding to each relay. So, from left to right the first terminal is designation NO or normally open the middle one is common and the third terminal is known as NC are normally close.

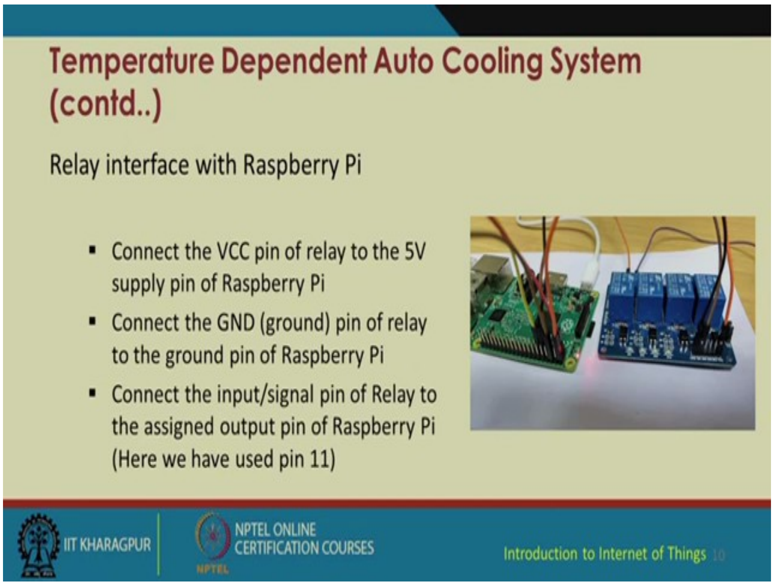
(Refer Slide Time: 06:37)



Now, what we are about to attempt is a temperature dependent auto cooling system. So, for this the primary sensor interface with the Raspberry pi is going to be using DHT. So, we have already discussed and showed you the demos of how a DHT is connected to Arduino board as well as the Raspberry pi. So, again just to recapitulate we connect pin one of the DHT sensor to the 3.3 volt power supply of Raspberry pi we connect pin 2 of this DHT sensor which supplies data to Raspberry pi to pin seven and finally, we connect pin four of the DHT sensors to the ground pin on the Raspberry pi.

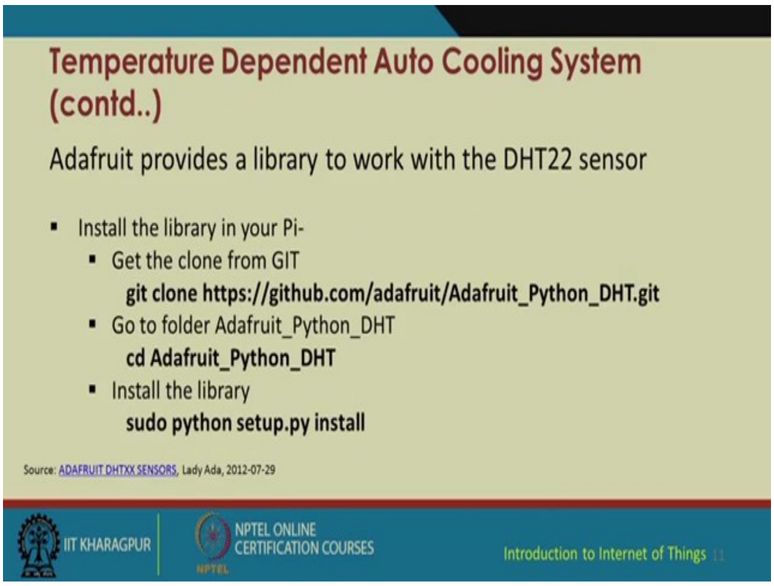
However it is to be noted for this DHT sensor this follows the BCM configuration of Raspberry pi. So, if you recall Raspberry pi has 2 configurations we generally discussed with the board configuration these 2 configurations are board and BCM. So, board configuration we had discussed in the previous lecture. Now in this one will be mainly working using this DHT sensor in the BCM mode as specified by its manufacturer.

(Refer Slide Time: 07:57)



Now additionally the relay interface with the Raspberry pi is as follows we connect the VCC pin of the relay to 5 volts supply of Raspberry pi you connect the ground to the ground of Raspberry pi and the input signal to the relay is assign to pin 11 and another point to remember is when we are using relay we are not using the BCM mode we are using the board mode. So, this pin number 11 is going to be according to board mode whereas, in the previous slide this pin 7 is according to BCM mode. So, these both these modes will be used simultaneously.

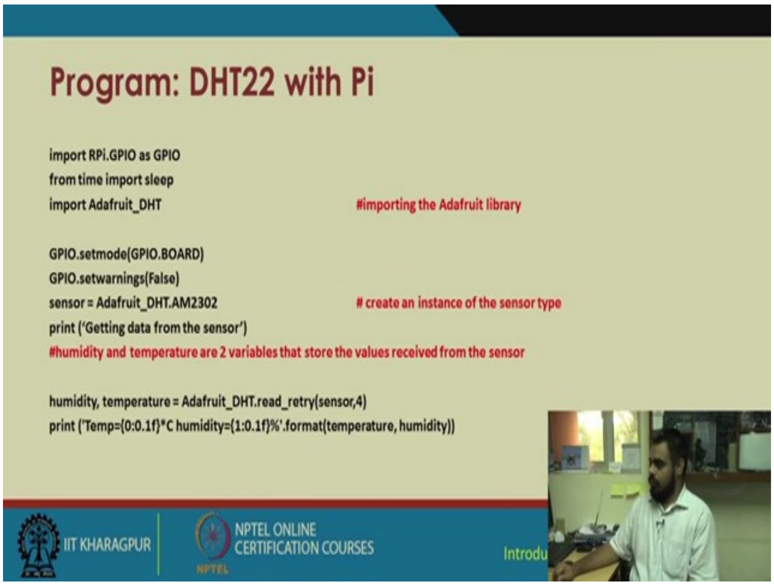
(Refer Slide Time: 08:42)



Now, try to beginning the programming part like in Arduino we install and additional library for this DHT sensor. Similarly for Raspberry pi we need to install in additional library from Adafruit which basically supplied this sensor. So, we are using this DHT 22 sensor first of all in your Raspberry pi you need to install your Adafruit DHT sensor library using the following command and a point to remember is since you your using python base scripting we are going to implement the DHT python library you may be able to find come or cross DHT C library, DHT C++ libraries but we are more interested on in the python library.

So, the first line is this git clone https you follow this link and you press enter you will see here Raspberry pi it terminal its starts if it is connected to the internet it will start downloading this folder if go to the once the download is finished we go to the downloaded folder by putting in this command cd Adafruit_python_DHT because this will be the name of the folder which has been downloaded on your Raspberry pi system and remember this is not the installation the installation is yet to come. So, after you go into the directory you install the library by running this command sudo python setup.py install. So, once your installation is successful you can easily start creating codes for DHT using python and Raspberry pi.

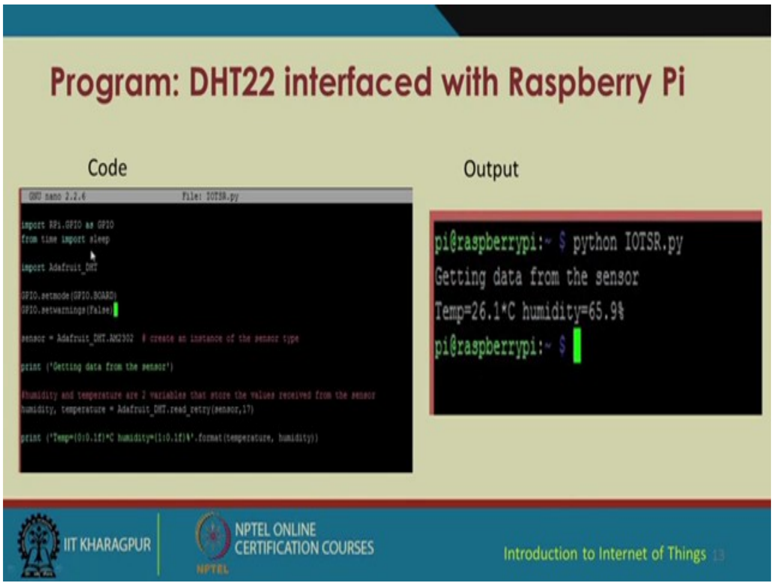
(Refer Slide Time: 10:32)



So, we have a sample DHT interfacing program with Raspberry pi first line starts off with importing the GPIO pins. So, import RPi.GPIO as GPIO then we import the time library for calling in the sleep function which provides delays 2 hour program and then we import the Adafruit_DHT library which we previously installed now the GPIO mode is initially set as board and warning have been set to false for the Adafruit it automatically takes the board mode as BCM. So, we are not explicitly identifying anything. So, sensor equal to Adafruit _DHT.AM232; 2302. So, this line has to be explicitly mentioned according to the documentation provided by the manufacturer and then we just print a line to signify whether this sensor have been successfully initialized or not and we assigned humidity and temperature values from the Adafruit library function by using read _retry and in name this sensor which we initially called and which is connected to BCM pin 4.

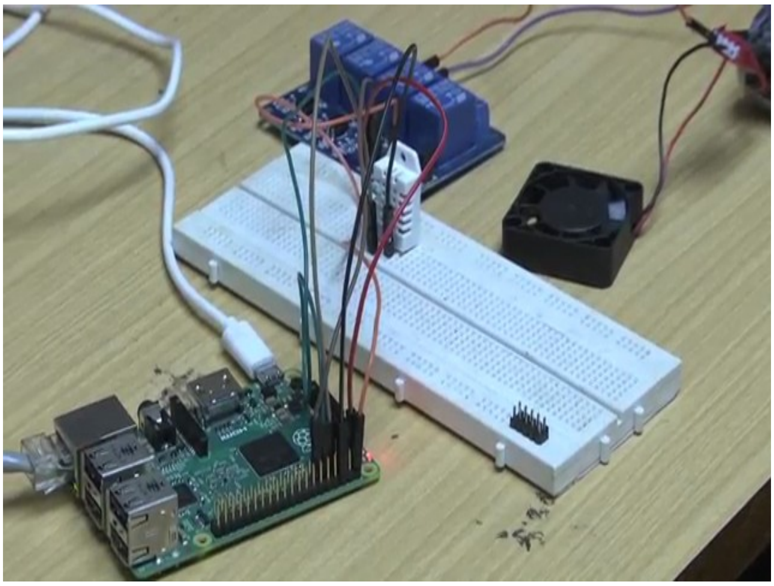
In the next line we print the temperature and humidity values iteratively not a iteratively we print this once, but we format it according to our needs.

(Refer Slide Time: 12:11)



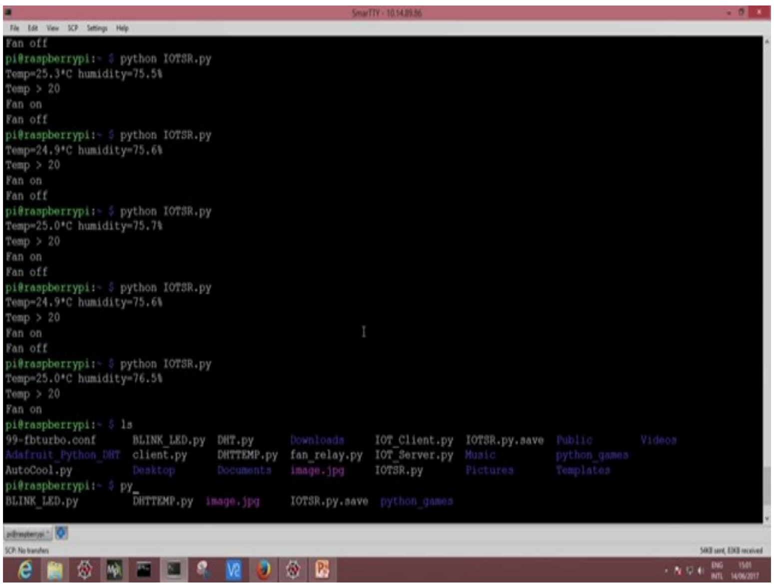
So, this is the code which we just showed on the right hand side you can see the output we created a python file on the Raspberry pi named IOTSR.py once it is executed it gathers data from this sensor and you can see your formatted print line is temp equal to 26.1 Celsius and humidity is 65.9 percent.

(Refer Slide Time: 12:52)



So, we can zoom into the hardware circuitry now as you can see this is your DHT sensor it is placed on the breadboard and according to the configuration mentioned previously in this slide we have connected the VCC ground and the data pin to the appropriate pins on the Raspberry pi board there are additional component attached will come to those later. But for now will be focusing on only these 3 wires the brown wire the red wire and the black wire.

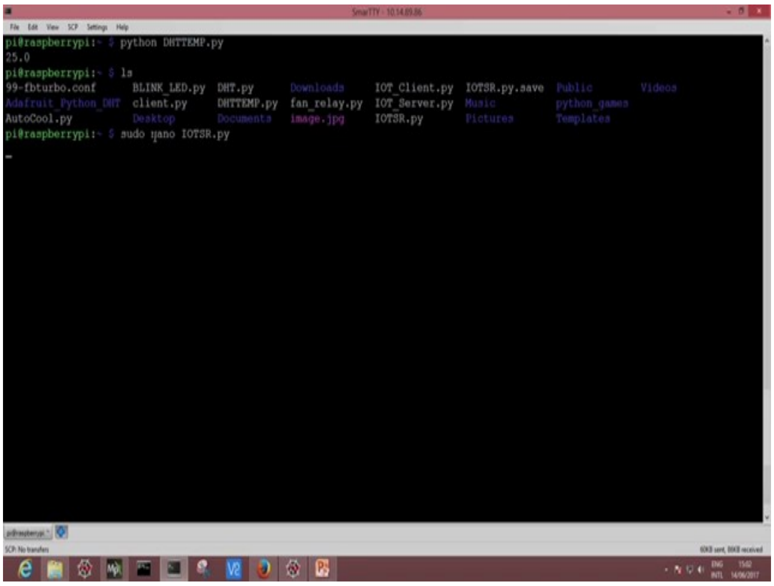
(Refer Slide Time: 13:35)



So, coming back to the programming part I have remotely logged into the Raspberry pi system just increase the font a little bit. So, using this terminal I have actually logged into the

Raspberry pi. As you can see over here pi at the rate Raspberry pi I go into the directory I see that I have testing file named DHTTEMP.py lets run this first.

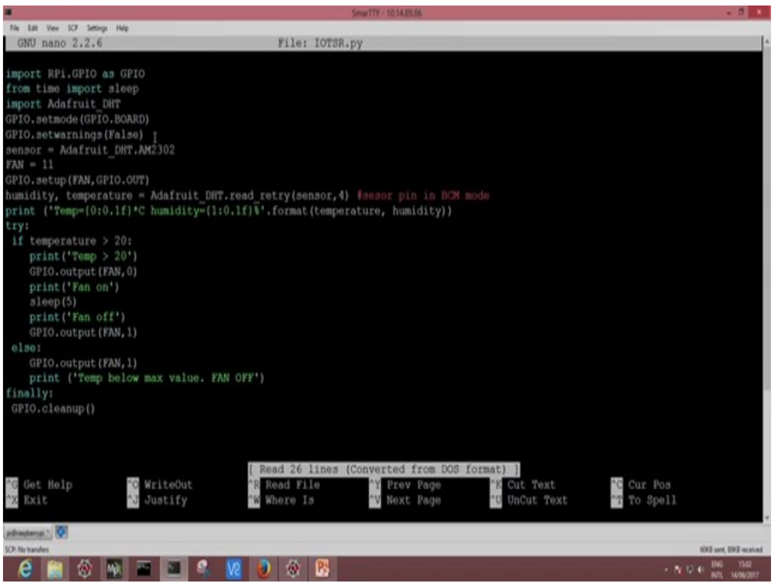
(Refer Slide Time: 14:41)



So, we give the simple command python DHTTEMP.py as soon as it is executed is a simple code to fetch only the temperature readings from the DHT sensor, so, the temperature reading as been read as 25.0 degree Celsius.

Now, will look at the IOTSR file, so, we have our IOTSR file over here lets open the editor and check whether the contents are the same.

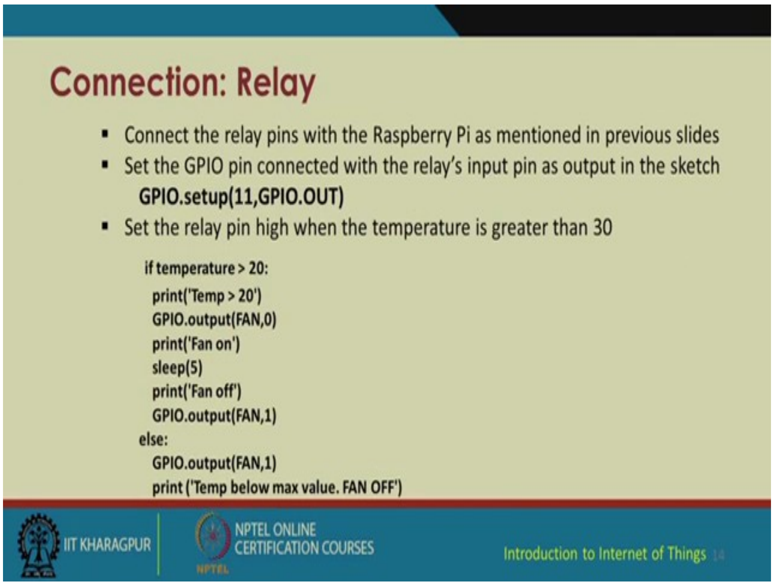
(Refer Slide Time: 15:33)



So, we have imported the GPIO library we have imported the time module we have imported the Adafruit library we installed we have set the board mode. So, as I have told you before the Adafruit.read_retry this thing is pin is on by defaults setting BCM mode. So, this pin number four is according to BCM mode whereas, I have connected a relay I will come to that in the consecutive slides have connected a relay and it is connected to pin eleven according to the board mode.

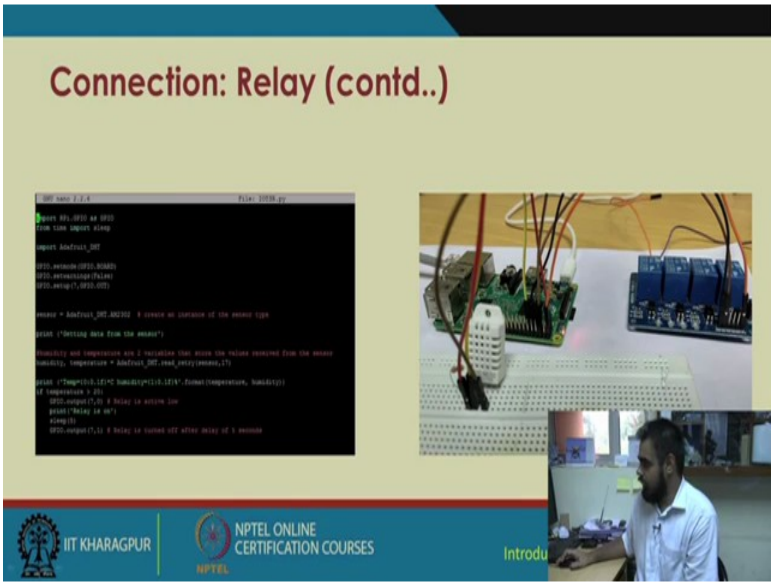
Before going furthers, we have not checked our Raspberry pi is working fine the DHT sensor is working fine.

(Refer Slide Time: 16:41)



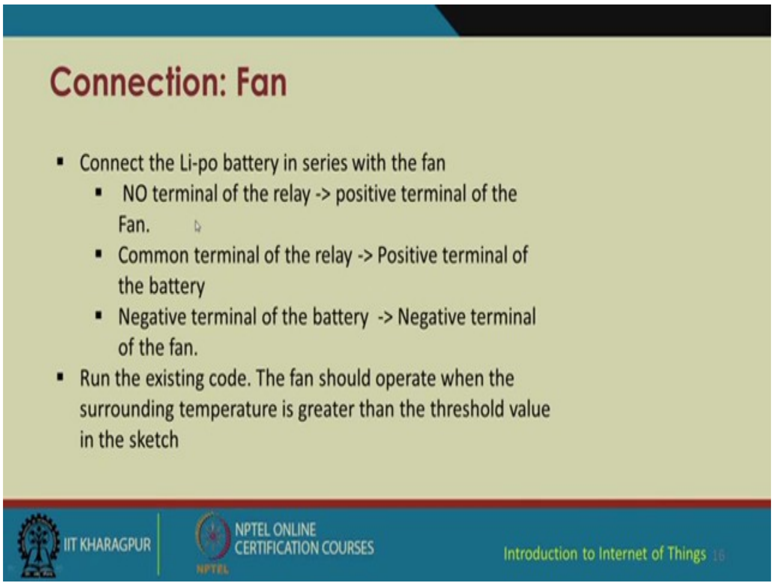
We are now connecting the relay part. So, we connect the relay input pin at pin eleven of the Raspberry pi using board mode and we put in the basic decision making loop that if temperature is greater than twenty you print temperature greater than 20 and it will turn on the relay. So, it will a fan is connected to the relay. So, I have just return fan comma 0 that is the fan will be turned on and then it will sleep for 5 minutes and then fan will be turned off and output pin will be again set to 1 otherwise if temperature is lesser then 20 the fan going to be switched on.

(Refer Slide Time: 17:32)



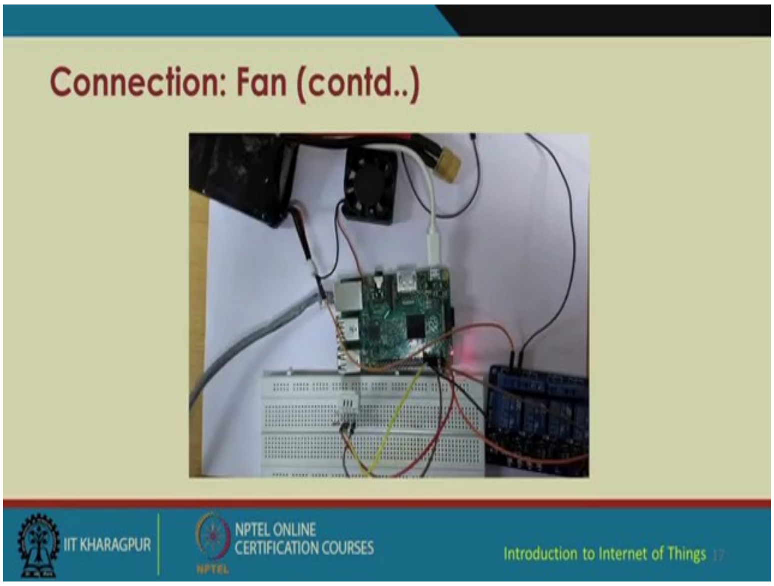
So, on the left hand side this is the code actually open this code few movements back on the Raspberry pi console and on the right hand side you have this relay board you have this DHT sensor connected to the Raspberry pi.

(Refer Slide Time: 17:52)

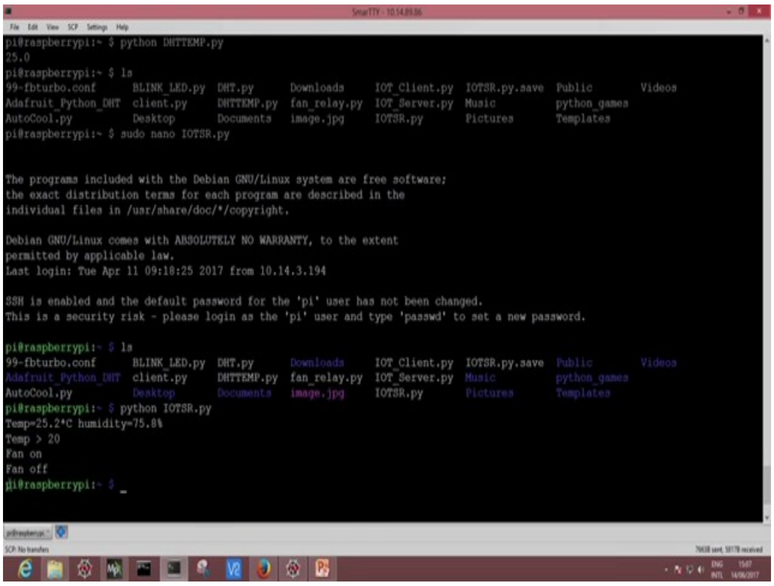


Now this connection of the Li-po with the fan sorry, the connection of the relay with the fan is as follows we are connecting we are using lithium polymer battery we can use any other battery of sufficient rating since the fan we are using runs on 12 volt we are using a 12 volt Li-po battery to operate the fan the normally open terminal of the relay or the positive terminal is connected to the positive terminal of the fan in the common terminal of the relay is connected to positive terminal of battery negative terminal of battery is connected to negative terminal of the fan and when these connections have been made and the connection have been rechecked we run the IOTSR.py file. So, the connection will looks something like this.

(Refer Slide Time: 18:46)



(Refer Slide Time: 18:58)



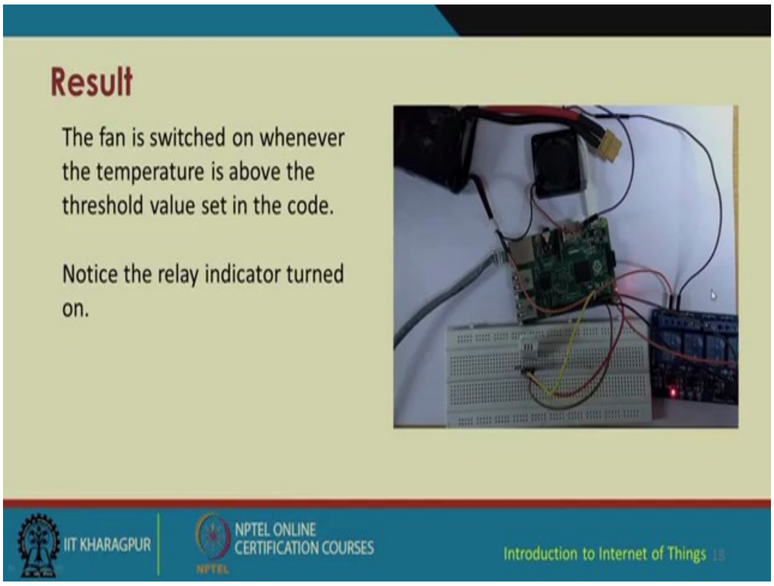
Now let us again log into Raspberry pi. So, once we execute this file you will see the output but prior to that I like to show you this is my Raspberry pi this was my DHT sensor giving me humidity and temperature readings this is my relay board this is the four channel relay board because you can connect four devices simultaneously. So, this one unit is known as a relay this single unit is called a sugar cube relay as you can see it has got 3 terminals normally open common and normally close and we have this small fan over here which is connected to a Li-po battery 3 cell Li-po. So, again back to the terminal will execute the code now.

So, as soon as the code is executed it gets the reading of temperature is 25.2 degree Celsius and humidity is almost 76 percent now the decision making loop has detected that the temperature is greater than twenty. So, it turns on the fan and after that after 5 seconds the fan is turned off. So, this can be modified the modifying the loop and instead of using a normal if else loop you can go for if else loop or a normal rule based decision making we can; obviously, go for various machine running best approaches only condition been that you need a lot of data historical data to predict the next action.

So, if you again focus on the circuit I like to show when I run this program again if you pay attention to the fan and it is connected to this relay board as soon as the program is executed and if the relay is turned on there will be a light blinking against the corresponding relay to which the fan is connected to this relay.

So, you see it has detected the temperature is greater than 25 the relay has been turned on, you see the fan is now also turned on after 5 second it will turn off. So, basic application is you can use this for automated cooling systems may be for your PC or may be for your various other systems or may be in industrial systems. Also suppose if the temperature of a Furness gets higher or if a temperature of a particular room or work place gets higher your fan automatically turns on and the network connected device remotely intimates you that your temperature is going high so, the fan has been turned on.

(Refer Slide Time: 22:22)



So, the outputs have been explode. I hope this gave you a bit of learning experience well cover other things and details in our next slide.

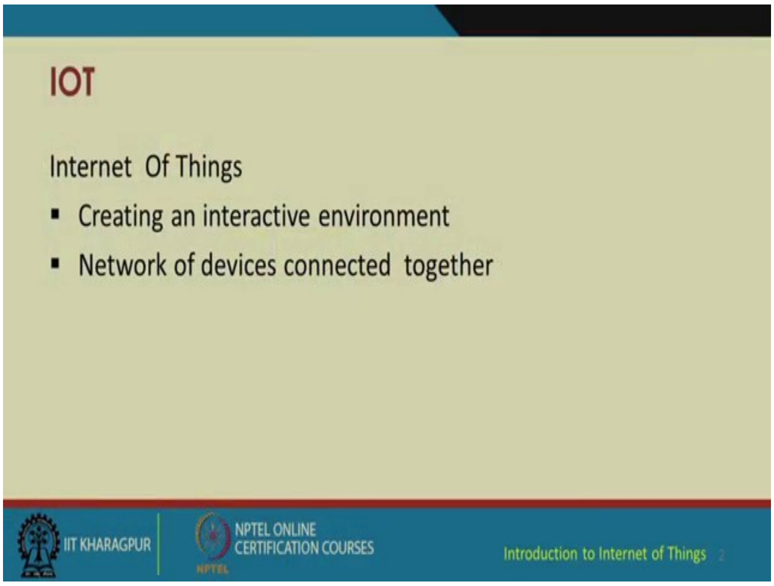
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 31
Implementation of IoT with Raspberry Pi – II

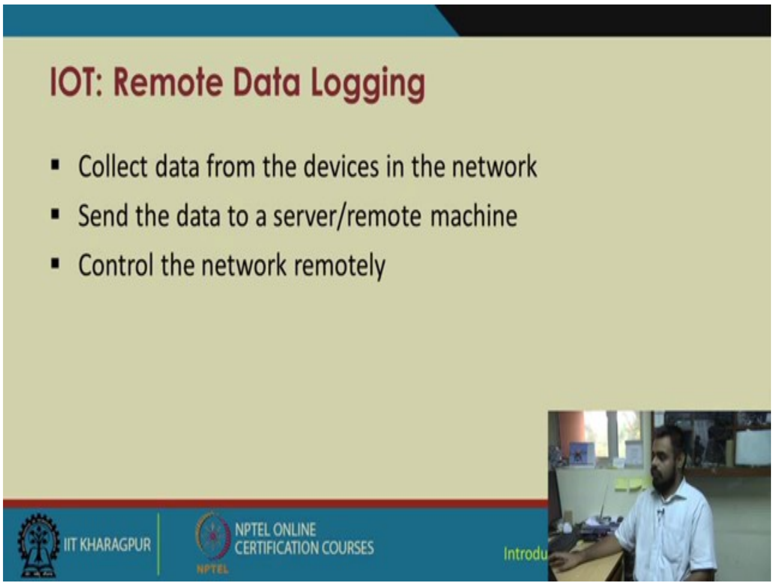
Hi, in this lecture of the second part of implementation of IoT with raspberry pi we are going to discuss the same integration we discussed previously that is integration of a DHT sensor with raspberry pi. Additionally we are going to include some networking components to it that is we are going to implement a python scripting for client making the raspberry pi behave as a client whereas, on the remote desktop which will act as a server will use another python script which will act as a UDP server. So, in this way we are going to create a datagram based connection between the raspberry pi client and the desktop based server.

(Refer Slide Time: 01:09)



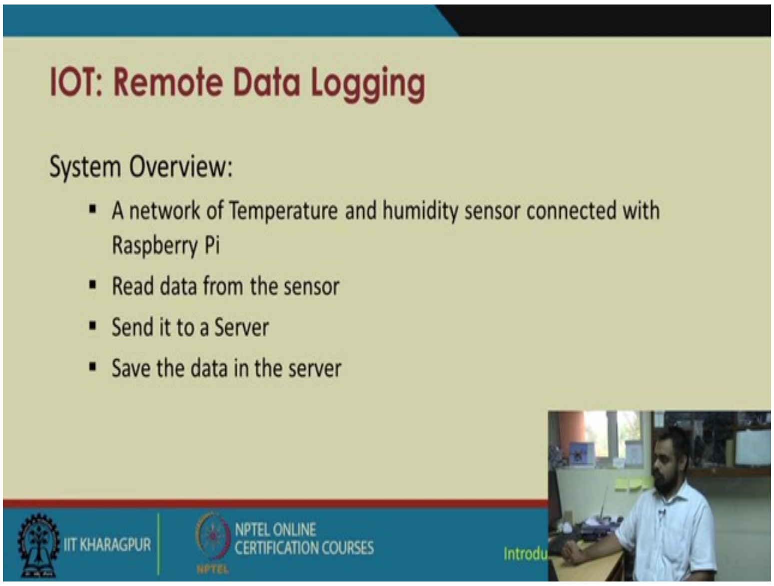
So, again basic aim of this internet of things is to create an interactive environment of network devices which are all connected together additionally your devices more the number of devices.

(Refer Slide Time: 01:20)



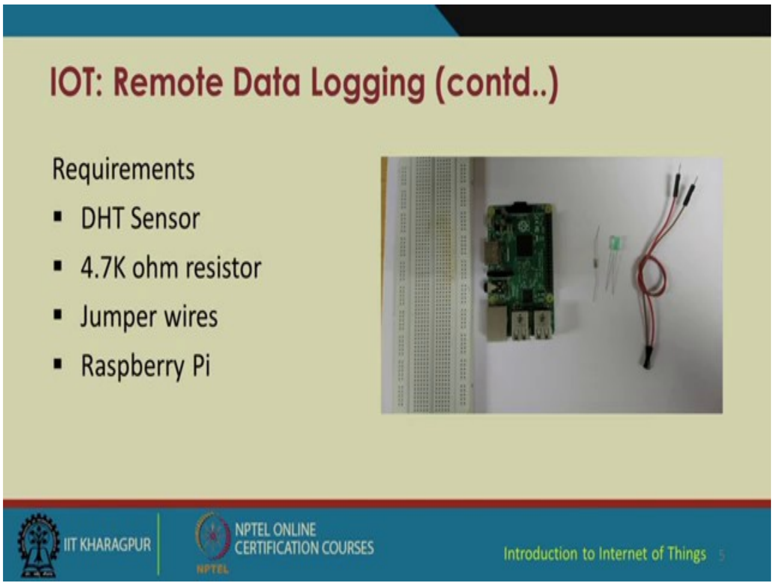
The more intelligent and interactive your whole system should be it should not be that you are increasing your device number of devices whereas; your system performance is going down. So, by maintaining your system performance the device integration has to be made. So, I am sure the various strategies have been covered in the previous theoretical lectures in this one we are going to give a basic demonstration of whatever you have learnt in your previous lectures a very rudimentary demonstration.

(Refer Slide Time: 02:29)

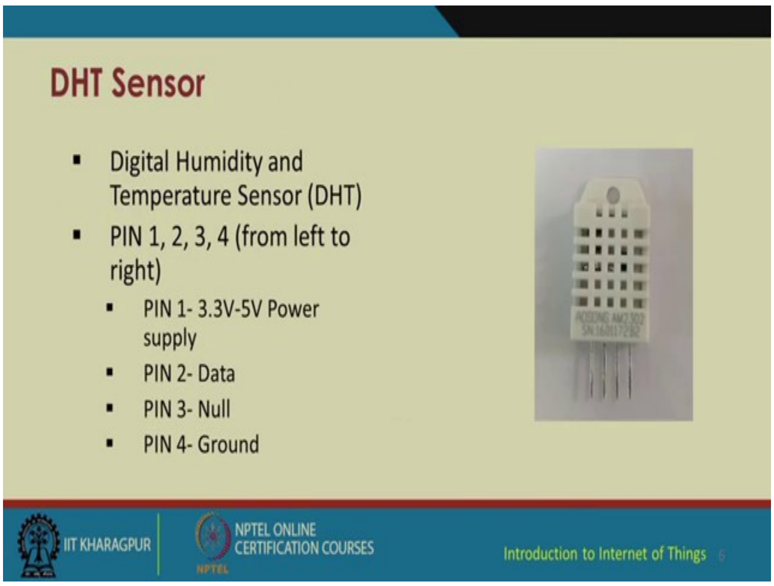


So, in this second lecture we will be focus more on remote data logging. So, it will be collecting data from the devices in the network, it will send the data to a server or a remote machine and that remote machine will the remote machine will control the client or the data sending device remotely. So, the system overview is as I have told you previously and network of temperature and humidity sensors will be connected to raspberry pi. Here for the sake of demonstration we are only connecting one temperature and humidity sensor with single raspberry pi data from the sensors are read it is sent to the server over the network and the data is saved in the server.

(Refer Slide Time: 02:51)



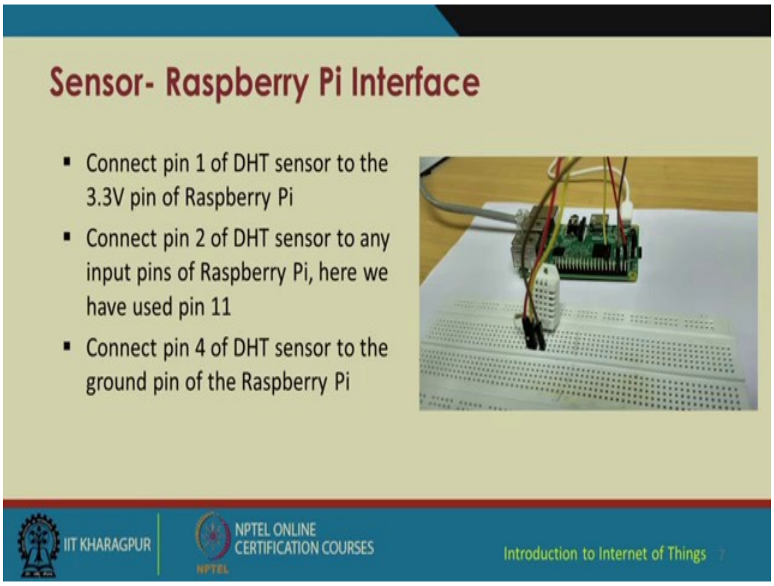
(Refer Slide Time: 03:20)



So, same as before we have the same requirements a raspberry pi a DHT sensor a 4.0 kilo ohm resistor it is to be noted that for raspberry pi this 4.7 kilo ohm resistor must be obtain between the BCC and the data pin that is between pin one and 2 additionally we will be requiring jumper wires to make our connections again for recapitulation well go about discussing the DHT.

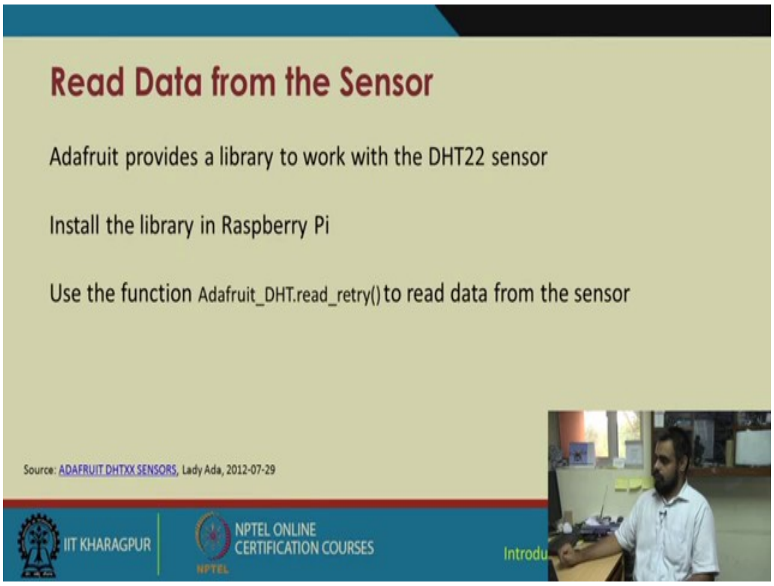
So, from left to right if you keep the grid side up; you have pins numbered 1 to 4 first being the Vcc pin 4th being the ground and the second pin is used for transmitting data.

(Refer Slide Time: 03:40)



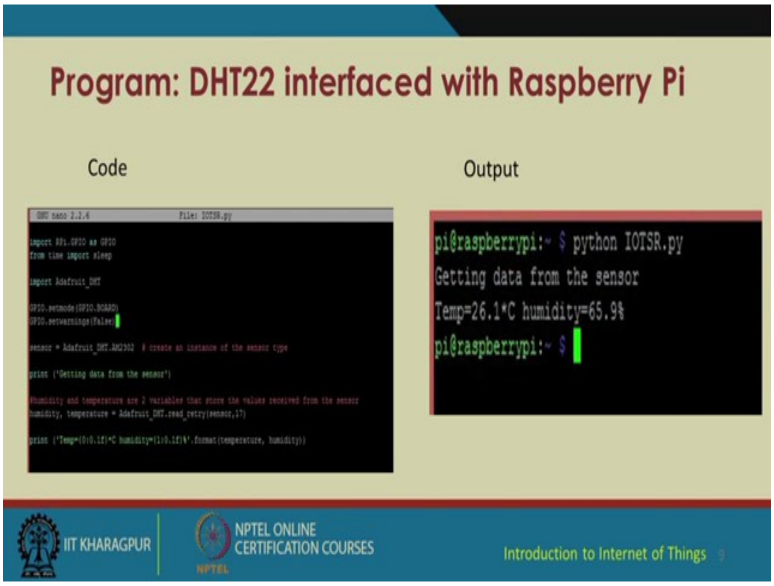
So, the connection to the raspberry pi will be as follows from the previous lecture we have just debuted a little bit you can also use the same configuration as done in the previous lectures, but remember the board configuration for this DHT sensor must be in BCM mode not in board mode. So, we are connecting the DHT sensor to 3.3 volt pin of raspberry pi we are connecting the data pin or pin 2 of the DHT sensor to pin 11 of raspberry pi this pin 11 is in BCM mode and we are connecting pin 4 of DHT sensor to the ground pin of raspberry pi pin.

(Refer Slide Time: 04:26)



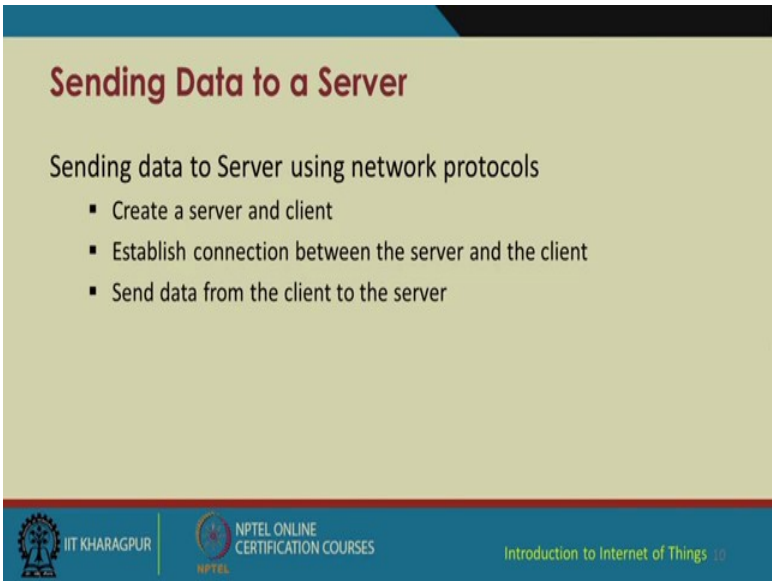
Now, as in the previous lectures we have already covered this Adafruit which supplies this DHT 22 sensor they also provide a library to integrate this sensor to raspberry pi via python frame work. So, this has already been installed during our previous lecture. Now we are going to call the Adafruit_DHT.read_retry() function to read data from the sensor.

(Refer Slide Time: 05:01)



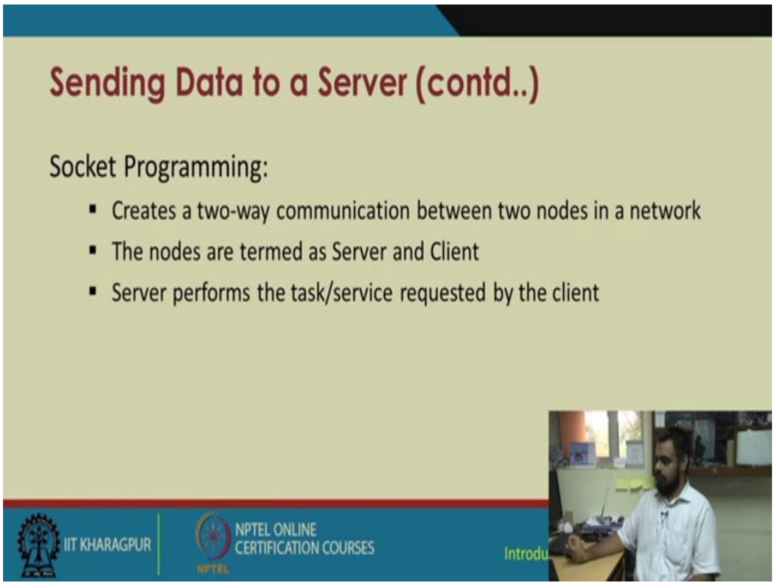
So, as you can see the codes and the outputs or more or less similar to the previous one.

(Refer Slide Time: 05:16)



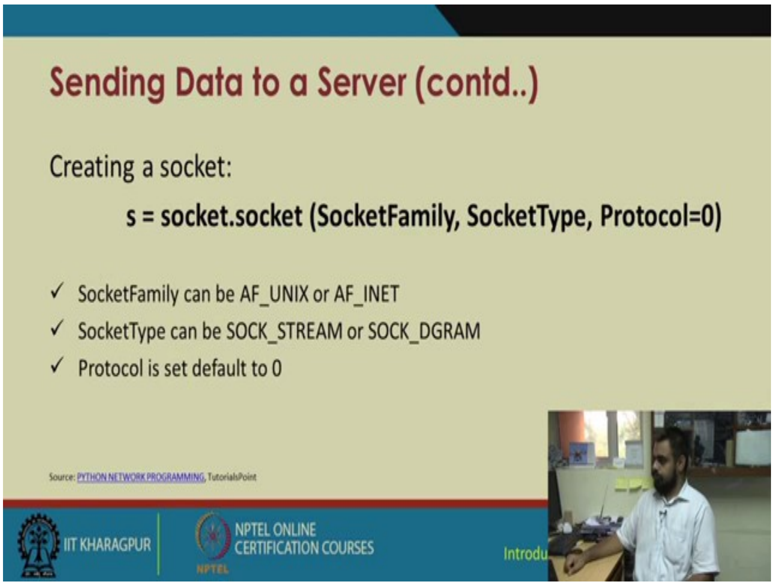
We are going to read the temperature only the additionally you can attach your humidity readings also, but for the sake of testing you can just go with the temperature readings. Now for sending the data over the network we will be using a client server client server model and to establish the connection you are going to take the help of a UDP based socket will make a UDP based socket which will send data from client to the server now for this socket programming.

(Refer Slide Time: 05:51)



This generally sockets create a 2 way communication between 2 nodes in a network, 1 node is termed as the server whereas, the other as is termed as the client the server performs the task or the service as requested by the client.

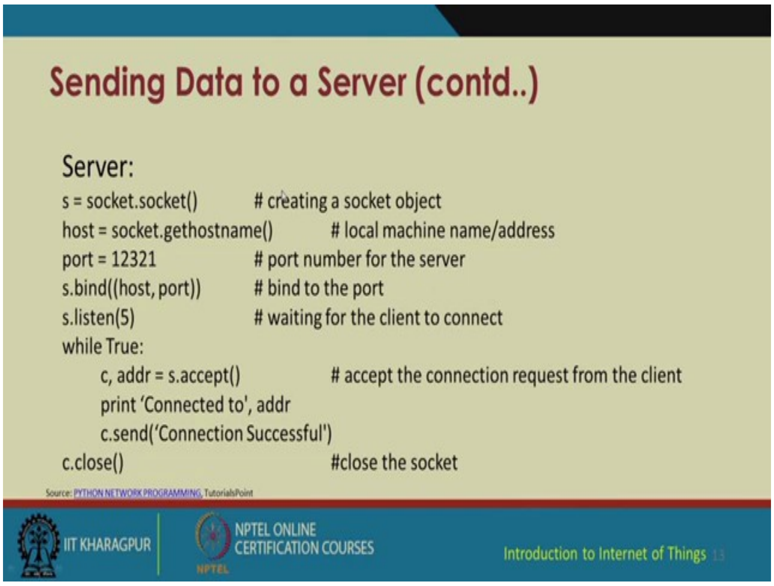
(Refer Slide Time: 06:11)



So, how do you proceed by creating a socket on raspberry pi this was also covered in the previous lectures on introduction to raspberry pi. So, it is quite simple to assign the socket.socket function to a variable and you manipulate that variable.

So, this socket.socket function it has three arguments first is SocketFamily second is SocketType and third is Protocol which is by default zero socket family can be either AF_UNIX or AF_INET. So, UNIX as you recall it is mainly for on the UNIX base systems whereas, for most of the general purpose programming we are going with AF_INET or internet protocols socket type can be either Socket_Stream or Socket_data gram.

(Refer Slide Time: 07:10)

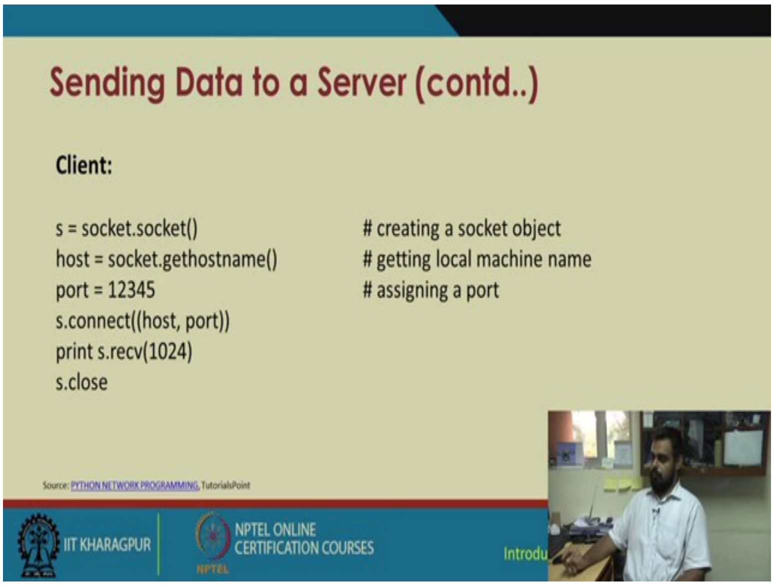


Now while sending a data from a client to a server we need 2 scripts one for the server and one for the client and 2 things will be required first is the IP address of the server and the port of the server to which your client will bind.

So, your client can have a variety of IP addresses, but it is important that your server retain a singular IP address see for this infrastructure for this exact project we are demonstrating you only require one way communication that is from the client to the server. So, your clients do not need to have fixed IP addresses may be they can have a variety of IP addresses about which the server has no prior knowledge, but it is very important that each and every client should be aware of the servers IP address as well as the port to which the client is going to connect. So, we start off with calling the functions of socket.socket we put the host as socket.gethostname we assign a particular port and we bind to the port by calling the host name is the first argument and the port number as the second argument and we start our listening function which waits for a client to connect to it.

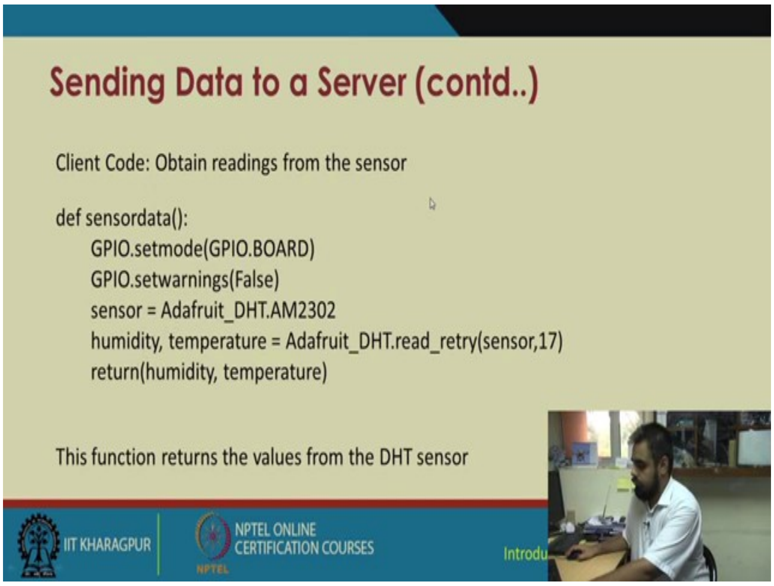
Now, while true it signifies while a client has accepted the connection and connected to your server on that particular port it will generate one address and this address can be stored and later on used for later on used for time stamping your data to which on your server in various data logs. So, imagine your your server has been connected to 20 different IP addresses or clients. So, these 20 clients are sending variety of data to you, but you need to know the exact location of each of these clients. So, that later on you can segregate the data and connect to it.

(Refer Slide Time: 09:53)



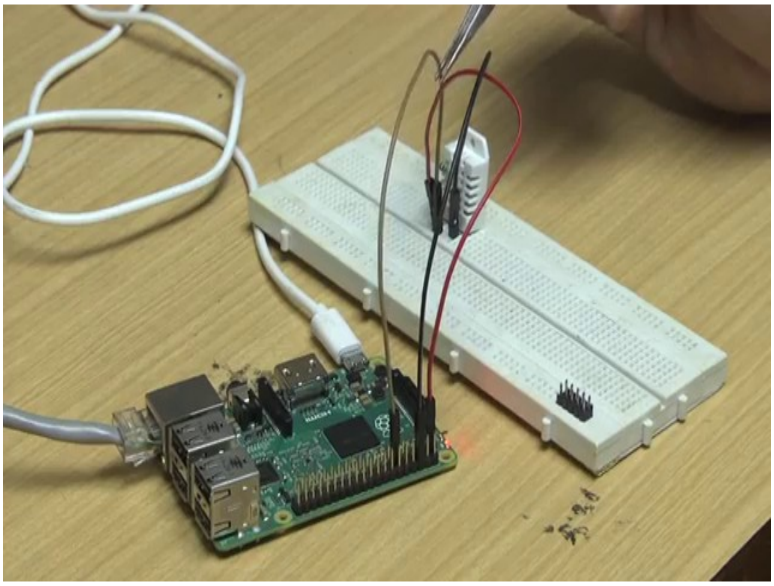
So, once your connection has been accepted it sends the server sends connection successful and eventually when the socket is terminated by the user you call the functions c.close() for the client side again you call the functions socket.socket then you get the host name assign the port. Point to remember is this port number is similar to the servers port number because your client will be connecting to servers that particular port number and this host or the host name we are talking about this has to be the servers IP address.

(Refer Slide Time: 10:38)



So, s.connect you connect to that particular IP address of that server on that particular port and you print that your data is being received s.receive and eventually you close the connection.

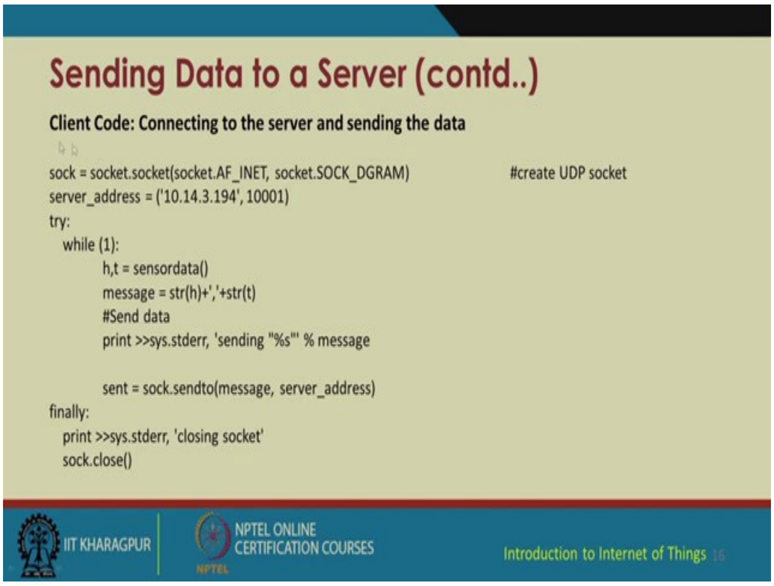
(Refer Slide Time: 10:57)



So, prior to this let to show the basic circuit connection, it is again back to the basics we have this DHT sensor the Vcc; the ground and the data pin are connected to their corresponding pins as defined in the previous slides this raspberry pi is connected to the network and we have already put in the client program on the raspberry pi we have already downloaded and install the Adafruit python library on this. So, we are ready to go now again back to the presentation. So, we are actually aiming to capture data from this sensor create a socket transmit a data to our remotely located server.

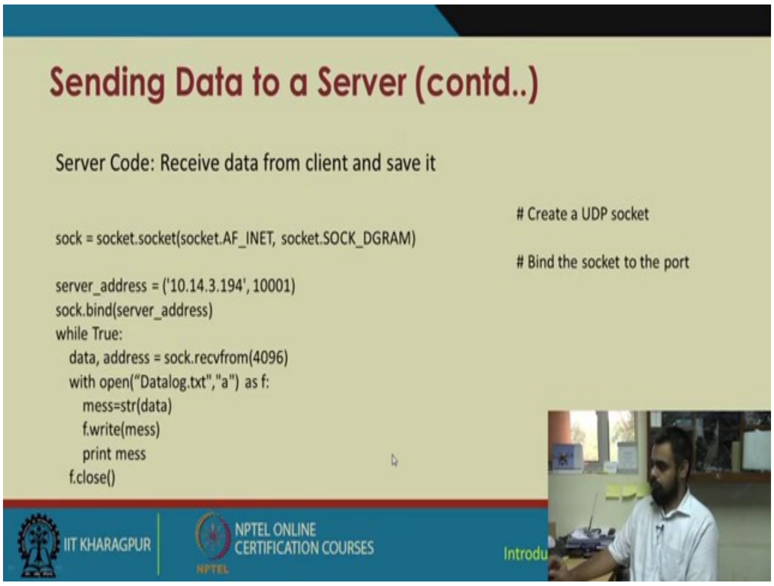
In this case my desktop will be the server and raspberry pi will be the client both of these are physically separate, but connected via a singular network to which various other devices are also connected, but since we are dealing with IP addresses and particular ports. So, we can expect zero interference from other devices. So, the client code for obtaining readings from the sensor can be given as we define a function called sensor data you can give it any other name. So, we set the board set the GPIO to board mode we set the warning to false sensor is Adafruit unless called DHT.AM2302 then we graph the humidity and temperature functions from the sensor and we return it to the calling function.

(Refer Slide Time: 12:39)



So, in this client code for creating the socket as you can see the AF_INET has been called and a socket datagram is being used for this particular program my pc has this following IP and I opened up port number 10001 if you can randomly choose ports to create a socket. So, I open port 10001 to accept connections from various clients. So, my system client will try on sending data over the network to the server. So, h, t; that means, these will be assigned the humidity and temperature data from the sensor data function which we defined in the previous slide and we formatted in the terms of a string and we transmitted over the socket to that particular server address and when this transmission is complete from input receipt from the user and the user terminates the code the sock the close function will execute.

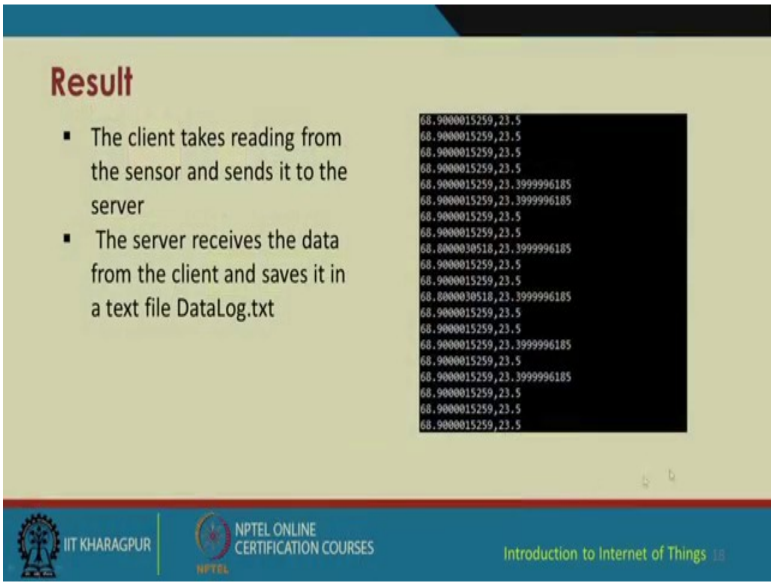
(Refer Slide Time: 13:55)



Similarly, the modification for a server side is you again create an AF_INET and sock underscore data gram socket the address will be the servers address and the port will be the port which will be use for connecting various clients to it and sock.bind it starts the server port. Now, while it is true it will keep on infinitely looping the data and address will be received from the socket and chunks of 4096 bytes you open a any text file called data log text or any other name you want to chose it may even not be a text file it may be a CSV file also.

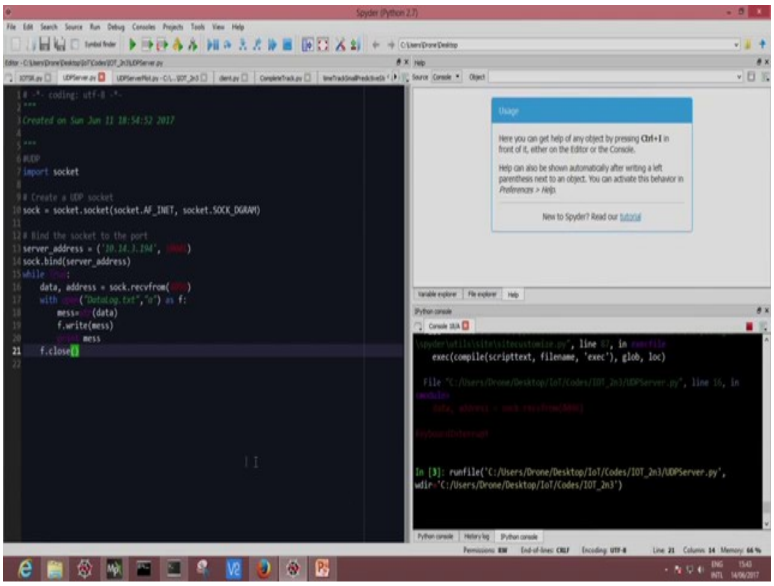
So, you use that file if you remember we covered file reading and writing in programming introduction to programming in python. So, using that similar concept you open a text file and whatever data you are receiving over the network you start writing to the text file as well as if you want you can keep one printing the data also.

(Refer Slide Time: 15:15)



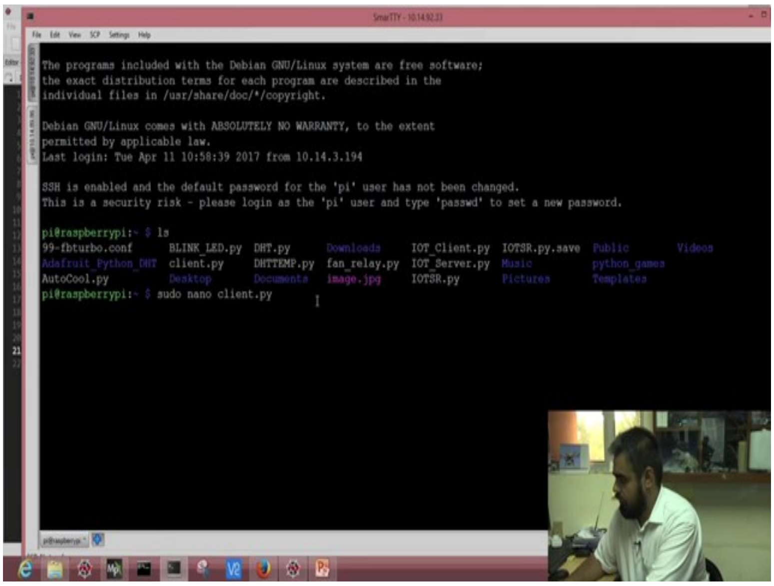
So, if you see we will get an output something like this your temperature reading first is humidity and the next one is temperature. So, separated by a comma yours client will keep on streaming this data over and over again new values not the old redundant values every time every data pole it will generate a new value . So, let us look into the sever code first.

(Refer Slide Time: 15:44)



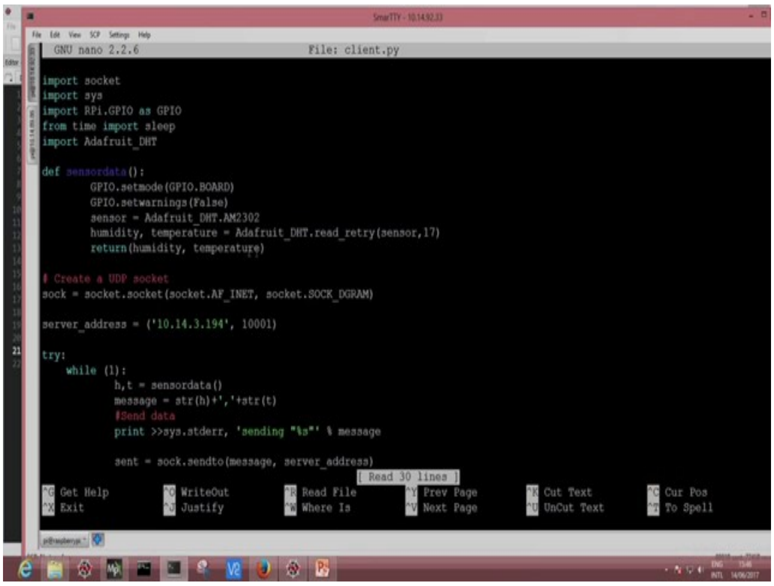
So, over here I have my UDP server. So, I have put in my IP and put in my port right data log txt for there was this file data log dot txt. I will delete it right this I have opened in append mode. So, that your data keeps on appending on to the same file again and again without overwriting the previous data. So, I start my server now as you can see the server has started it will wait for connections from the client and until then it will do nothing.

(Refer Slide Time: 16:33)



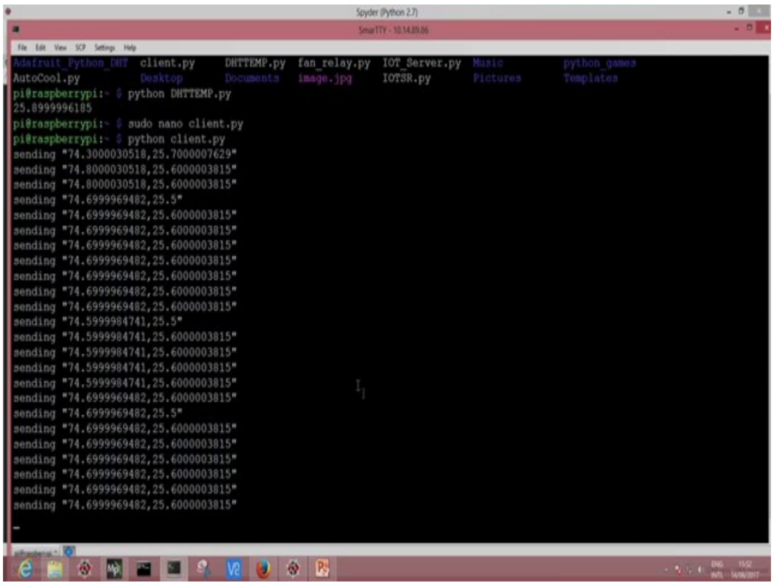
Now to access the client or the raspberry pi we remotely to this raspberry pi way system. So, we run this particular program client.py try to doing this you may just check whether our sensor is working fine or not let us try to read some temperature just like the previous lecture I will try running this DHT temp file, ok I need to change the port this system is not responding ok I will login to this raspberry pi again yes. So, this is my correct raspberry pi actually we have lots of raspberry pi is connected to over the network. So, we check; what exactly is the file content.

(Refer Slide Time: 18:45)



So, this was covered in the presentation we opened our script file in a editor. So, you are first going to check whether our temperature sensor working fine or not.

(Refer Slide Time: 19:04)

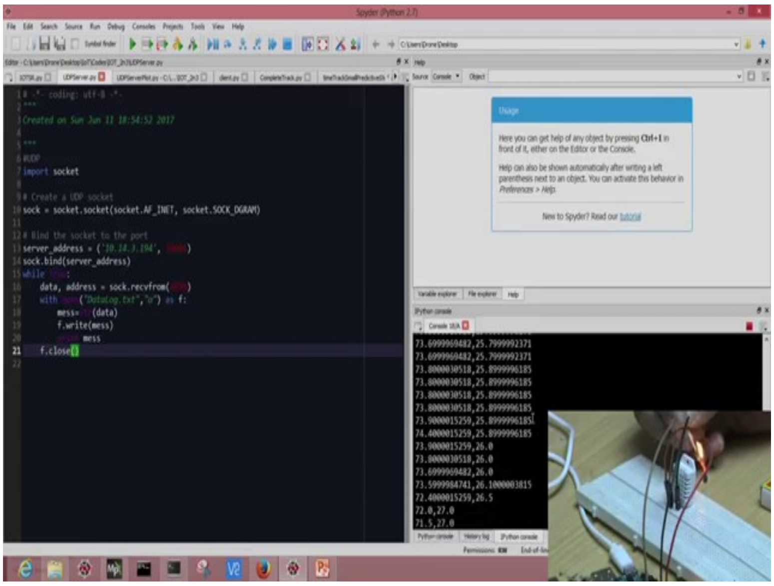


We will try running this code DHTTEMP.py I have shown in the previous lecture. So, once this is executed if the sensor has been correctly connected if the pins are correct it is suppose to return temperature value on the terminal. So, yes it appears that sensor is properly connected returns a value of 25.89 degree Celsius now we can proceed with the more complicated part we will have a look at the client program.

This is a same program which was covered in the presentation we define a function called sensor data we open up a socket aimed at this IP address which is my server or desktop for this particular port 10001 you can change the port according to your needs and you iteratively keep on pushing data to this server . So, before beginning we will check yes the server is still on it is still waiting for incoming messages from any client which will connect to it now a last made client to send data to this server. So, you see it is sending 2 values this 74.3 and 25.7. So, first one is for the humidity value and the second one is from the temperature readings.

So, this will iteratively keep on going again and again until the user terminates this program over at the server side you see the same thing is being received that humidity readings and the corresponding temperature readings. So, for a demonstration I light up a match in front of the DHT sensor and you can check the corresponding readings change over at the server.

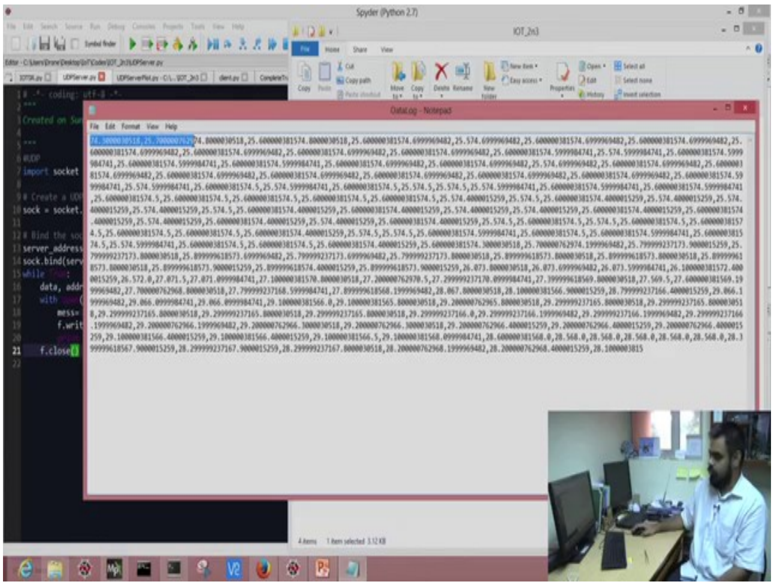
(Refer Slide Time: 22:02)



So, see the temperature is slowly increasing. So, it has reach all most 27 you can see the same variations over at the client side. Now I will terminate my client code. So, once this socket is close once I terminate this will send a message closing socket and closes down the socket you see the server code has stopped coming in right. So, whenever I start this code again my server will again start receiving this code. So, this we demonstrated using one single raspberry pi as a client and one single sensor you can; obviously, include multiple raspberry pis and multiple sensors all sending data to this particular server or a single IP at the port and another thing we will check when this data is incoming into the server initially I deleted this DataLog.txt file.

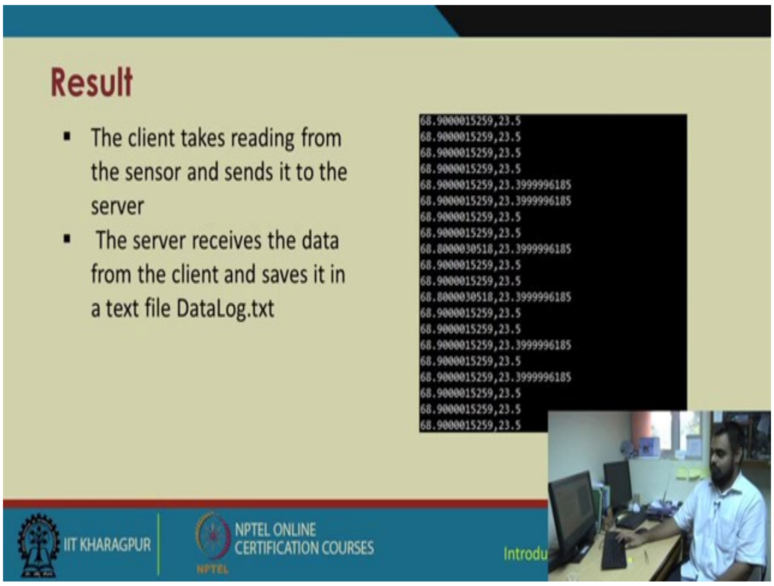
Now, you see it has automatically created another DataLog.txt and this function once I open it you see all the data has been stored.

(Refer Slide Time: 23:52)



So, this can be used as the server log or it can be extorted and use with various algorithms for higher processing.

(Refer Slide Time: 24:08)



So, I hope you gained some experience of integrating various sensors over the network and creating a client server connection and I hope this will give you a little bit touch of this IoT.

The course for which you have been attending these lectures and in the next lecture we will be focusing more on what to do with the data and what exactly can be integrated can be done you can may be plot the data you can store the data you can refine the data you are storing and other such tasks.

Thank you.

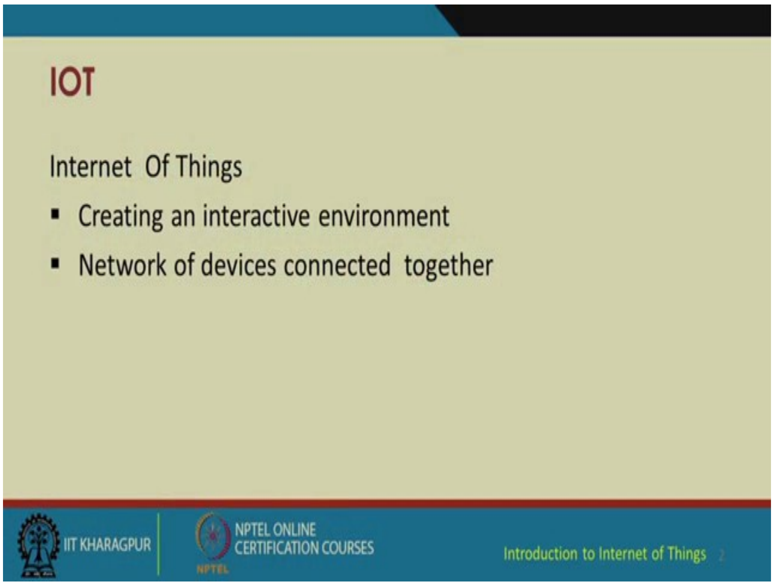
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 32
Implementation of IoT with Raspberry Pi– III

Hello in this third part of this implementation of IoT with raspberry pi. Will be covering the topics we discussed in the previous two lectures that is integration of sensor with a raspberry pi, then in the previous lecture that was integration of sensor the raspberry pi and making the raspberry pi configuring the raspberry pi as a client device, and we configure another desktop pc as a server device, and we initiate communication between this client and server and we also initiate storage of data.

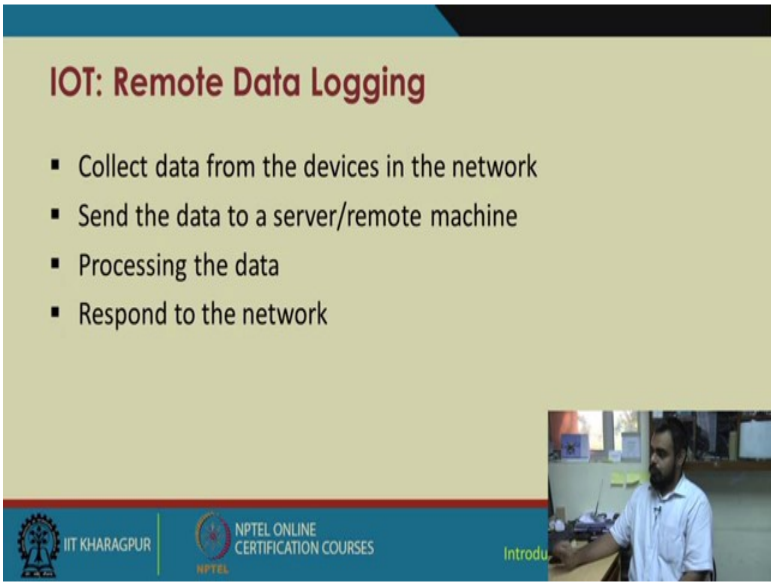
When the data is being uploaded on to the server, and thirdly in this part we will be focusing besides those previous applications will be focusing more on the server side that is once the data has arrived what exactly can be done with the data.

(Refer Slide Time: 01:18)



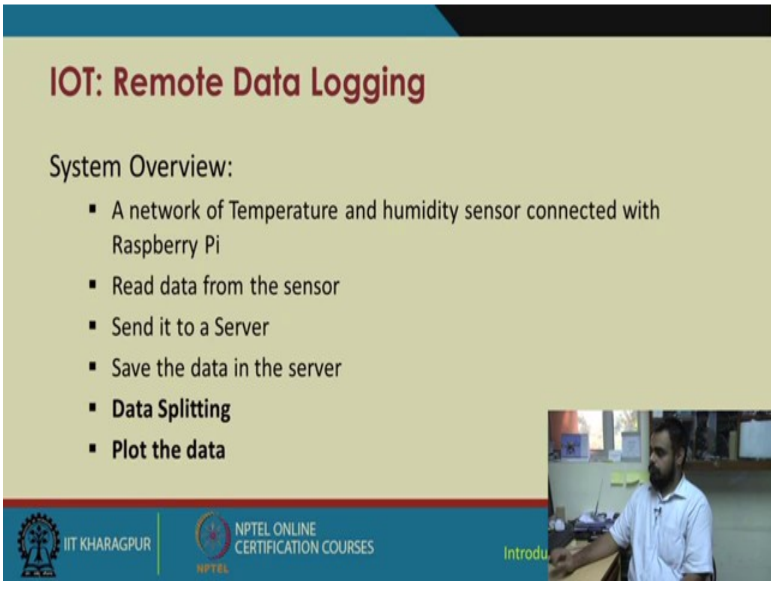
So, as we have covered previously we are mainly focusing on creating an interactive environment using a network of connected devices, and the data logging being done is remote which is connected to a network.

(Refer Slide Time: 01:25)



And the data may be processed on the client side as well as it may be processed on the server side itself.

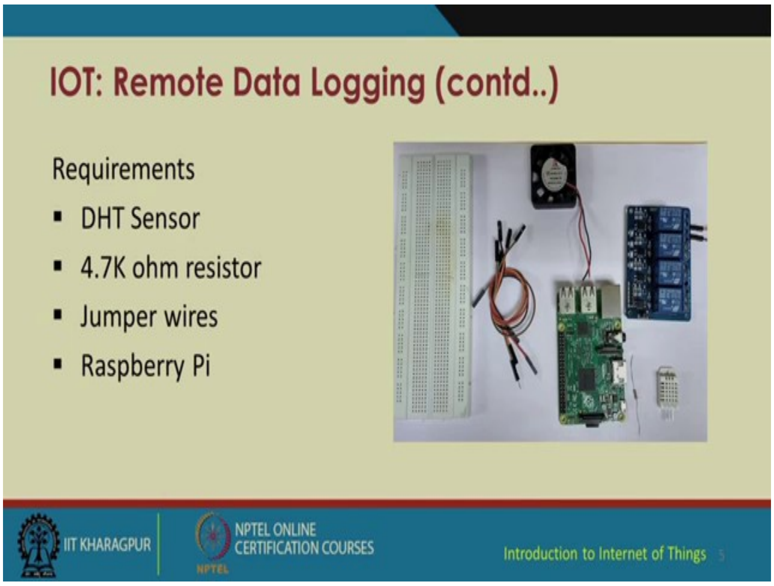
(Refer Slide Time: 01:42)



Again going through the system overview, as you can see we will first start off with a network of temperature and humidity sensors connected with raspberry pi board, for this demonstration we have connected only one sensor to a single raspberry pi we read data from that sensor we send it to a remote server over the network received the data at the server.

Then till this part we covered in our previous lectures over here we will be doing all these things, and after that we will be splitting the data which we saved in the data logs and will try to create a running plot of the data which is coming into the server.

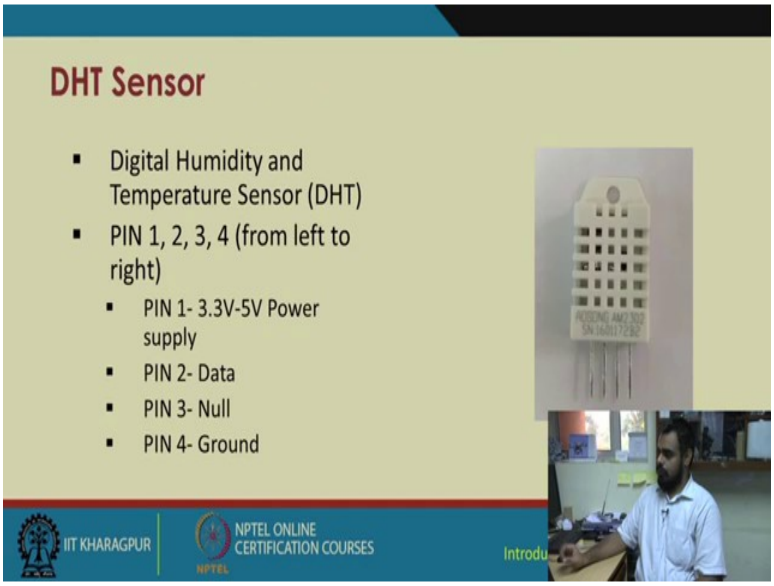
(Refer Slide Time: 02:32)



So, imagine regarding this running plot imagine your devices you have a network of devices spread over the city, and which are uploading data to a remote server and instead of running the script on a local server.

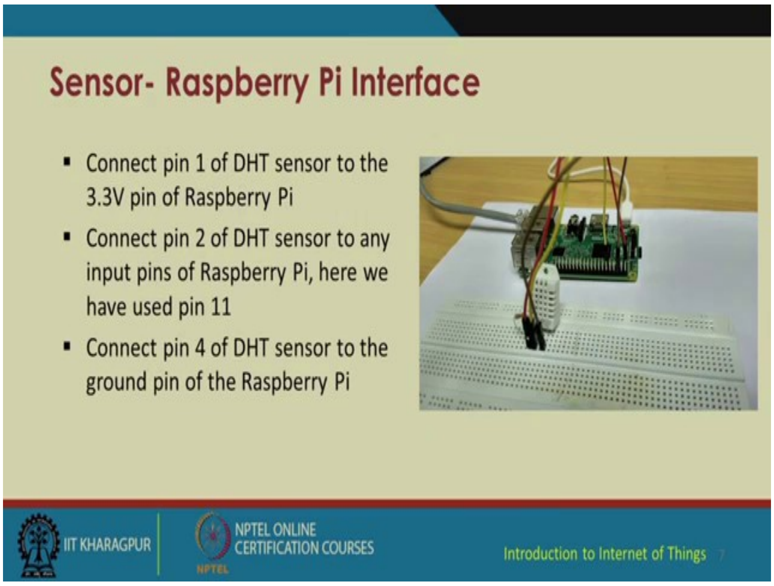
If this can be hosted on the internet, you will be able to access your sensor readings sensor data you may be able to remotely actuator sensors or actuators or IoT node from any part of the world and you may be able to visualize the changes in the environment in a particular area to which the node is deployed by accessing the whole system through the internet or through a browser.

(Refer Slide Time: 03:28)



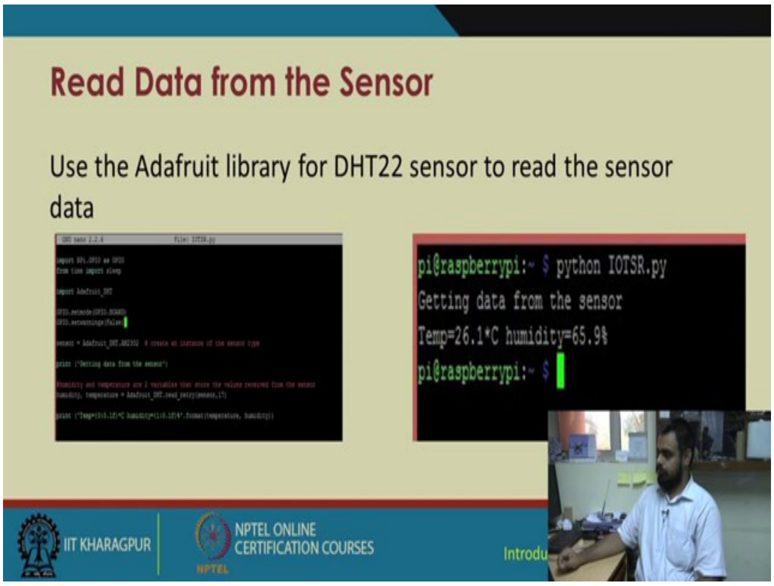
So, again back to this topic, for this remote data logging we will be using the DHT sensor and raspberry pi the pin configuration pin one is connected to power pin four to ground and pin two is connected to the data pin. The raspberry pi interface is the same as before only changes pin 2 of DHT is connected to pin 11 of the raspberry pi.

(Refer Slide Time: 03:38)



So, we already have the adafruit python library for this DHT sensor

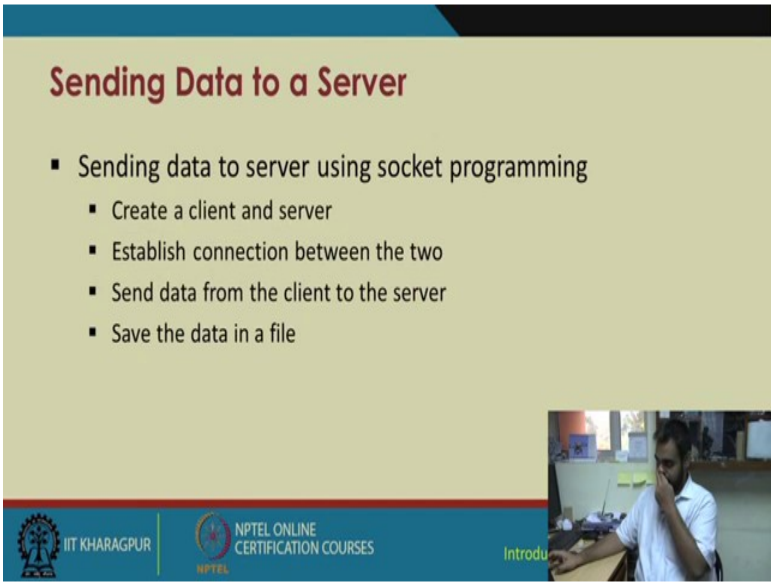
(Refer Slide Time: 03:50)



And we have all the libraries installed as covered in the previous lectures, the code is also similar to the previous lectures.

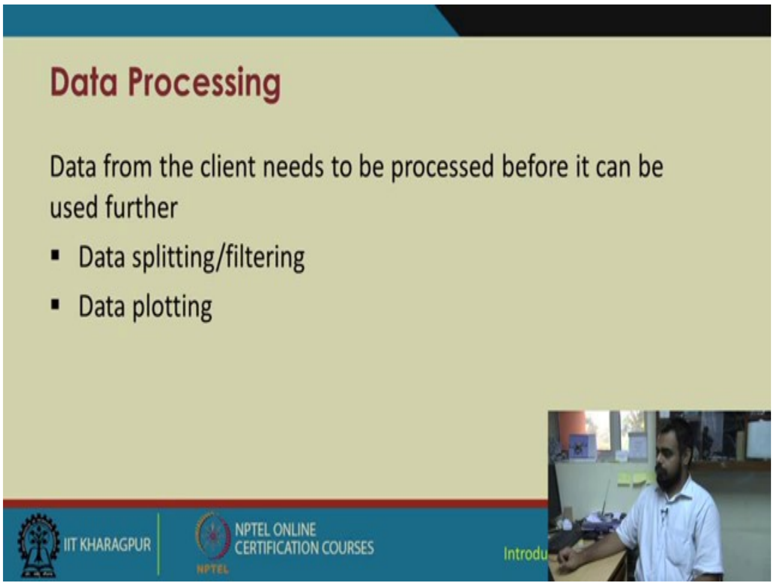
So, on the left hand side you can see this is a screenshot for that IOTSR.py file, and on the right hand side will be getting the output. Once this file is run on the raspberry pi you must remember this IOTSR.py file is kept on the raspberry pi and when you remotely run this file it will generate a temperature and humidity value. So, this will be on the client device itself sorry this will be on the sensor device itself which is the raspberry pi we cannot call it a client yet, because it has not been connected to the network as of now.

(Refer Slide Time: 04:47)



Now, when we attempt to connect this over the network, we create client server architecture and establish connection between one client device and a desktop which acts as the server device, and once the data transmission from the client initiates successive data will be in coming into the server and get stored into a log file.

(Refer Slide Time: 05:16)



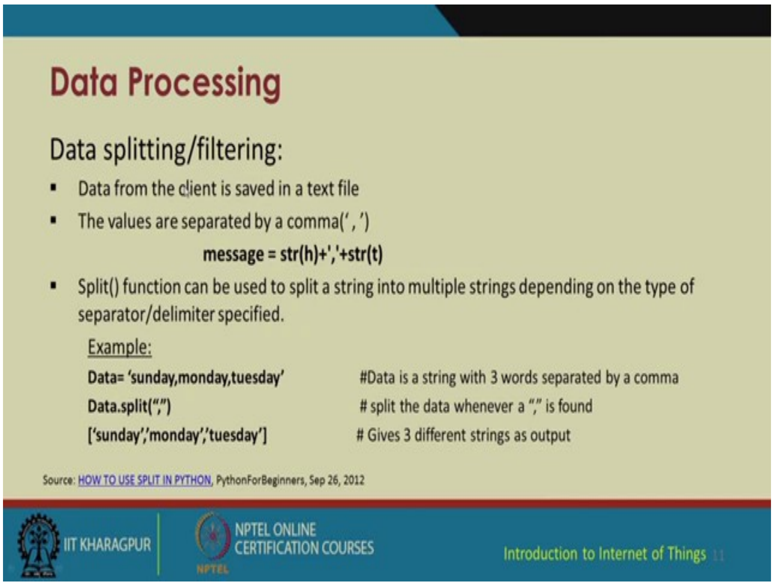
Now till the previous slide we had covered all these things in details in lecture 2.

So, over here will be going through those as well as a basics of data processing like data splitting and filtering and data plotting, but big question is why do you need processing of the data. As in imagine you have hundreds and hundreds of sensors all rapidly uploading their data to this remote server. So, at certain instances there maybe chances of data corruption, there may be chances of incomplete data being transmitted, there may be chances of server not able to receive the whole data despite the client being sent client sending the whole data.

So, there may be various reasons that data may not be properly formatted and so on. So, in those cases you need to filter the data to create a seamless and well structured data base and as regards to data splitting since you have multiple data coming in from a client which may be stored in the form of a csv file or even in the form of a text file. So, we need to if we need to access individual data.

Suppose you are getting temperature readings humidity maybe presence of gases light intensity and so on So, suppose you have five to six sensors connected to a single node, and these data are routinely updated to a server, but you only need to access the temperature value for this to happen you need to split your data at the data log. And once this data has been split and individual data can be accessed we can go about plotting this data.

(Refer Slide Time: 07:16)



Regarding this data splitting, now imagine the data from the client is saved into a text file and the values are separated by a comma as we have covered in previous lectures this is called a csv or comma separated value file. So, instead of a comma you can use any other delimiter, it may be a semicolon, it maybe colon, it maybe even a question mark better avoided, but still. So, these values which were incoming it were in the form of string h, string t.

So, we need to split these values on the server in the form of individual h and t's. So, we will be using this basic inbuilt function of python called split. So, it can be used to split a string into multiple strings depending on the separator or the delimiter we are specifying. For example, suppose we take a data string as within single quotes we assign Sunday, Monday, Tuesday or it can be any other data string separated by a delimiter over here the delimiter is this comma we have chosen this is a comma.

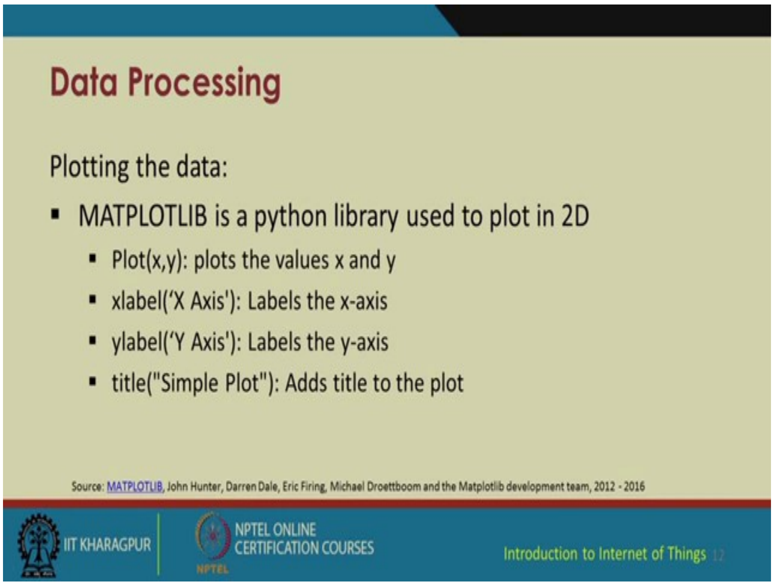
Now, when we call this Data.split function and we specify the delimiter in the arguments, you will see the result will be individual substrings Sunday, Monday Tuesday. We input the data as a single string Sunday, Monday, Tuesday, but we get the output as individual data strings. So, it would be better if we just do a bit of hands on. So, let us suppose our data is maybe 123, abc right.

So, I have given one 123 numeric value I have given abc alphabetical value and I have given a combination of both alphabets and numbers. So, this is my data let us check what has been stored. So, this has been stored this data variable has been assigned a single string that is 123, abc, xyz12 now I need to split this data. So, I use data dot split the separator I have used is a comma.

You see it has been split into three different parts 123, abc and xyz12 you must remember since these were separated by comma. So, these have been separated accordingly, you can obviously, go for another value let us say data equal to 123432454abc44. So, I have used to many 4's let us see what happens. So, this is my data right.

Now, I will use the number 4 as my delimiter. So, data.split I will give the delimiter as 4 you see. So, according to the position of four in the string your single string has been broken down into multiple substrings and the 4 delimiter is obviously, not included. So, you have 123 then you have 32 then you have 5 then abc then a blank since it has two 4's. So, it includes a blank and then rt right. So, it is quite simple.

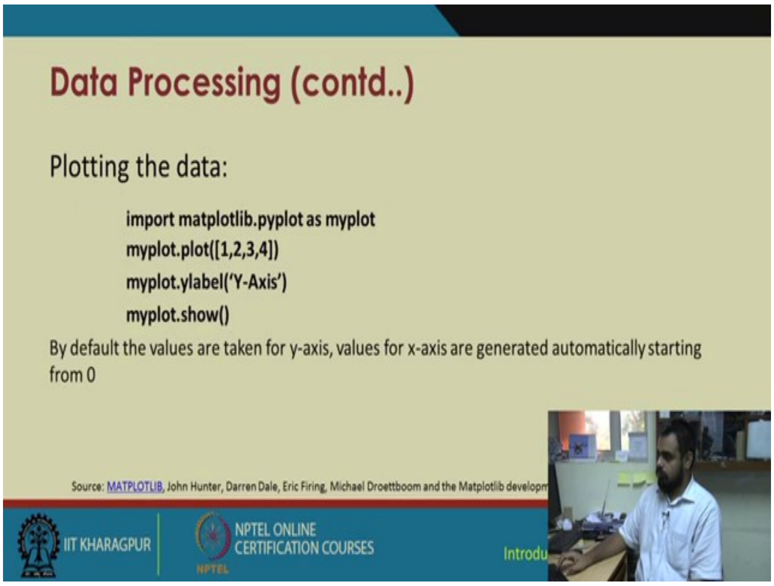
(Refer Slide Time: 11:38)



Now regarding data plotting in MATLAB, so MATLAB sorry regarding data plotting in python it is quite similar to plotting the data in MATLAB so, both of this support a very powerful library called MATPLOTLIB. So, this MATPLOTLIB library you can use the appropriate version in MATLAB as well as in python most of the functions are almost same with a bit of variations, but it is more or less same in both the languages.

So, basic commands for plotting in two dimension are you write Plot(x, y), where you put the x axis and the y axis values, x label gives provides the labels on the plot for the x axis y label provides the label on the plot for the y axis title gives title to the whole plot.

(Refer Slide Time: 12:37)



So, this is a sample code import matplotlib.pyplot as maybe a variable and then you call this myplot.plot you give a range of values then myplot.y label you name it y axis and you show this plot. So, we can again go for a bit of hands on let us say we import this MATPLOTLIB function as let us say plt, we define a variable as maybe I will give a range of values may be from one to twenty.

plt.plot I put in 'a' plt.show(). So, when I run this basic code see what I have done is I have imported this MATPLOTLIB.pyplot library, I have defined a variable 'a' by assigning a range of values between 1 and 20. So, this range function automatically assigns values let us see what it does, range 1, 20. So, it will give you range of values between 1 to 20.

Now, we initialize this plotting by calling a figure, within this figure we plot this value of a which will be; obviously, corresponding to the y axis, the x axis is if not provided it is automatically taken and the show function shows the plot. So, once we run this thing as you can see this plot has been generated.

Since it is a linearly increasing line 1, 2, 3, 4 upto 19. So, I will give you a straight line you can even change the plot type, let us say instead of plt.plot a straight line plot. Let us go for a scatter plot sorry better still it will be more interesting if we give two values assign a variable a1 as for this we have to import this random function.

If you see if you remember in one of the previous lectures this random function was also covered we need to import the random function first sorry starting and ending. So, whenever you are in doubt for this particular spyder base console even actually checking the syntax of this function or you need two arguments a and b.

Let us say I give a as 1 b as 20 and put this whole thing within range. So, this will be my range I will start with this I will change this to length of a1 if it is denoted by len(a1) when I run these two together. So, a1 is 0 to 5 a is 6 right sorry this is going to be only scatter. So, this seems to be a size mismatch

So, for this scatter plot we take two arguments one for x another for y and we have used two function for the x1 we need a linear spacing of numbers. So, we started off with -1 because this would not be included, it will go up to 50 with a step size of one. So, you will have 0, 1, 2, 3, 4, 5, 6 upto 50, so you have 50 points on the x axis where as we call a random function from numpy library module let us call it import numpy as np.

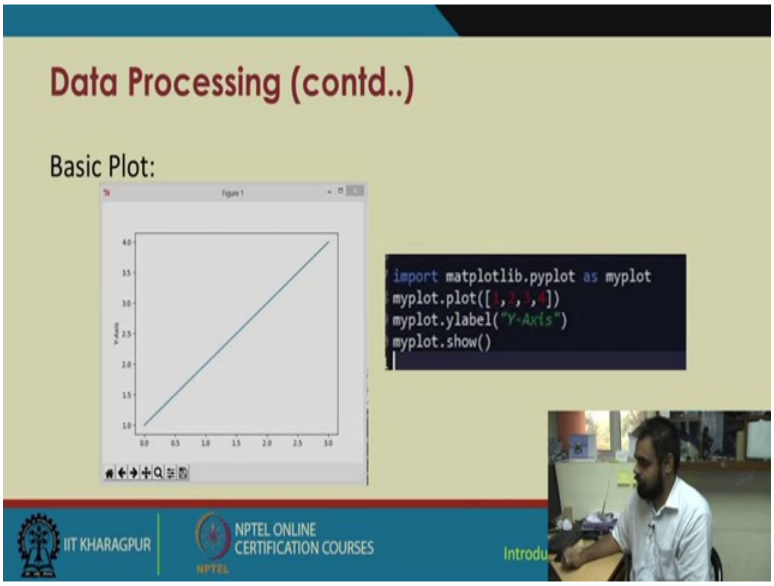
So, on this numpy module we would not be requiring this. So, np dot random dot random number within argument 50 means it will generate 50 random point. So, this will act as my y axis or the data points. So, corresponding to the points on the x axis will have corresponding randomly generated points on the y axis and within this same figure and show let us see what happens when we run this thing.

So, you see on the x axis and corresponding to the x axis you have 50 points on the y axis. So, let us add a few bits to it, if you run this part you just added a title for this plot you see this scatter plot example additionally you can have plt.y label you must remember these labels are strings. So, should be within quotations.

Let us put the y label as randomly generated, the x label as linearly spaced let us run this you see the y label has changed to randomly generated the x label has changed to linearly spaced you just add one more command to it. If you add this command it will show a it will turn up a grid on your plot. So, you have a linear grid on your plot.

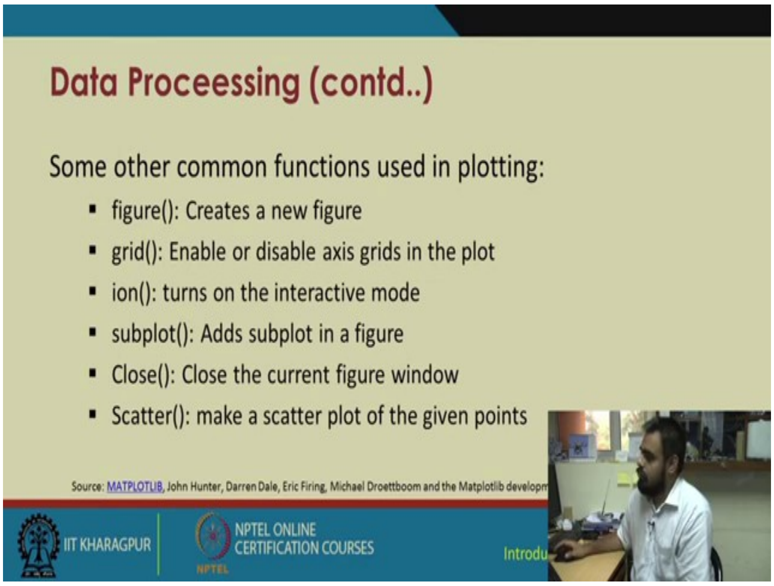
So, I hope this basic plotting function is clear. So, you have a simple plotting you have labeling you show this plot and besides your normal 2d plot line plot and scatter plot, you have a huge range of plotting option you can even venture into 3d plots which are much more attractive in a browser base system or for various publication. So, this basic plotting you saw previously.

(Refer Slide Time: 23:04)



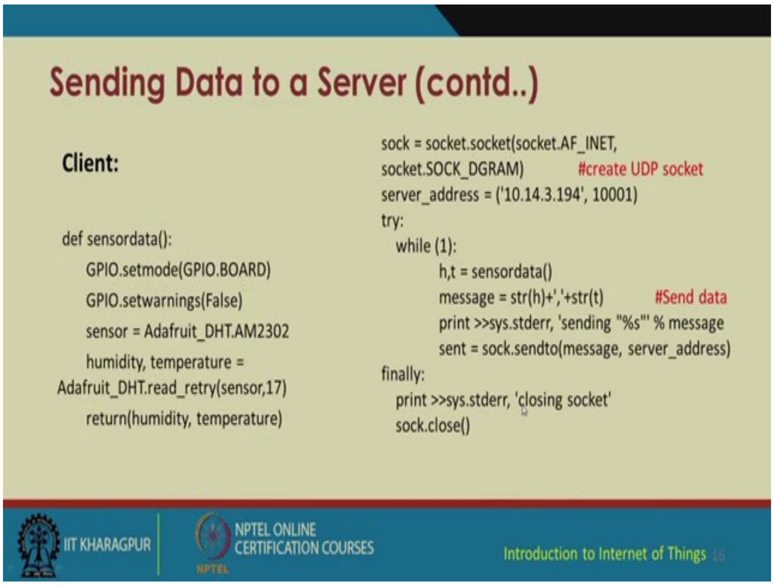
Now, some other functions used in plotting are covered this figure it creates a new figure grid it enabled or disabled an access grid on the plot ion is the interactive plot mode.

(Refer Slide Time: 23:12)



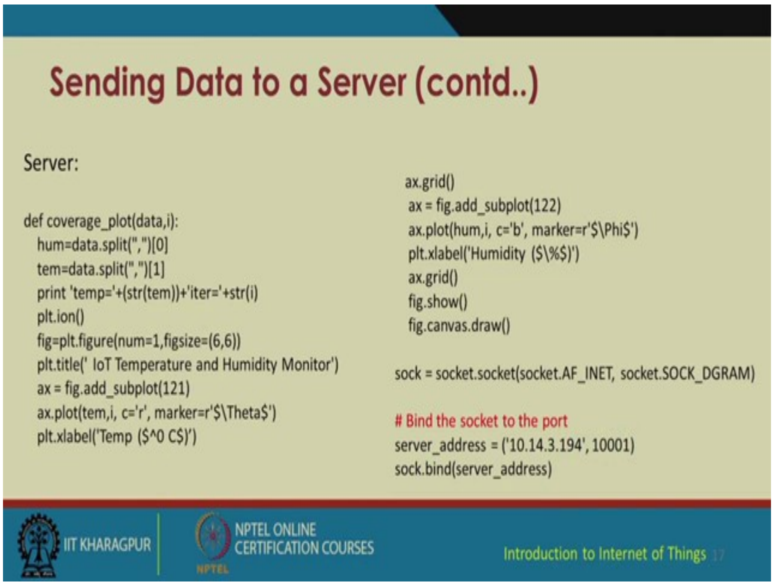
This is generally used for animations your subplot it adds a subplot in the figure close it closes the current figure scatter makes a scatter point plot of the given points, so will try this small. So, it would be better if we directly go into this model again.

(Refer Slide Time: 23:52)



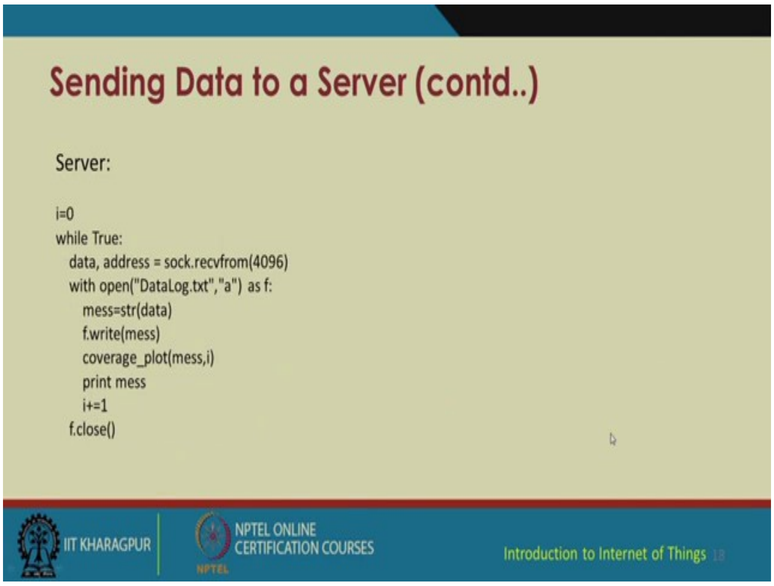
So, if you remember for the client side this sensor data module is more or less same. In fact, it is the exact same one, the client does not require a IP address because we are aiming for a one way communication from the client to the server. So, we just put in the servers IP address and that required port to which on which the server is listening and just like before we are packaging the data in the form of h and t, and transmitting it over the socket to the server.

(Refer Slide Time: 24:32)



Now, on the server side we have added a new function called coverage plot. What it does is it animatedly plots whatever data is in coming into the server over the socket. So, for the time being ignore this part this particular function, let us pay attention to this socket creation. So, it is somewhat similar to the previous examples over here your server address is the server address and the particular port to which the server is listening.

(Refer Slide Time: 25:09)



And while it is true it is receiving data in 4096 bytes junks you open a data log file store the data to it and additionally call this plotting function.

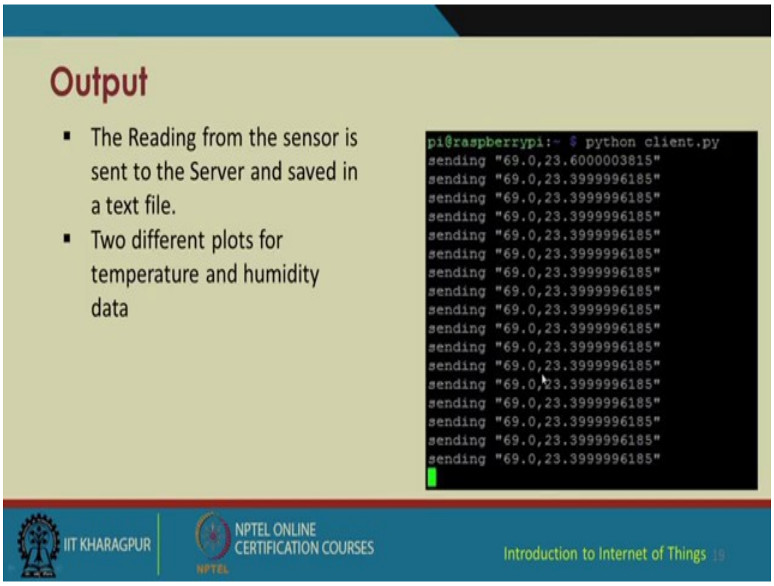
So, this plotting function is being called again and again basically iteratively within this loop. So, as long as your data is incoming this plotting function will keep on going. So, once the server is closed by the user or the client is closed by the user this plotting function will stop. So, and this I plus one this keeps on incrementing this normal counter which we sent to the coverage plot.

Coming back to the coverage plot it accept two arguments one is the data which comes from the server, and I which is the counter now the data is being split in terms of two parts humidity and temperature. So, after splitting since the data was in a csv format. So, after splitting the zeroth element becomes humidity and the first element is temperature. So, you need to actually study the data very carefully like what format the client is sending a data and so on.

Now, if you want to print the temperature, you just print the temperature and the iteration number then you start the interactive plot mode you set the figure two similar number as number 1, otherwise it will keep on creating new windows every time it plots something new to set the window to 6 comma 6 it can be 8 comma 8. It is up to the user actually you give the plot a title, you add a subplot to it and just basic you plot the temperature versus the iteration that is normal temperature plot with respect to whatever data is incoming we label it.

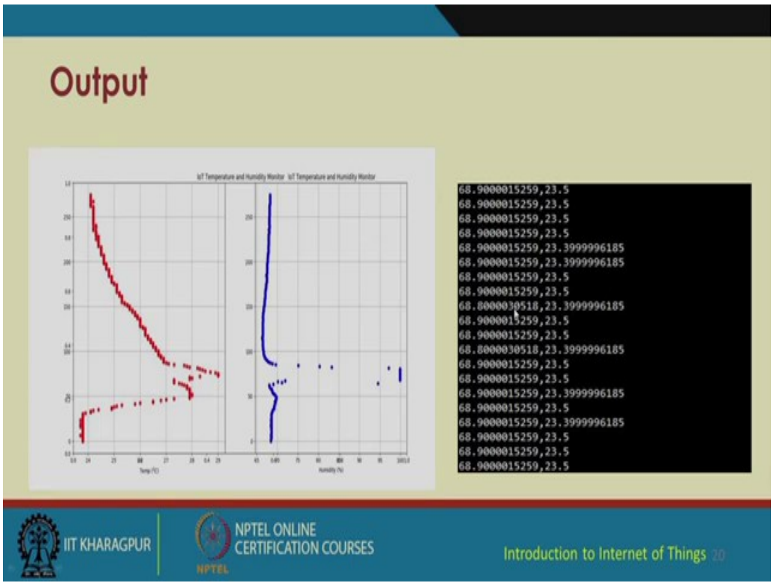
Similarly, for the humidity part also you iteratively plot the data against i, and eventually show the data and figure.canvas.draw it redraws the image without overwriting the previous points.

(Refer Slide Time: 27:36)



So, your output will be something like this. So, this will be on the raspberry pi this is the client code.

(Refer Slide Time: 27:47)



And on the server side you will be getting your data as your covered in the last lecture, and for the plot you will be getting something like this, left one side is the temperature plot the right one side is the humidity plot.

So, let us look at the plots, first of all I will start my server. So, this desktop I am operating acts as my server. So, I will open up my server. So, my server code is now running, now login to the remote client and I need to run the client code which is the same as the previous one. So, one more point you need to notices is suppose you have 100 clients, you do not need to update each and every client.

Even if you need some minor adjustments make some minor adjustments. So, you can just update a singular source code or a singular script file on the server end and that will save you a lot of time as well as a lot of effort. So, I will run this client code client.py . So, you see client has started sending the data and on the server side it is receiving the data this is a new addition this iteration number.

So, this keeps on increasing the left hand side denotes the temperature on the plot, the right hand side denotes the humidity, it is maybe will stop the plot run this thing again. So, see even after stopping this program data which was previously stored maintains there. So, there is very minute variation between 75.5 and 76.

(Refer Slide Time: 30:48)

So, it is giving changes where as the temperature is more or less constant. So, will try increasing the temperature little bit and you can see the plot changing. As you can see the temperature points now logged are raising see the temperature has risen and there have been changes in the humidity also, now let us wait for it to recover. Now you can again notice the temperatures gradually coming down on the left plot the red plot you can see the temperature gradually coming down in steps.

So, this will keep on coming down until it reaches the normal room temperature value. So, now, let us close the client program see the client program has been stopped manually and this data logging stops. So, one more thing you notice is in the previous examples your temperature humidity values were coming in concurrently, now in this one since we have spitted the data over here in these parts. So, we have a separate temperature component and iteration number and a separate humidity component which is saved in the same data log, data log is still the same only the scripting part is changed.

So, this thing will help save you a lot of effort you do not need to individually code the clients. So, once your client has been coded and deployed on the field if you need to make changes make design your architecture in such a way that only changing the server will help you only changing the scripts on the server will help you change your whole implementation and functionality. So, I hope this was of some values to you.

Thank you.

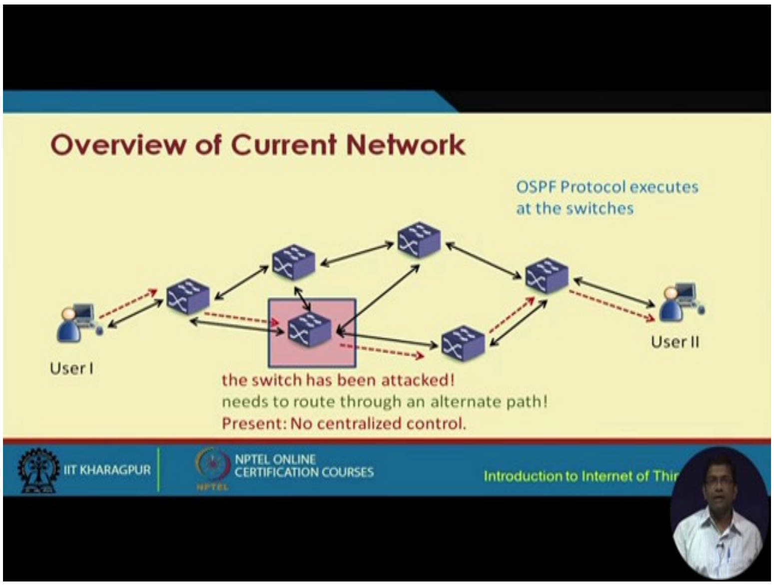
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 33
Software – Defined Networking – Part – I

We are going to discuss a very important technology the software defined networking in short it is called as SDN and it is a very important technology which has lot of potential for use in internet of things for making IoT efficient. So, we will discuss about the basics of SDN first what software defined networking is and some of the basic concepts that surrounds SDN and thereafter in another lecture we are going to discuss about how SDN can be used for in the context of IoT to make IoT efficient.

So, when we talk about SDN it is about transforming or restructuring the existing network infrastructure and that can be done in an efficient manner. So, how that can be done is what we are going to discuss now.

(Refer Slide Time: 01:22)



So, if we look at the current day networks this is what happens. So, we have users different users connected to the network enjoying network services and this can be any network you know we are talking about SDN in a general network a wired network let us say a very simplified wired network.

Now, let us say that the topology of the network is something like this. So, this is the topology of the network. So, what we have are different L3 switches like this and maybe the data has to be sent from user 1 to user 2 and back. So, the data can be sent in different ways different you know. So, these are the routes through which the data can traverse from the user the data can traverse maybe one of the possible routes is like this to the user 2.

Another possible route is may be like this and another possibility is like this and there are few other possibilities also for the data to be sent from user one to user 2. So, we have multiple different routes and the data or the packet basically traverses through multiple switches L3 switches and this is how it looks like. So, before I proceed further I would like to mention that in this particular lecture and let; that means, lecture on SDN and SDN IoT.

I am going to use the terms switch and router interchangeably. So, when I mention about switch and basically talking about the L3 or the layer 3 switch and. So, L3 switch and router these terms are going to be used interchangeably in the SDN lecture. So, let me just you know let us look at the slide once again. So, what we have is a scenario like this and then let us say for switching or routing the protocol that is used is the OSPF protocol.

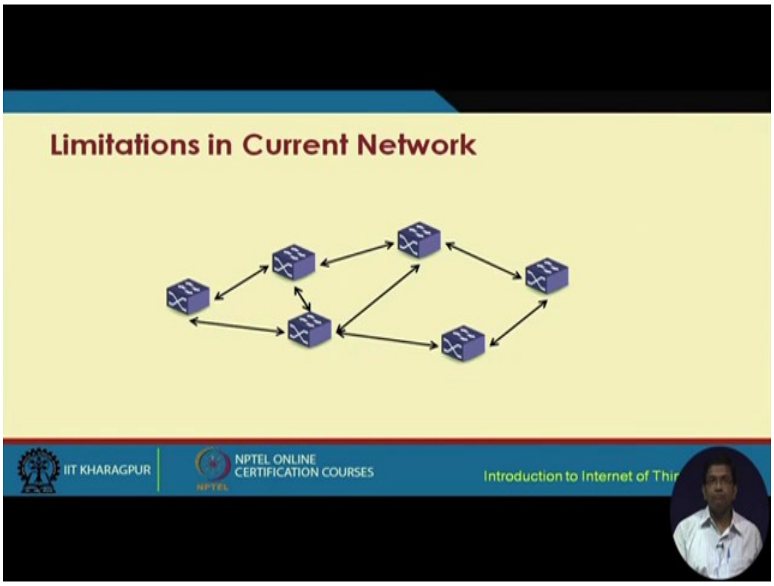
So, what essential happens is every switch is going to every switch over here it is going to implement OSPF. So, it executes OSPF and so when the data is sent you know the OSPF PF protocol is going to the packet is sent the OSPF protocol is going to route the packet through these corresponding switches depending on which route the OSPF protocol finds to be the best.

So, what essentially happens is every switch basically knows how it has to send the packet based on the routing table that it has. So, it does not have a global view of the network as a whole now let us say that a particular switch the one that is shown in this particular figure this one let us say that it becomes down for one reason or another maybe because it has been attacked. So, let us say that it has been attacked and the switch is down.

So, then traditionally what has to happen is a new route or an alternate route has to be found for the packets to be sent from the source to the destination node and because there is no centralized control. So, you know this becomes a difficult task. So, what happens is at present the technology the routing technology is such that there is no centralized control over the network.

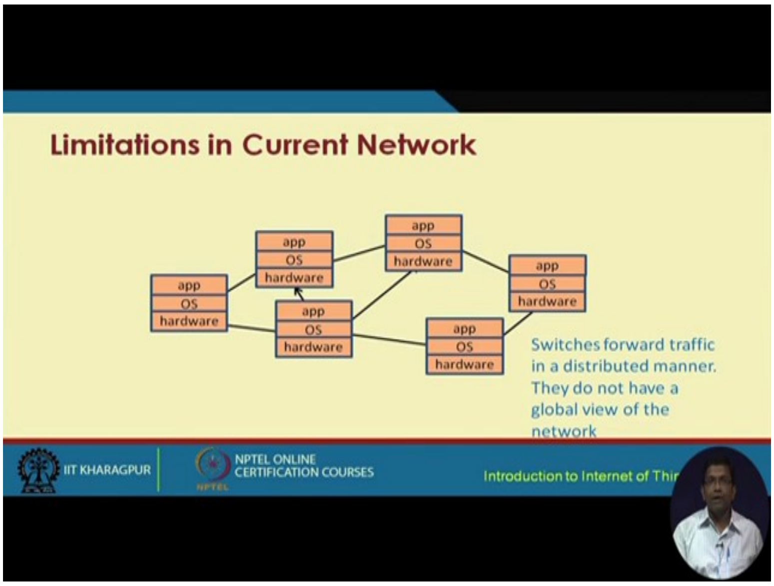
So, if one switch becomes down the other switches can; will become affected and there is no centralized way that we can address this particular problem. So, there are different ways to read out you know found find routes depending on the protocols you know what are the alternate route. So, on, but there is no centralized solution there is no centralized entity that can take care of it.

(Refer Slide Time: 05:53)



So, these are the limitations of the existing network and if we look at this network you know. So, what we see over here is just a snapshot of a very simple network consisting of different switches.

(Refer Slide Time: 06:13)

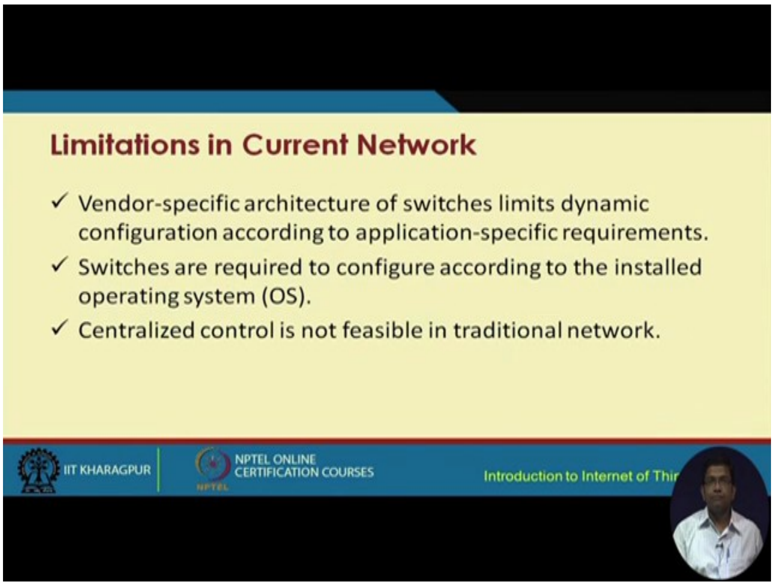


And each of these switches they run these different layers we have a hardware then we have the operating system and we have the applications that are running on top.

So, essentially a very skeletal view of the stack that is run on each of these switches is hardware OS and app and that is basically applicable to all these switches that are there in the network. So, each of these switches is running these 3 different layers. Now these switches they forward the traffic in a distributed manner and they do not have the global view of the network this is what I was mentioning in the previous slide as well.

So, each of these switches they do not have the global view they route the traffic they forward the traffic in a distributed fashion they just know locally what you know what has to be done.

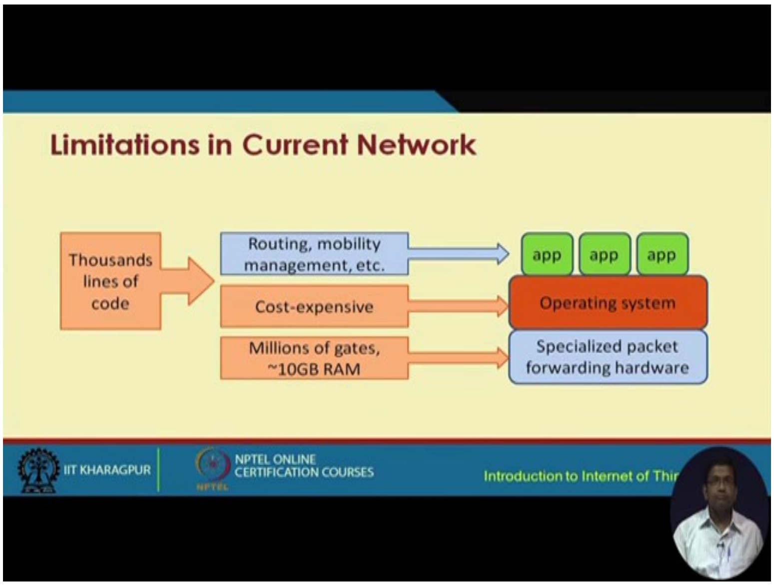
(Refer Slide Time: 07:08)



So, if we now summarize the present network has different limitations; limitations which are for example, the architecture of these switches are vendor specific and correspondingly you know if we have to do any dynamic configuration based on the application specific requirements that we cannot do very easily. So, that cannot be done in a dynamic way dynamic configuration cannot be done.

Switches are required to configure according to the installed operating system in each of these stacks. So, each of these switches they run their different operating system and they have to be this way they have to be configured according to that particular operating system and there is no centralized control that is feasible in these networks there is no centralize controller.

(Refer Slide Time: 08:03)

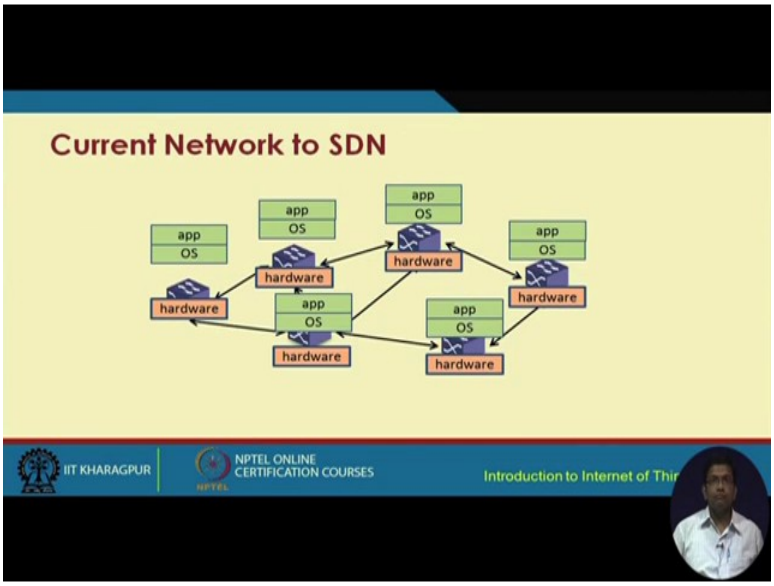


So, if we look at another view point of these current networks. So, we have each of these switches running thousands of lines of code they have each switch has millions of gates logic gates that are implemented requiring more than 10 GB of ram they are cost expensive each switch is cost expensive and they run different you know applications for example, routing, mobility, management, etcetera.

So, here basically you know. So, we are not talking about you know when we mention about applications we are talking about the different application functionality and not simply the applications that we used to refer to in a OSI model. So, here we are talking about applications in general. So, like the general network applications like routing, mobility, management, etcetera.

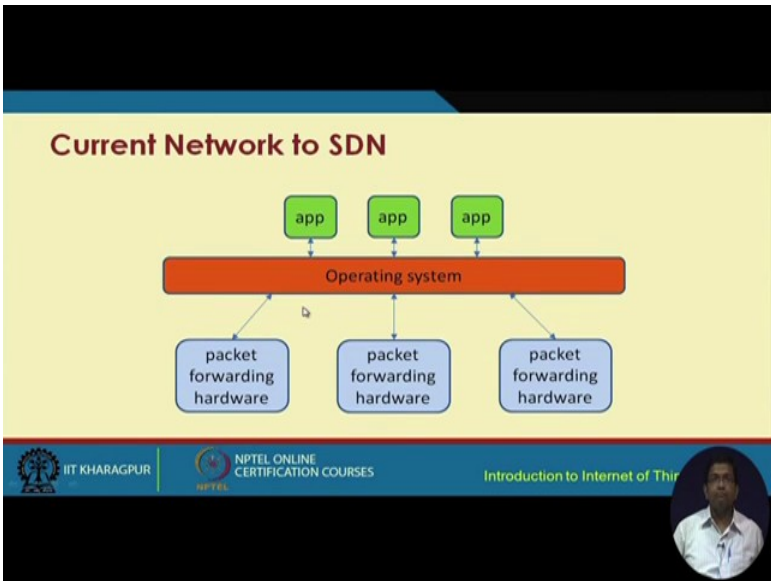
So, this is the challenge with these networks. So, each of these you know networks you know these each of these switches in this networks the have specialized packet forwarding hardware they have their own operating system and they run their own different applications with respect to routing mobility management and so on and so forth.

(Refer Slide Time: 09:21)



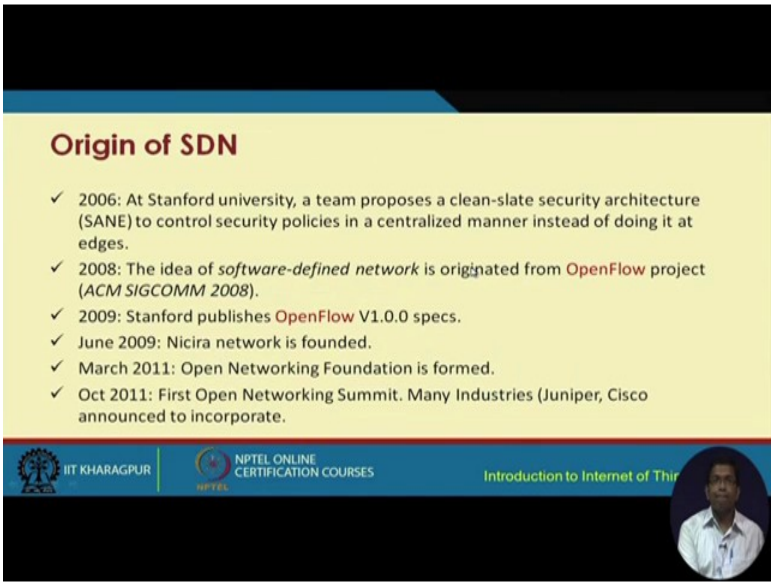
Now, what is required is to make these networks efficient by trying to overcome these challenges or the limitations that we have just gone through. So, the whole idea in SDN is to take care of the limitations by separating the application and operating system from the hardware. So, earlier in the earlier view what we had seen is the app OS and hardware were hold or were all put together in each of these switches and here what we are doing is we are separating the application and operating system from the hardware in each of these switches. So, hardware is separated out from the app and the OS.

(Refer Slide Time: 10:10)



So, what we will have is the packet forwarding is going to be packet forwarding is going to be separated out from the OS and applications.

(Refer Slide Time: 10:23)

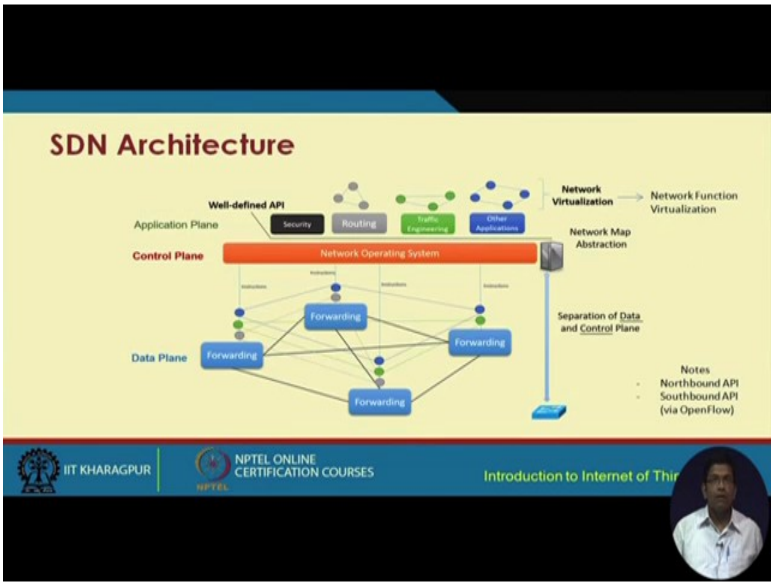


So, before we look any further into SDN. So, let us try to look at the history the brief history about the genesis of SDN. So, in the year 2006 a Stanford University team proposed a clean slate security architecture which was termed as SANE to control the security policies in a centralized manner instead of doing it at each of these edges; that means each of these switches.

In 2008 the idea of software defined network was originated with the open flow project and that was published in the very popular ACM SIGCOMM paper in 2008; in 2009 Stanford basically published the open flow version one specifications and June 2009; the Nicira network company was founded in March 2011 the open network foundation was formed and in October 2011 the first open networking summit and many industries for example, all these routing router companies like Juniper, Cisco etcetera they basically announced that they want to incorporate SDN into their switches.

So, basically it the whole concept of the SDN technology goes back to only a few years back; that means, in 2006. So, it is not a very old thing it is very new and we will see that how what are the different features of SDN further in the next few slides we are going to look at what are the different features of SDN open flow is sort of like a de facto protocol or and architecture that is used for SDN. So, both of these are not the same, but open flow basically follows you know open flow is used for SDN.

(Refer Slide Time: 12:16)



So, let us now look at this particular architecture. So, what we have you know let us say that each we have different switches which perform forwarding individually. So, that is the data plane and then we have the control plane which has the network operating system and then the application plane performing functionalities like security, routing, traffic engineering and different other applications.

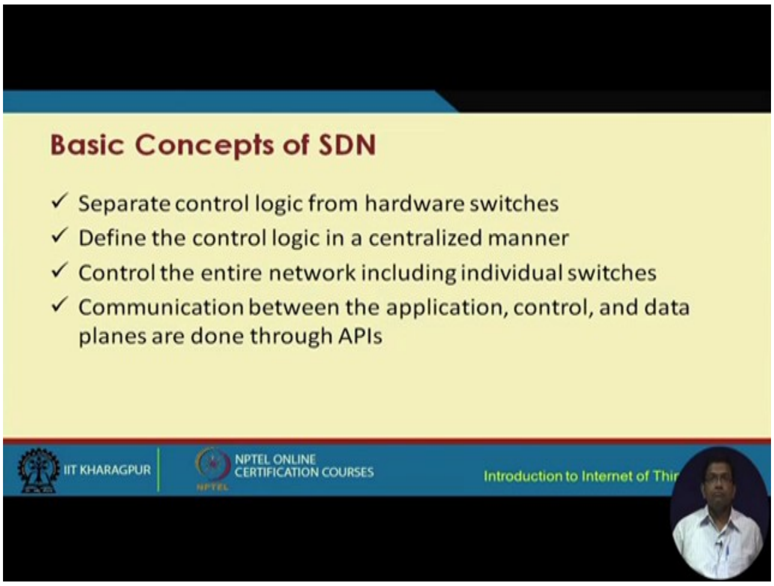
So, the whole idea behind SDN and this SDN architecture as a whole is to separate the data plane from the control plane or rather the control plane from the data plane. So, you see that the control plane has been separated in SDN this control plane has been separated in SDN from this data plane which takes care of things like forwarding. So, this is made possible they the concept of SDN is made possible through the process of network function virtualization NFV.

So, this network function virtualization. So, what happens if these different network functions for examples you know security, routing, etcetera, etcetera, these have been these have been you know these are performed on a virtualized networks. So, this network function virtualization basically gives a logical view of the network and based on that these functions are performed.

So, one more concept I should mention over here before we proceed further is. So, we have 3 different planes in SDN in the you know in the SDN architecture we have the data plane, control plane and application plane and we have also seen that the data plane and the control plane are basically decoupled in SDN.

Now, we have the concept of northbound API and southbound API. So, the northbound API is between the control plane and the application plane. So, this particular interface is known as the northbound API in SDN and this particular interface between this forwarding; that means the data plane and the control plane this is known as the southbound API and the current protocol supporting this southbound API is the open flow protocol.

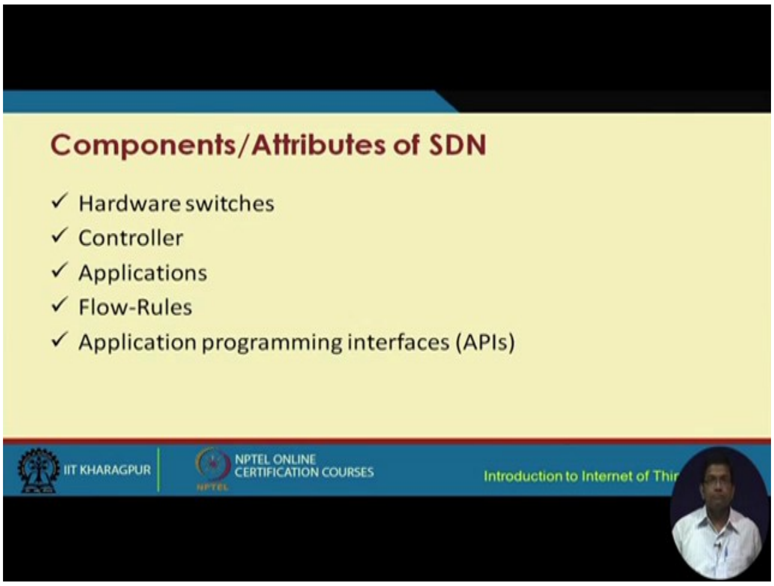
(Refer Slide Time: 14:45)



So, now let us summarize some of these basic concepts of SDN the whole idea is to separate the control logic from the hardware switches to define the control logic in a centralized manner. So, the everyday all this control functions are going to be centralized because this control plane has been separated out and is centralized. So, you know. So, this is how this SDN is going to work. So, the control logic is going to be centralized and is separated from the data logic, the data plane.

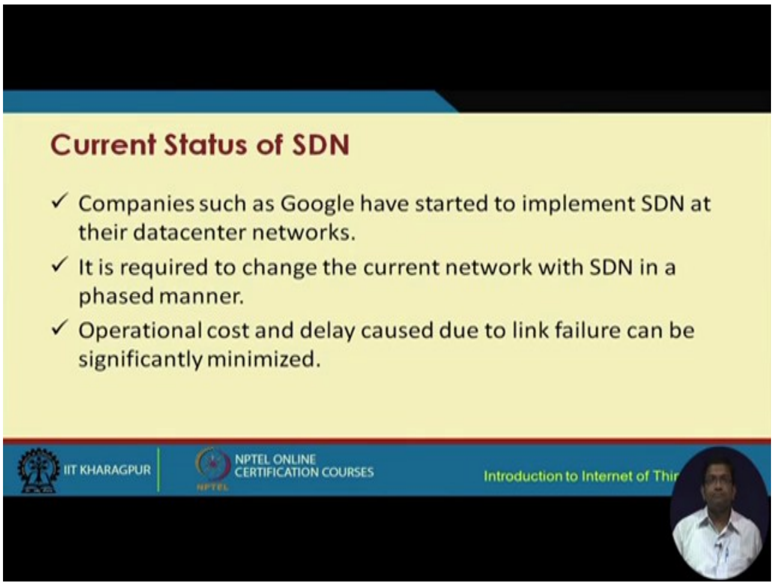
Control in the other concept of SDN is to control the inter network including the individual switches in a centralized manner and the communication between the application the control and the data planes are done through different APIs northbound APIs southbound API.

(Refer Slide Time: 15:38)



So, we have different components or attributes of SDN we have hardware switches we have controller applications flow rules and different application programming interfaces or the API these are the different components of SDN.

(Refer Slide Time: 15:59)



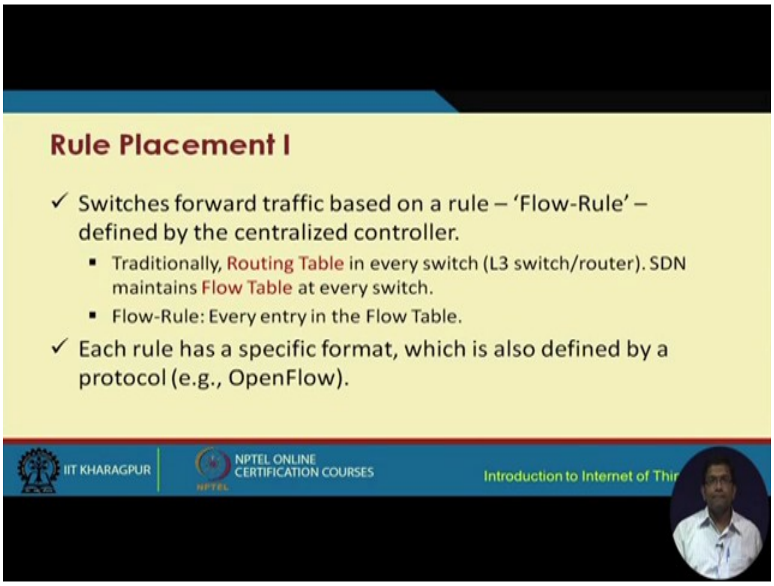
Now the current status of SDN are companies big big companies joined companies like SDN who have their own data centers they have started to implement SDN in their own data centre networks SDN it is required to change the current network with SDN in a phase manner you know it is not like you know we can go and we can change the existing network we can transform the existing switches to support SDN it is not. So, simple you know I has to be architected the hardware have to support the software have to support and so on.

So, these has to be done in a very progressive manner in a very phased manner you know step by step it has to be done operation cost and delay that are caused due to link failure can be significantly minimized using SDN.

(Refer Slide Time: 16:47)

Now, let us come to 2 main challenges when we want to implement SDN in any network. So, these are the rule placement problem and the controller placement problem. So, these are the 2 main problems to be taken care of fundamentally when we talk about SDN.

(Refer Slide Time: 17:08)

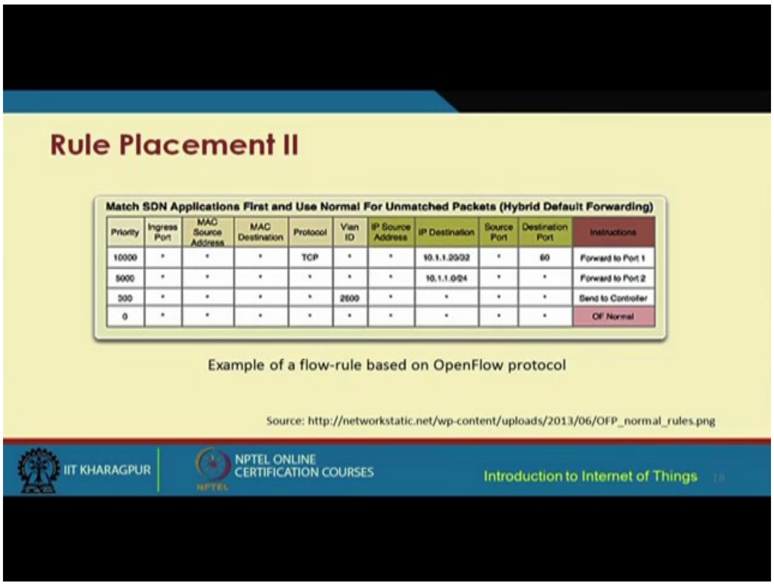


So, with respect to rule placement what happens is here we are talking about flow tables instead of routing tables in the concept of SDN. So, these flow tables. So, basically what happens is this flow tables have different flow rules which are implemented in the same way as traditionally these routing tables have their routing table entries you know different entries in the routing table very synonymously analogously we have flow rules implemented in this flow table.

So, these switches basically in the network they forward the traffic based on this flow rules and this flow rules are basically defined by the centralized controller and this controller as we can recall does not exist in each of these individual switches controller is centralized you know it is separated out typically implemented you know the controller side implemented as the server.

So, from a server this controller is implemented and these controllers basically takes care of this flow rules defining the flow rules based on which the strings of packets that are coming to each of the switches this flow rules are going to determine what is going to be done with the streams of packets that are arriving at the switches. So, we are going to talk about that you know in further detail in a short while.

(Refer Slide Time: 18:47)

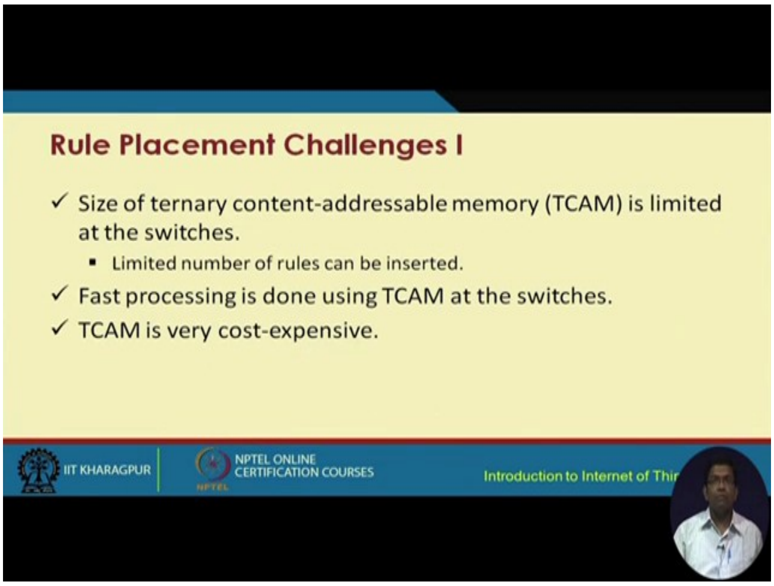


So, each rule has a specific format and that is defined by a particular protocol and currently we are talking about open flow which is sort of like a defacto protocol that is used for implementing SDN. So, you have the rule placement issue. So, you know here what we see over here in this slide is an example of a flow rule that is based on the open flow protocol. So, you know essentially what we see over here is if a packet arrives then it will check the priority if the priority matches maybe in a star means that you know it is it does not require any match.

So, you know if the values of the packet corresponding to this particular fields are different it does not matter, but the protocol has to be TCP and if the IP destination is this and the destination port is this then the instruction; that means, the action that has to be taken is to forward to the particular port. So, here it is forward to port one like this the other flow rules are given over here.

So, for different priority and these things can be anything if the IP destination is this and the; you know the source port and the destination port can be anything then forward to port 2 and so on and so forth for the other entries. So, these are the different flow rules and these fields basically you know we have to remember one thing. So, these fields are fixed this particular fields in open flow these are fixed no one cannot go and change this field and if one changes then we have a different protocol. So, in open flow this field cannot be changed.

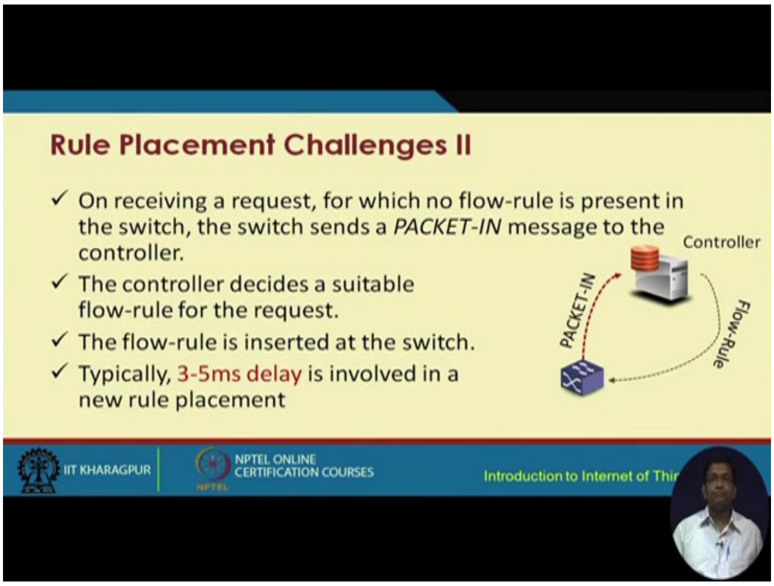
(Refer Slide Time: 20:41)



So, this you know. So, when we place these rules they are placed in the open flow table the flow tables and this flow tables are basically stored in the switches the size of their you know the size of these flow tables are such that they have to be stored in a specialized memory which are known as a TCAM memory ternary content addressable memory and these memories are very limited in size and so, that only a limited number of rules can be inserted in this flow tables. And so, basically the flow tables are residing in these TCAM memories and these TCAM memories are very fast; that means, fast processing can be done that is why the specialized memories are required.

We cannot use any other memories that is at normally available in the switches and other computing hardware and we have to use this TCAM memory at the switches and this TCAM memory they are very expensive as well they are very expensive. So, you cannot you know very easily you cannot scale up we cannot you know get as much memory as we want because of the cost for prohibitiveness.

(Refer Slide Time: 22:01)

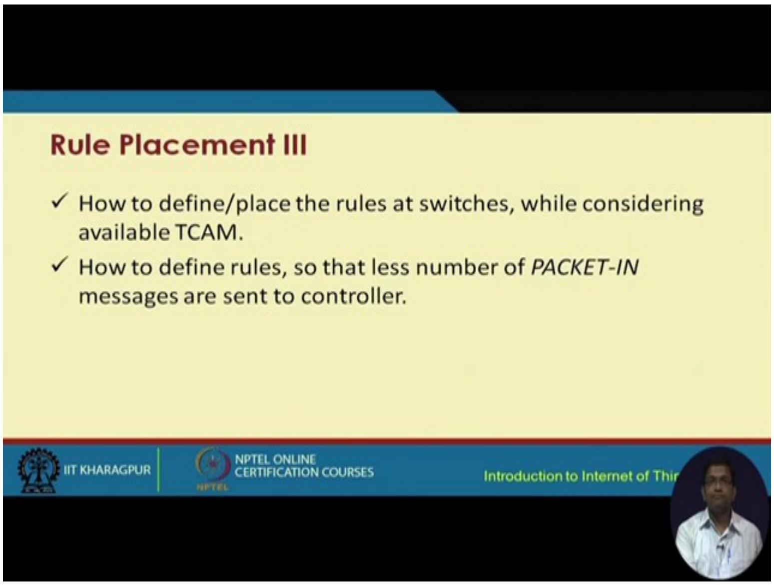


So, on receiving a particular request for which no flow rule is present in the switch, what happens is the switch basically sends a packet which is called the PACKET-IN. So, we have this switch; switch receives a request and it checks its flow table if there is no flow rule that is present in this particular switch in that particular table the switch sends the packet in message to the controller.

Now, this controller besides a suitable flow rule for this particular request and this flow rule is then communicated back to the switch and then this flow rule is going to be inserted in that portable in the switch and typically there is a delay of 3 to 5 milliseconds involved in the new rule placements. So, whenever there is a new rule that has to be placed in the switch which is which is not already existing in the portable in the switch.

This entire communication with controller; controller deciding and sending back the flow rule this takes about 3 to 5 milliseconds delay.

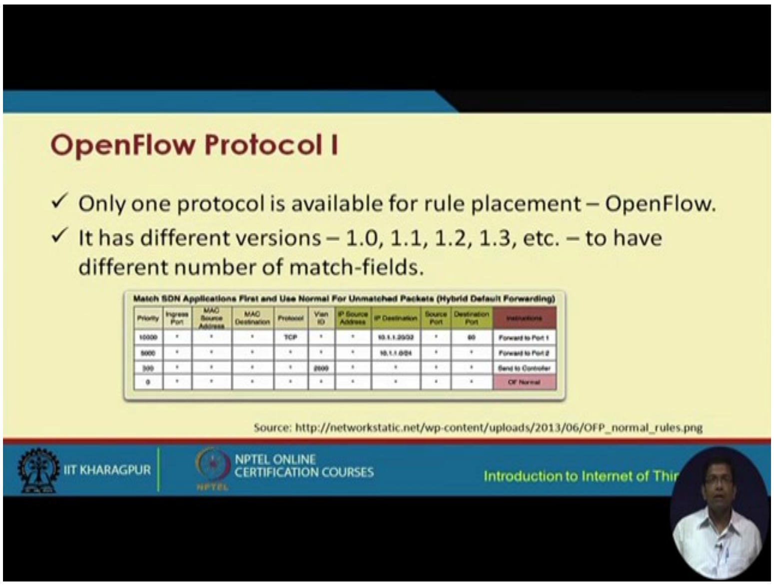
(Refer Slide Time: 23:17)



So, one of the challenges is how to define or place the rules at the switches while considering the available TCAM I already mentioned to you that TCAM is very small in size and it is very expensive it is not very easy to skill scale up.

So, how do we define one of the problems is to define or place the rules at the switches the other problem is how to define the rules. So, that less number of packet in messages are sent to the controller and these are challenges that people the researchers are working on at present defining solutions to these specific problems.

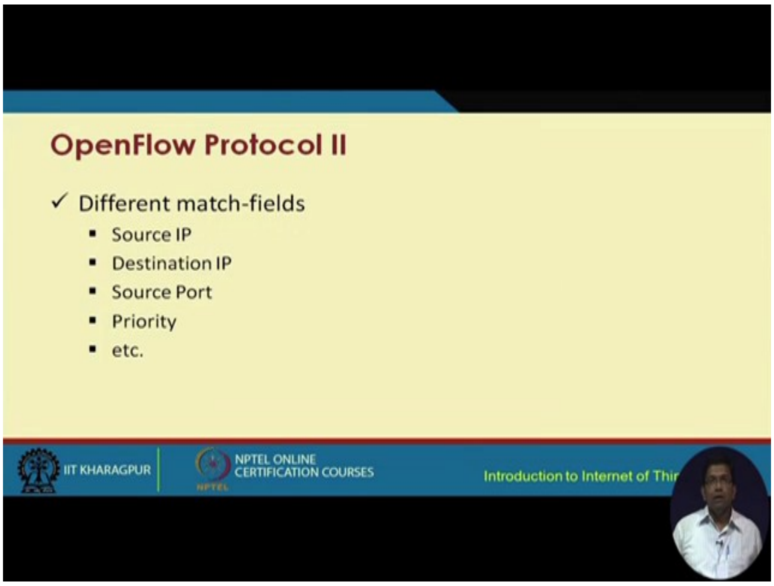
(Refer Slide Time: 23:56)



So, in the open flow protocol rule placement is done it is one of the vital things only one protocol is available for this rule placement which is the open flow protocol.

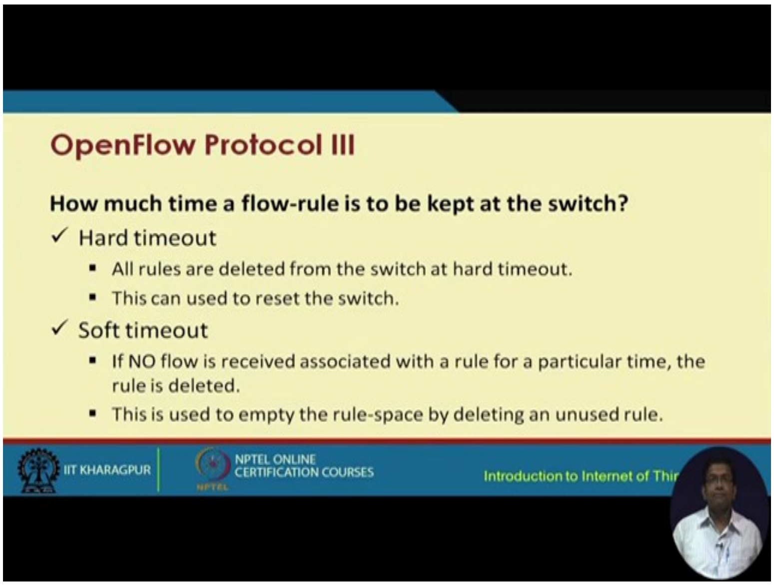
And it has different versions 1.0 1.1 1.2 1.3 open flow has different versions and they have different number of matching fields, but in a particular version of open flow this fields are going to be fixed.

(Refer Slide Time: 24:30).



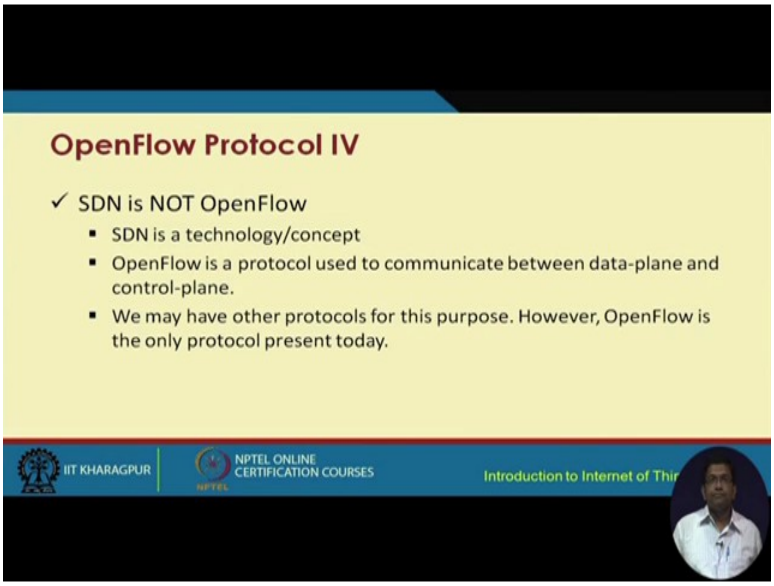
So, there are different matching fields source IP, destination IP source port priority etcetera in a particular version of open flow and that these fields are fixed as I already mentioned.

(Refer Slide Time: 24:45)



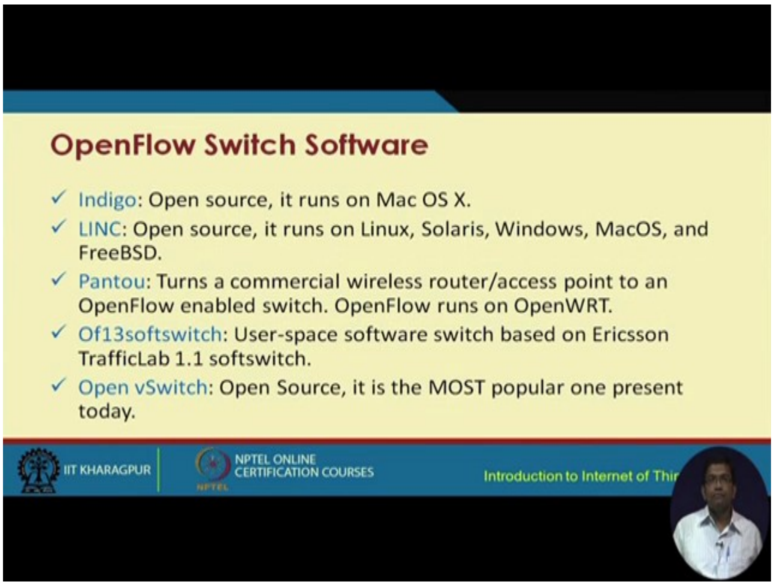
So, one of the issues is that for how long a particular flow rule that is generated is to be kept in the switch for this there are 2 times time outs that are defined one is known as the hard time out the other one is known as the soft time out. So, all the rules are deleted from the switch at a particular hard time in the hard time out methodology this can be done by resetting the switch for example and in the soft time out methodology if no flow is received associated with a particular rule for a timeout interval of time then this particular rule is deleted. So, this is the soft time out.

(Refer Slide Time: 25:37)



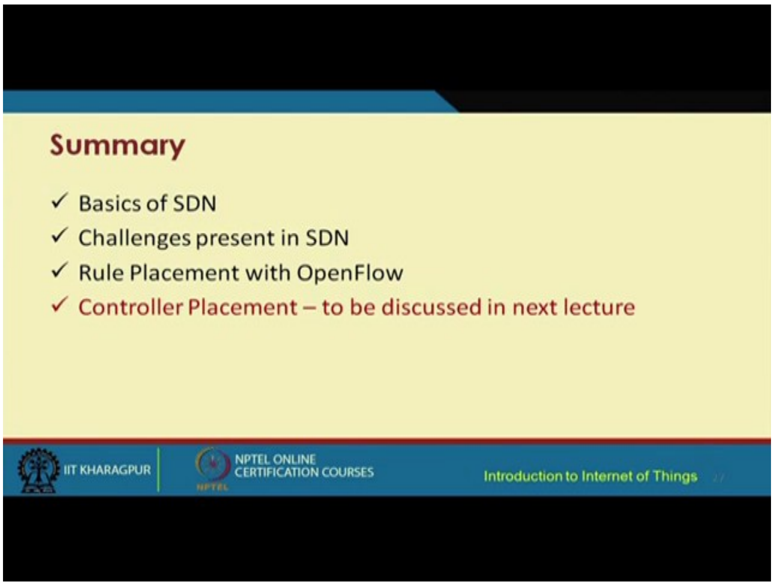
So, we have to remember one thing that I was also briefly mentioning at the outset of this lecture is that SDN and open flow are not one and the same SDN is a technology or a concept, open flow is a protocol that is used to communicate between the data plane and control plane. So, they are distinct and we have to understand and remember this particular difference between these 2.

(Refer Slide Time: 26:05)



Now, these open flow switches are implemented in sorry open flow is implemented in different switches there are different software that have to be that are associated to with open flow implementation. Here is a list of these different software I am not going to go through them most of them are open source and they run on different platforms, different ways for example, linux solaris windows etcetera, etcetera, Indigo, Linc, Pantou open vSwitch these are some of the popular open flow switch software that are available currently to support open flow.

(Refer Slide Time: 26:44)



So, to summarize we have gone through the basics of SDN we have understood the architecture for SDN. We have also understood that in SDN the whole idea is to separate the control plane from the data plane and there is a centralized controller which is typically implemented in a server that takes care of the control logic that has to be implemented while any flow in any flow is received at each of these different switches of the routers.

So, the rule placement is an important problem that we have talked about and there are different issues with the rule placement and another very important problem is the controller placement problem and this is what we are going to discuss in the next part, the second part of the SDN lecture.

Thank you.

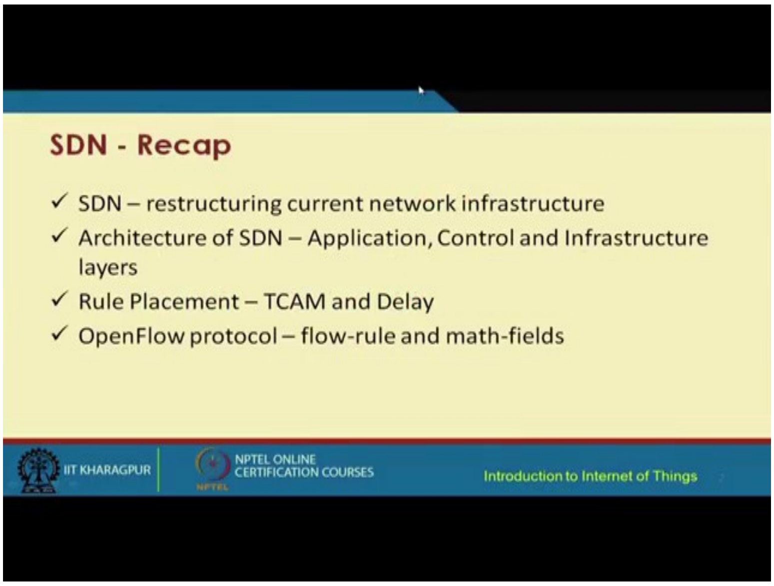
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 34
Software-Defined Networking - Part- II

Now, let us continue our discussions from what where we were in the first part of SDN. So, we are now in the second lecture second part of software defined networks. So, we have already talked about we have understood the rule placement problem and what are the different issues surrounding rule placement and TCAM; TCAM memory, it is limitations and how the rules can be created and how much time these rules are going to be maintained at the switches in the different-different flow tables of these switches.

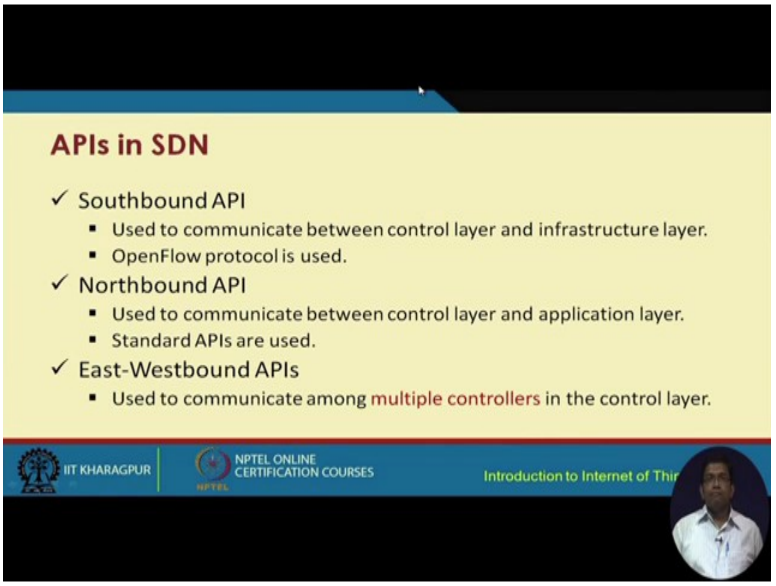
So, the other issue that is very important is the controller placement problem and this is what we are going to discuss next.

(Refer Slide Time: 01:01)



So, we have just as a recap we have already in the first part of SDN. We have understood the basic concept behind SDN the architecture of SDN the rule placement problem and the tradeoff between TCAM limitations limited memory TCAM memory and the delay. And we have also understood the open flow protocol and flow rule.

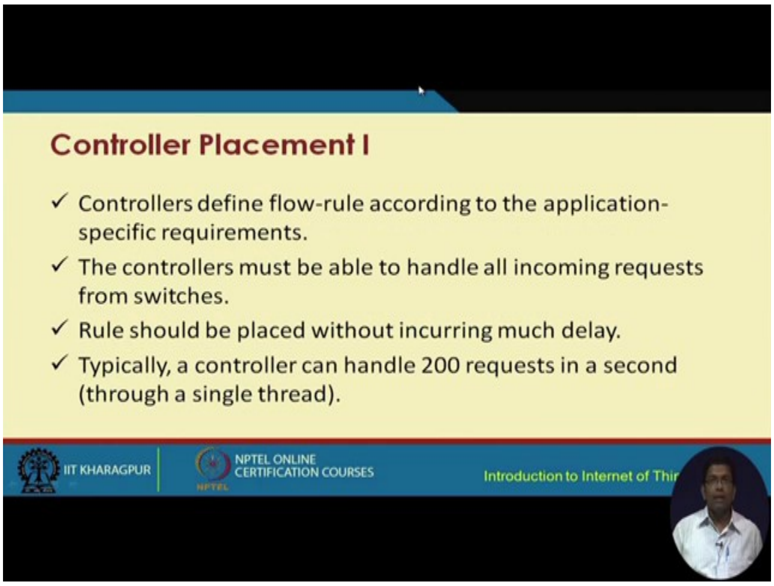
(Refer Slide Time: 01:32)



And the math rule math fields in the open flow protocol. So, in SDN between the data plane and between the data plane and the control plane we have an API and another API between the control plane and the application plane.

So, the first one; that means, between the control plane and the data plane and; that means, the infrastructure what we have is the south southbound API. And the open flow protocol is the protocol that is used for the southbound API communication for the northbound API this northbound API is used to communicate between the control layer and the application layer these 2 planes control plane and the application plane. And the all these existing standard API is that are used can still be used in the northbound API there is also the concept of another kind of API which is called the east westbound east westbound API and this concept this terminology comes into picture when we are talking about not a single controller, but multiple controllers in the control layer.

(Refer Slide Time: 02:41)

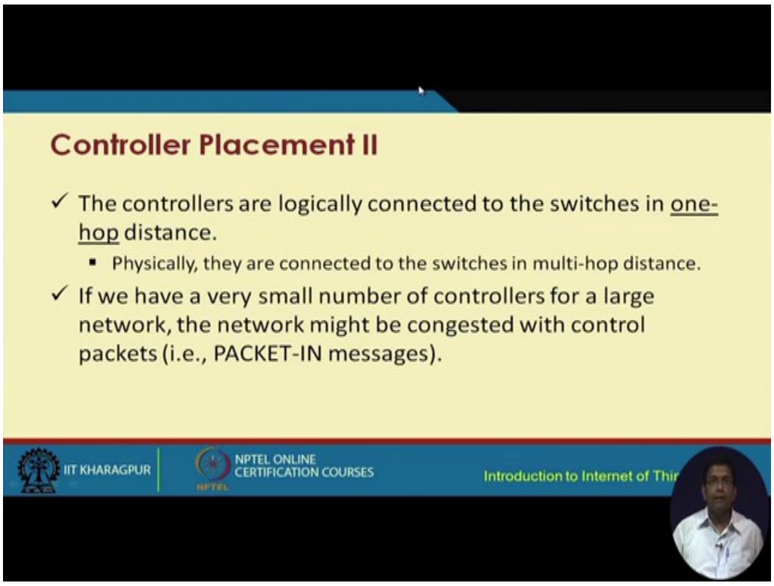


So, controllers basically define the rule the flow rule according to the application specific requirements. So, basically you know what is happening over here in SDN is that the control logic is basically you know taken care of by the control plane. So, you know control logic is separated out and as a result the controller knows what has to be done with a particular flow. And the controller basically controls the overall flow in the network and each of these switches what they are going to do that is done by the controller.

So, now, going back the controllers define the flow rule according to the application specific requirements the controller must be able to handle all these incoming requests from the switches and the rules should be placed without incurring much delay and that is important. Typically, in the rules the placement of the rules if it is not already existing in the flow table of a switch typically as we have seen before takes about 3 to 5 milliseconds, but you know this has to be minimized because otherwise what is going to happen is there are you know there will be a huge control overhead and that has to be that, because the controller is being separated out the control logic is separated out to the controller we do not want too much of a control delay control linked delay to happen there is a trade off definitely we cannot avoid this delay, but we have to minimize this particular delay.

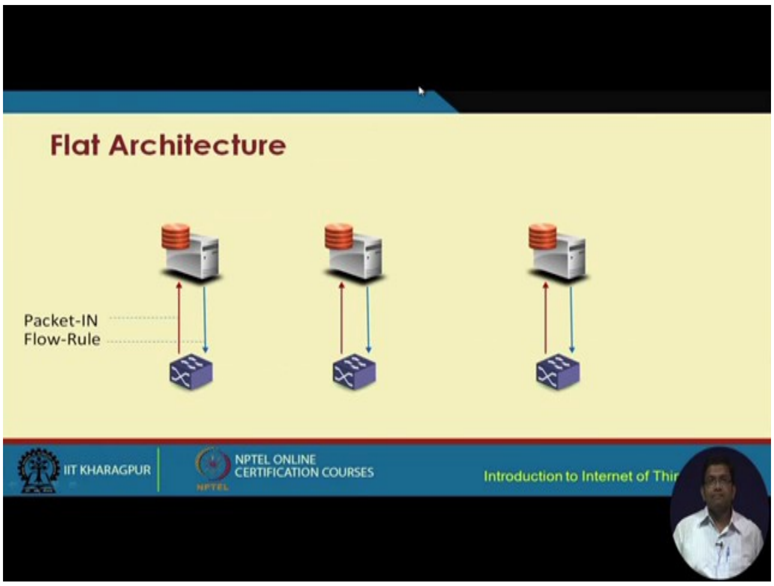
So, typically a controller can handle roughly about 2 hundred requests in a second and that is applicable for only the single threaded applications thing.

(Refer Slide Time: 04:24)



So, the controllers which are implementing similar thread, but currently multi threaded applications in controllers are also possible. The controllers are logically connected to the switches in a one-hop distance it is just a logical connection. So, the controller from the switch the switch thinks that the controller is away just a hop distance from it just one hop from it, but actually it is not so; actually you know physically when we are talking about the controller and the switch can be multiple hops away and typically they are multiple hops away.

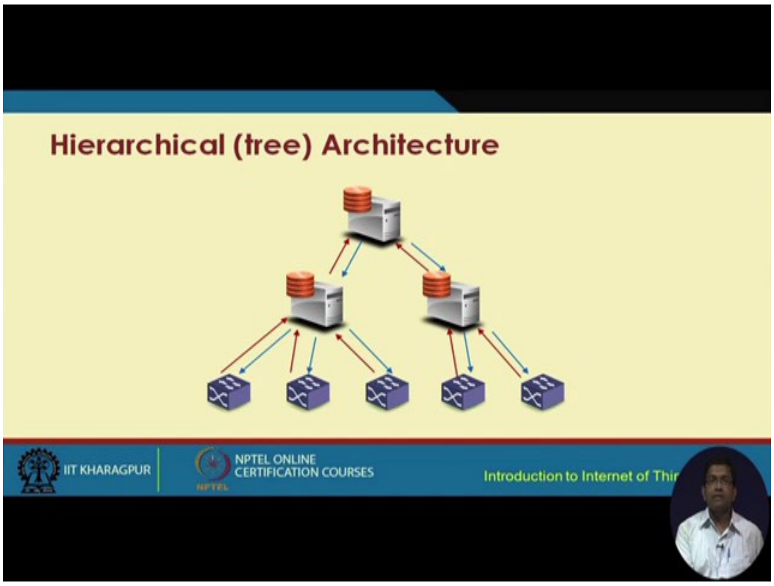
(Refer Slide Time: 05:03)



So, if we have a small number of controllers for a large network the network might be congested with control packets these packet in messages and so, if we look at this controller placement there are different architectures you know how and where we are going to place this controller. So, one architecture the basic architecture is called the flat architecture, and here basically the switch and the controller they are just logically one hop away the switch sends a packet in message to the controller if the switch already does not have this flow rule for the particular flow that it has received.

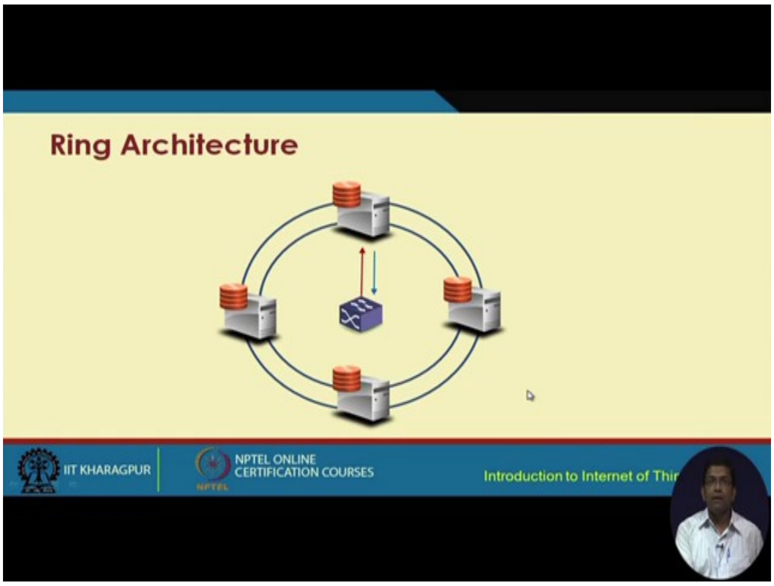
So, it will set a send a packet in message to the controller and the controller is going to send back the flow rule corresponding to that to that particular. That means, how it is at how the switch is going to treat it you know that particular instruction is going to be sent by the controller the controller knows it the controller knows how the different flows how the different packets are going to be handled this is the assumption in this particular technology SDN technology.

(Refer Slide Time: 06:09)



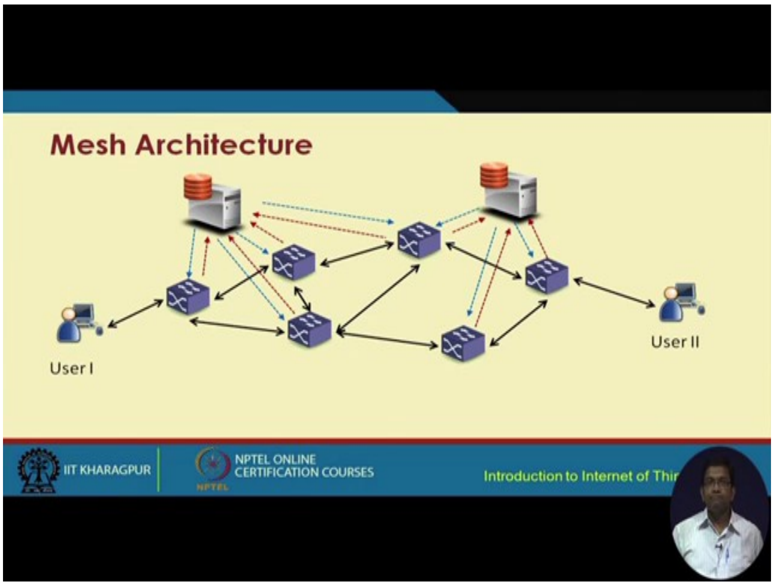
So, this is the flat architecture then we can have different other architectures this is the hierarchical or the tree architecture and these I do not need to elaborate further, but it is quite obvious we have these different switches and hierarchically they are placed within the controllers are placed and connected to these different switches in a tree like fashion.

(Refer Slide Time: 06:33)



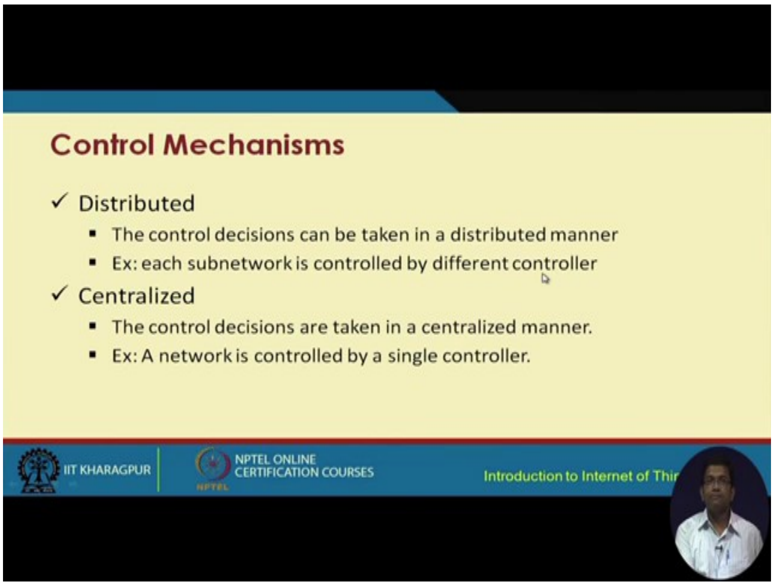
And we have this packet in message and the corresponding flow rule coming back for each of these connectivity's then we have the ring architecture. In the ring architecture we have a similar kind of thing, but we have to keep in mind that in the ring architecture. So, basically these controllers are placed in a ring like fashion we have multiple controllers like this placed in ring like fashion, but a particular switch is connected to only one controller in this version.

(Refer Slide Time: 07:18)



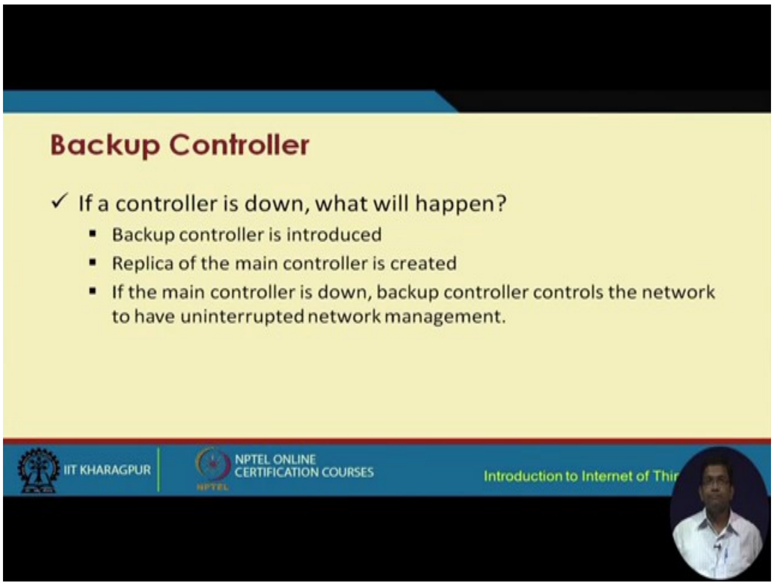
So, when the packet in request has to be sent this PACKET-IN request will be sent to a single controller only not that it can be sent to any of the other controllers in the ring it will be sent to a single controller and the flow rule is going to be sent to this particular switch that has requested the rule, and then we have the mesh architecture mesh as we know increases the reliability. And as you can see over here for instance we have 2 different switches who can be connected to a single controller. So, if this one goes down there is the other one which can take over and so on.

(Refer Slide Time: 07:41)



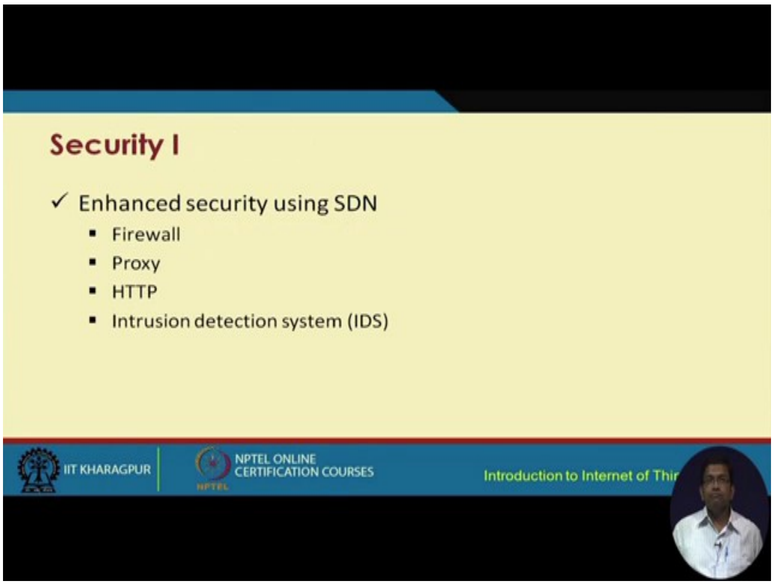
So, it basically increases improves the fault tolerance and improves the reliability of the network the mesh architecture. Now this control how this control is going to be done, how the control decisions are going to be made there are 2 different approaches one is the distributed the other one is centralized. In the distributed the control divisions can be taken in a distributed manner. For example, each sub network is controlled by a different controller. And in the centralized mechanism the control decisions are taken in a centralized manner. For example, a network is controlled by a single controller.

(Refer Slide Time: 08:21)



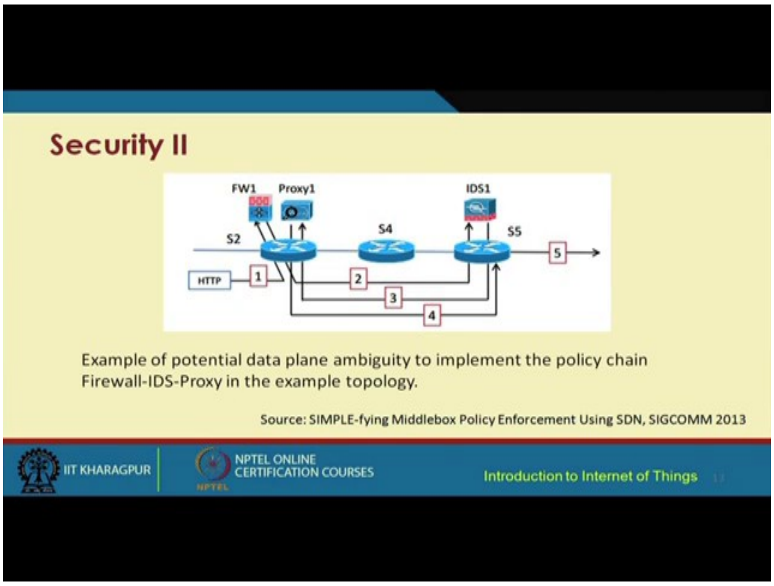
So, in such a case it is a centralized control and dividing into different sub networks are having a controller corresponding to it will be distributed solution there is also a concept of backup controller. So, if the primary controller is down then the backup controller takes over.

(Refer Slide Time: 08:42)



So, backup controller has a replica of the main controller and if the main controller is down the backup controller controls the network to have uninterrupted network management another very important thing is true in SDN one can have enhanced level of security in the network and in this particular case we will be taking help of the firewall proxy http etcetera, etcetera and the IDS and these can have improved security with respect to this technology.

(Refer Slide Time: 09:05)

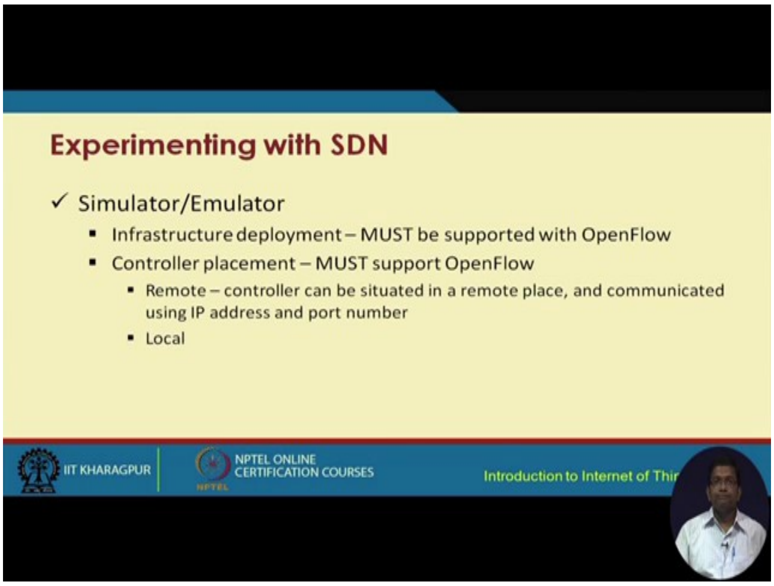


So, just as a very brief you know here we are not going to discuss about you know improving security with SDN and in much detail, but just as a brief you know this is the this is this is a this is a paper which was published in SIGCOMM in 2013 very recently; that means, which is talking about the simplifying protocol for policy enforcement.

So, what it does? So, you know let us look at this particular figure. So, it is an example of a potential data plane ambiguity to implement the policy chain this chain firewall IDS proxy in this particular topology and the sequence of flow of instructions is like this. So, it will this is from the http when a http request comes then it is sent from one switch to another switch. This particular switch then it goes to the IDS comes back goes to the proxy and the forwarding and the firewall.

And then finally, to this particular switch and then to the then finally, out of the network. So, this is how you know security is implemented and enhanced using SDN. So, we are not talking about as I mentioned already I just wanted to show you that security can indeed be improved with the help of SDN. And we do not want to discuss anything further on this particular issue.

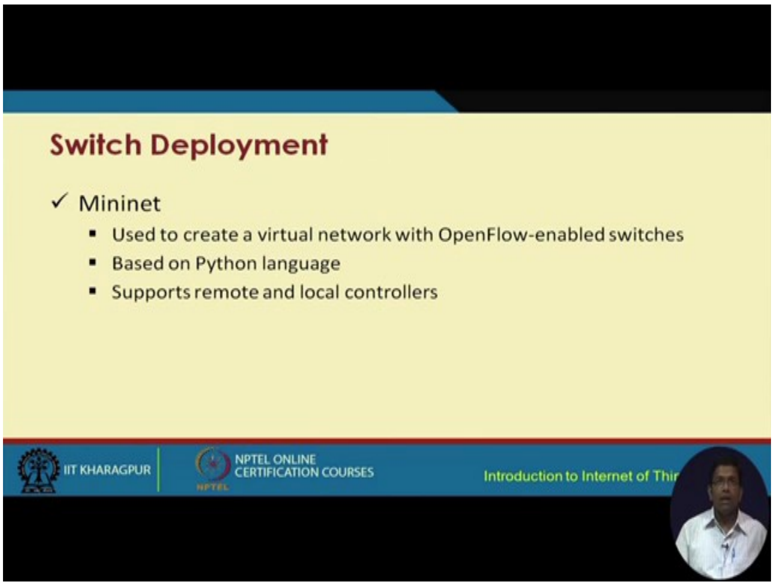
(Refer Slide Time: 10:39)



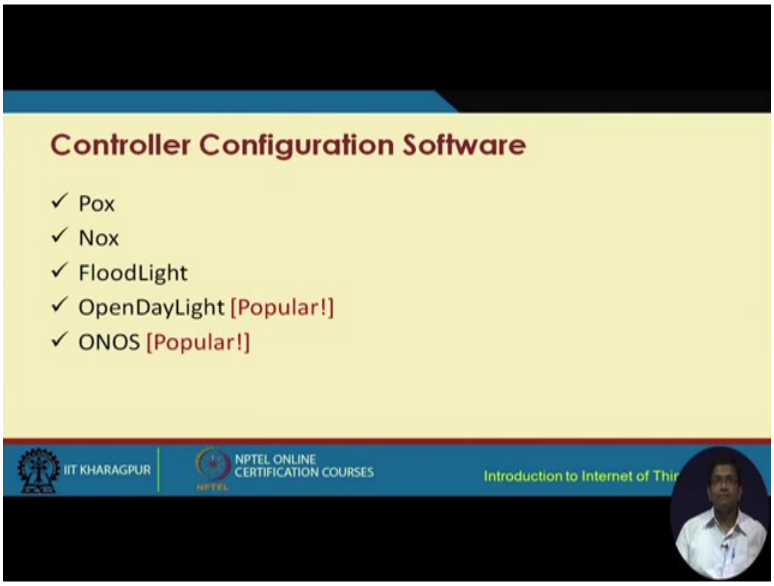
So, how do you. So, let us say that we have implemented SDN or we want to implement SDN and. So, so one of the things is that we have to experiment we have to experiment we have to evaluate the performance through experimentation. So, experimentation can be done with the help of simulators or they can be done with the help of emulators in emulators, basically what happens it is little different from the simulators. So, here the real emulators can be connected to the real network where real traffic can flow through this emulator and the data can be analyzed the performance of the network can be analyzed using these emulators. Simulators on the other hand basically simulate the entire thing packet flows, the network, the nodes, everything is simulated.

So, these simulators or the emulators take care of few different things one is the infrastructure deployment and this must be supported with open flow and the controller placement which must support open flow this controller can be a remote controller or a local controller and in the remote basically the controller can be situated in a remote place and communicated using IP address and port number a local controller basically does you know everything is local the controller itself is local and you know it takes care of it in a takes care of it locally for switch deployment the Mininet software is very Mininet simulator it is an emulator as well. So, it is very useful it is used to create a virtual network with open flow enable switches it runs on python and supports remote and local controllers both remote controller and local controllers are supported by Mininet.

(Refer Slide Time: 12:18)

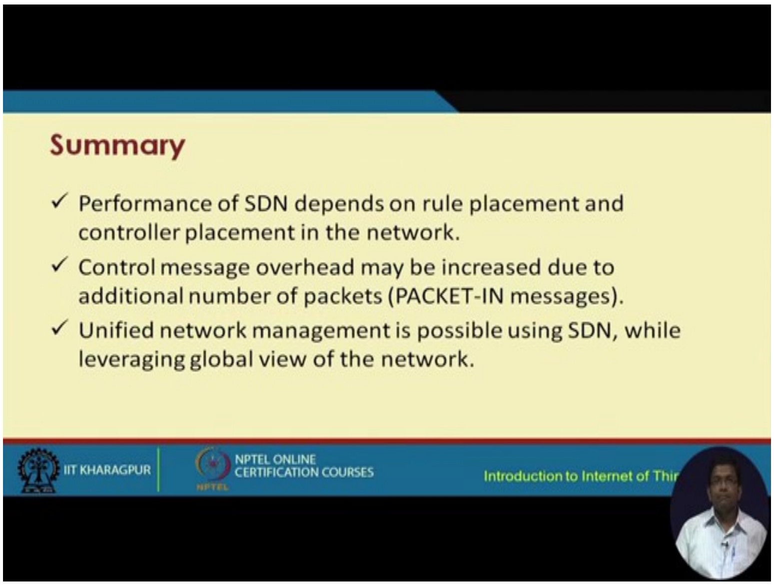


(Refer Slide Time: 12:45)



There are controller configuration software for example, Pox, Nox, Floodlight open daylight and ONOS particularly open daylight and ONOS are the most popular once that are used for controller configuration.

(Refer Slide Time: 13:02)



So, with this we come to almost the end of the lecture on SDN and we have understood the basics of SDN what is the motivation behind SDN why do we want to separate out the control logic from the data logic data plane which takes care of functions like forwarding etcetera to make the network efficient, but there is a trade off as well and we have seen that that more number of control packets are going to flow through the network.

But we want to minimize that control logic and this is where lot of research is being undertaken at present and we have also seen that the performance of SDN basically depends on 2 particular issues the rule placement and the controller placement in the network. Control message overhead as I was mentioning before will be increased due to additional number of packets the packet in messages from the switches to the controller going through. And what is required is to have an unified network management to be made should be made possible using SDN while leveraging the global view of the network. So, we need to have an unified unified network management architectural framework using SDN with this we come to an end of the SDN lecture.

And so, next what we are going to talk about in another the next lecture is how SDN can be used in IoT to make IoT efficient internet of things efficient. So, we will have to wait for the next lecture in order to understand this.

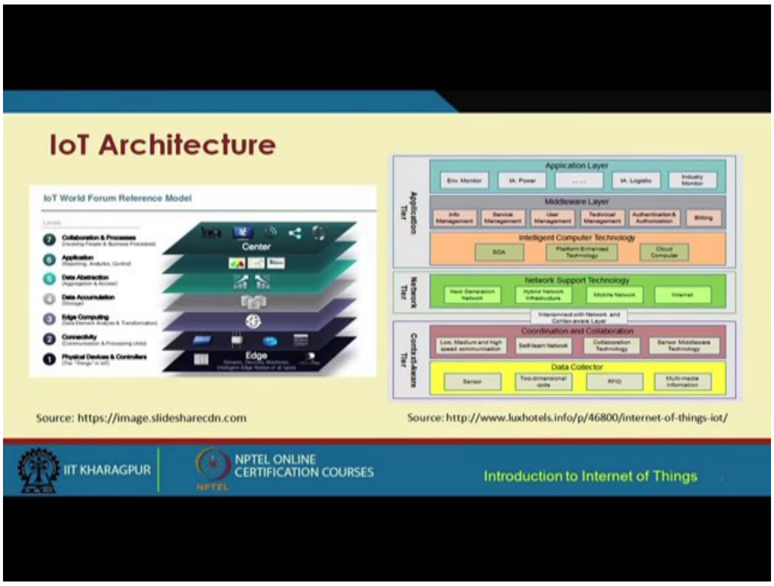
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 35
Software-Defined loT Networking - Part- 1

Having understood software defined networking basic concepts through the previous two lectures, we are now going to see how SDN can be used in the context of internet of things the theme of this particular course. And as we will see that there is lot of opportunity and lot of problems number of problems that are facing internet of things can be addressed with the help of IoT with the help of SDN technology.

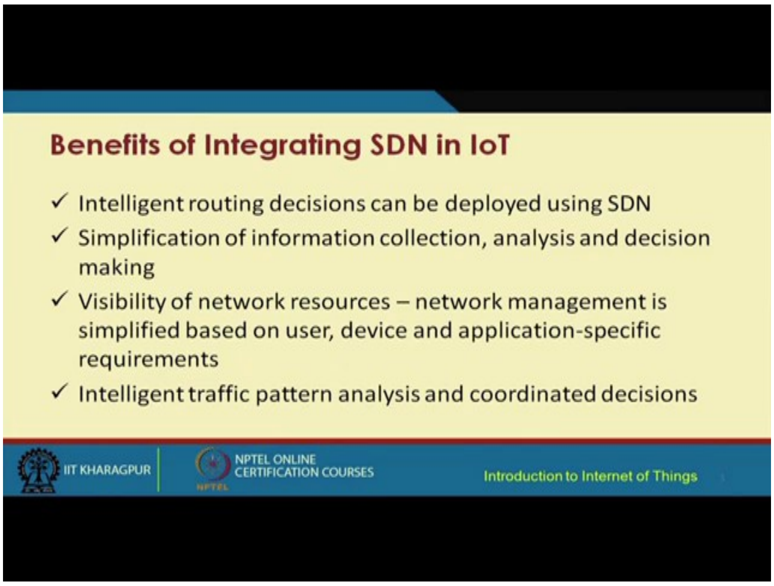
(Refer Slide Time: 01:08)



So, let us look at how SDN can be applied in making for making IoT efficient, so, if we look at the IoT architecture we have already seen the IoT architecture in different ways in the previous lectures. So, let us now look at from a different perspective. So, what we have as we can see here is the different layers in the reference model this is taken from the wall forum reference model and we have different layers. For example, the physical devices and controllers connectivity age computing data accumulation data abstraction application collaboration and processes and the right hand side figure shows a different view of IoT all together from a different viewpoint how IoT works.

So, we have this tiered segmentation of the IoT networks we have the context aware tier we have the network tier and we have the application tier and these different modules corresponding to each of these tiers are all given over here without. So, it is not required for us to understand each of this in further detail and with this particular background of IoT.

(Refer Slide Time: 02:32)

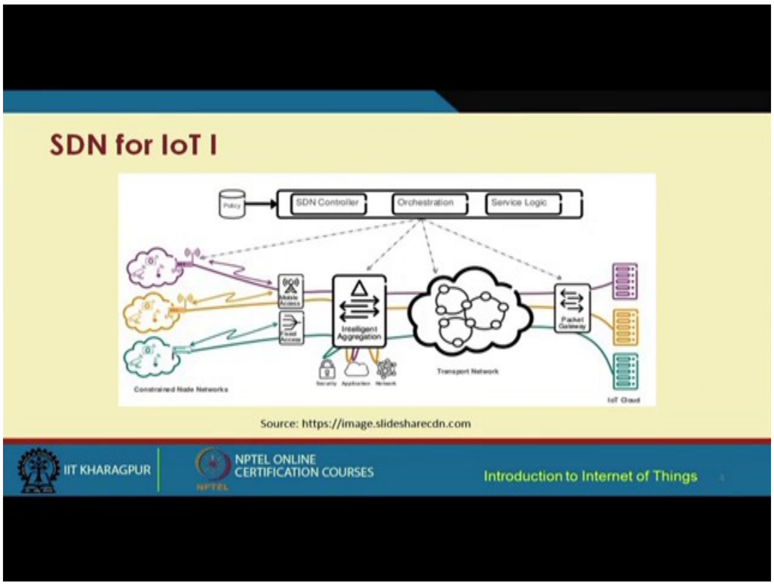


Let us now move ahead and see how SDN can benefit IoT. So, you know the integration of SDN to IoT. So, by doing integration of SDN to IoT one very important fundamental problem that can be solved is one can have intelligent routing decision making to be done to implemented in an SDN implemented IoT network.

The second thing is the information collection analysis decision making all of these can be simplified through the integration of SDN in IoT third is the visibility of network resources network management is simplified based on the user device the application specific requirements. So, this visibility of network resources and the simplification with respect to these criteria these aspects they can be done with the help of indication of SDN in IoT.

And the last one is intelligent traffic pattern analysis and coordinated decisions and I do not need to elaborate further on this, because this is quite self explanatory intelligent traffic pattern analysis and coordinated decision making through the controller right. So, we already know what a controller means and what it does. So, all these things can be done with the help of SDN. So, what is very important is intelligence you know more intelligence is proved into the network and improving the efficiency of the network with the help of the SDN technology. So, IoT can also benefit from these advantages.

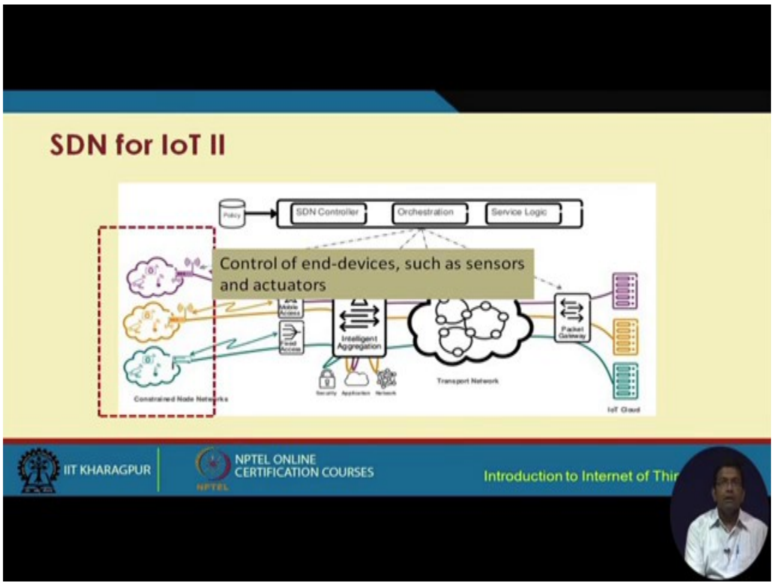
(Refer Slide Time: 04:24)



Now, if we look at this particular figure in front of us we have these different devices the IoT devices in different sub networks maybe and these devices through mobile axis or fixed axis channels this data from these devices they can be acquired and be transmitted to the data aggregator. Here all these data aggregation are going to be done of the data that is received from these different IoT devices. And then it passes through a transport network and from the transport network it goes to the different gateways and the packet segregation is going to be done using this.

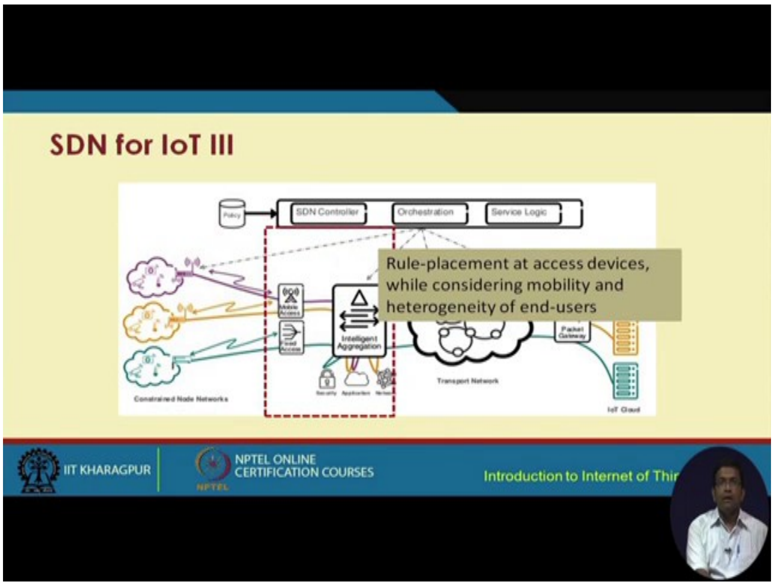
So, this is basically the simplified view of an IoT network now what happens is when we want to integrate SDN what we are trying to do is we are going to use the SDN controller. So, what the SDN controller is going to do is it is going to control each of these different things different aspects and also it is you know it is going to improve the orchestration between the different devices between the different protocols that are running, etcetera, etcetera in this network and overall it is going to improve the service logic that is behind it. So, this is going to be improved.

(Refer Slide Time: 06:00)

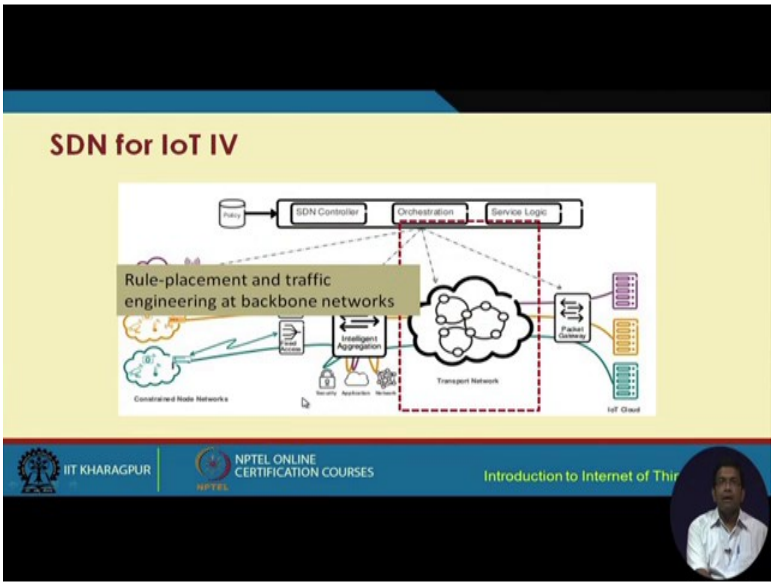


Now with the SDN with the implementation of the SDN the control of these n devices IoT devices which includes sensors actuators RF id tags and any other IoT device. So, you know the centralized control is made possible then here as we can see this part can take care of the rule placement, because we have these access devices over here the rule placement while considering issues like mobility etcetera and the heterogeneity of the n devices this can be implemented here.

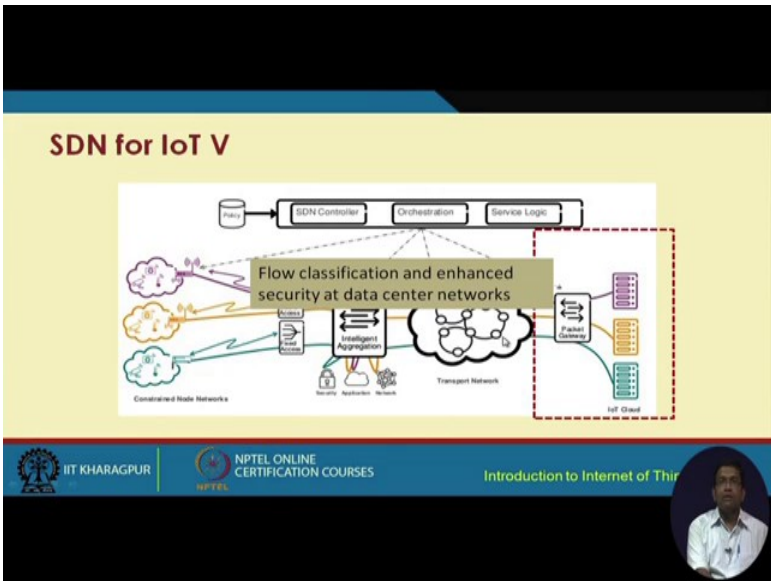
(Refer Slide Time: 06:28)



(Refer Slide Time: 06:47)

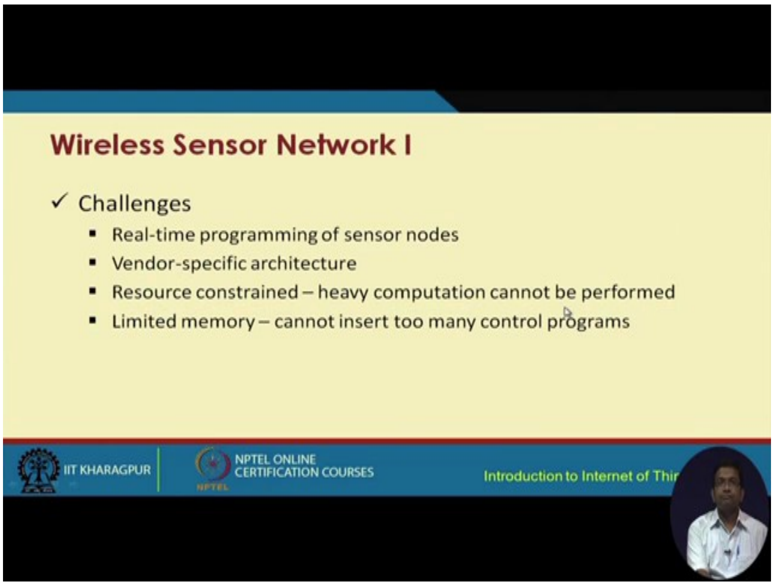


(Refer Slide Time: 06:58)



And the rule placement and traffic engineering and backbone networks can be taken care of at the transport network and flow classification and enhanced security are taken care of at the data center networks.

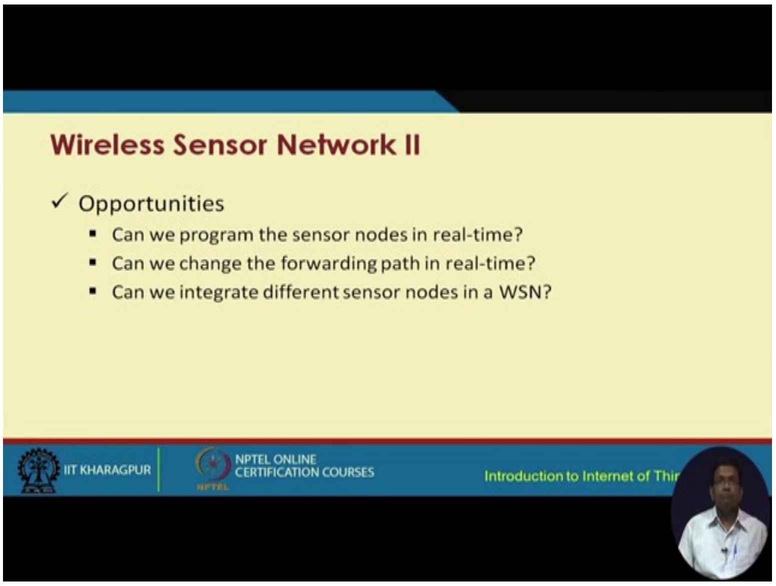
(Refer Slide Time: 07:06)



So, let us switch back our gear and let us look at one of the fundamental building blocks of IoT which is the sensor network. So, one of the challenge is in behind the working of the sensor network is real time programming of each of these sensor nodes is typically not feasible not at all feasible you know you cannot go and you know program the sensor nodes as such you know it is possible to program the sensor nodes, but you know real time programming of these sensor nodes is not possible. Then these sensor nodes and these corresponding networks they have they follow vendor specific architecture each of these nodes that are made by different vendors they have their own different architectures different layers implemented in them there is no one standard.

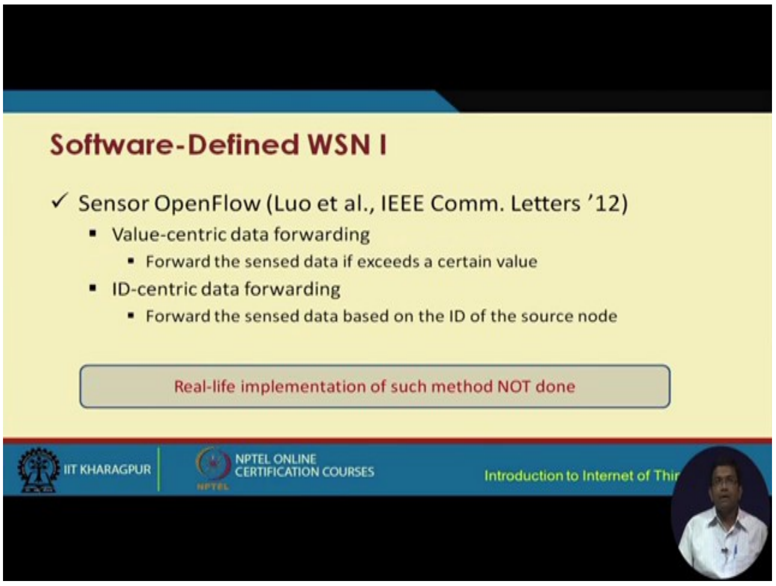
So, now the each of them they implement their own vendor specific architecture these nodes are resource constrained. So, you know the heavy computations that are often required cannot be performed at each of these nodes and additionally there is the resource limitation with respect to memory there is limited memory. So, we cannot insert too many control programs in these networks.

(Refer Slide Time: 08:26)



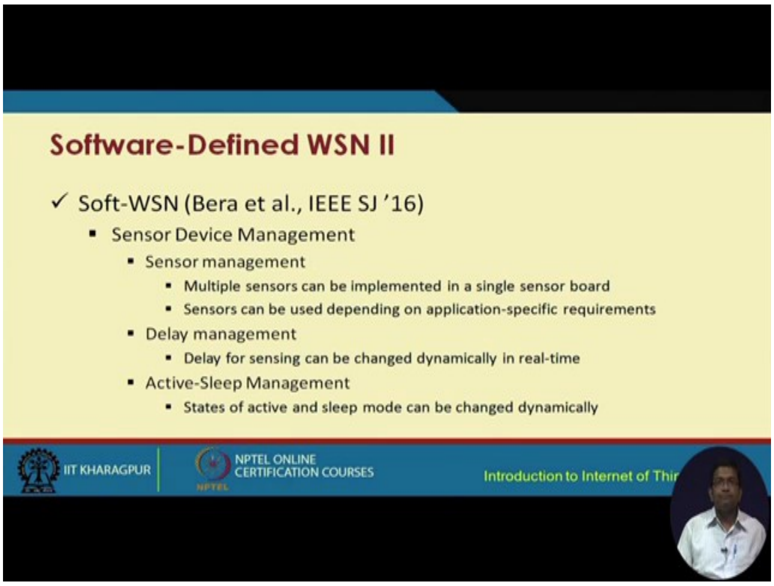
So, these challenges basically also gives us opportunities like can we program the sensor nodes in real time can we change the forwarding path in real time can we integrate the different sensor nodes in a sensor network.

(Refer Slide Time: 08:44)



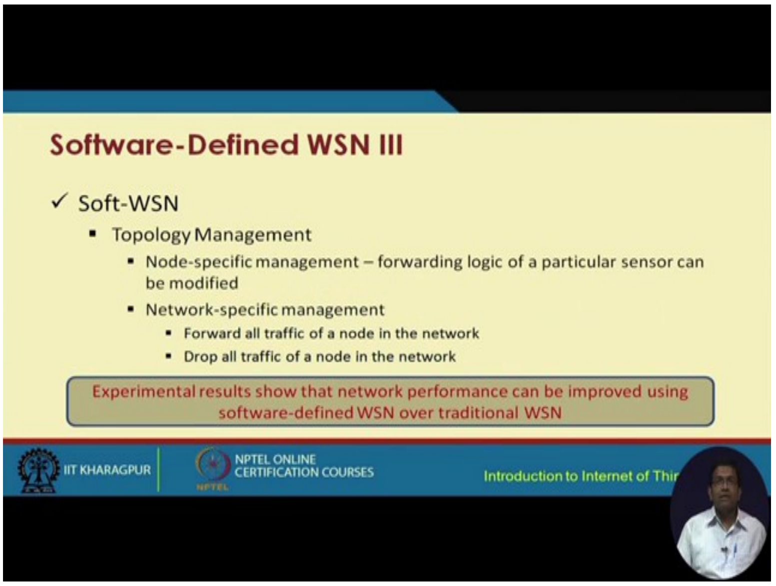
So, we have different solutions that have been proposed to take care of these challenges and opportunities that exist one of the recent works relatively recent works which was published in the IEEE communication letters in 2012 is the sensor open flow protocol. So, the sensor open flow protocol takes care of forwarding in two different ways one is the value centric data forwarding the other one is the ID-centric data forwarding value centric. For example, if the sensor data exceeds a certain threshold value then the data is going to be forwarded other way the other way round is to adopt the ID-centric data forwarding. For example, the data will be forwarded based on the ID of the source node if it is coming from a particular source node with certain ID then it is going to be forwarded otherwise not.

(Refer Slide Time: 10:00)



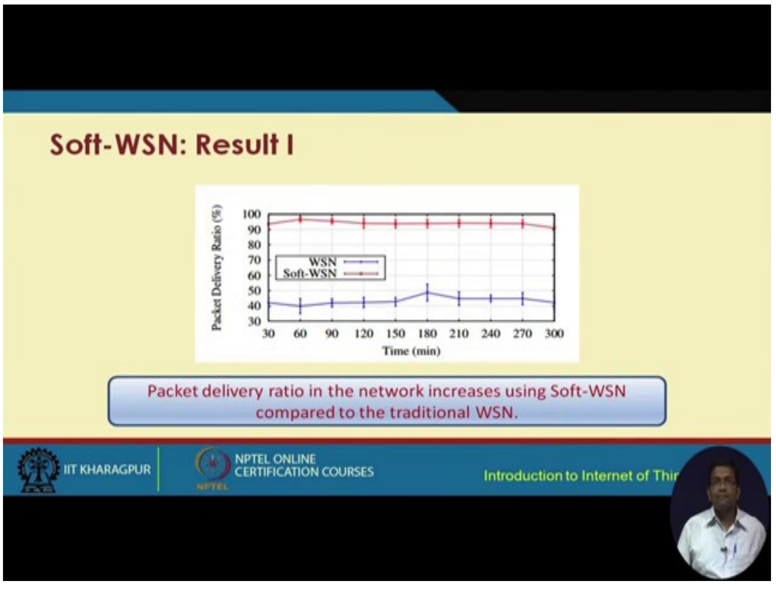
So, real life implementation of such a method is not yet available this is one of the limitations of these particular solutions Bera et al; that means, in our group this one group we have proposed the Soft-WSN protocol and it was published in the IEEE systems journal in 2016 here we have adopted different component solutions. So, we have the sensor device management which comprises of sensor management delay management and active sleep management I am not going to go through these in detail, but it is available and there is available for you in the slide and for further details it is there in the paper IEEE systems journal paper.

(Refer Slide Time: 10:47)



So, this is one major component the sensor device management and the other one is the topology management. So, topology management basically you know takes care of node specific management for forwarding of the data from their specific nodes and we have what we have done compared to the previous low et al's paper low et al's work which was published in IEEE communication letters in 2016 here we have performed experimental results you know here we have performed really real life experimentation. So, we have in this paper we have shown experimental results that show that the network performance can be improved using software defined WSN over traditional WSN.

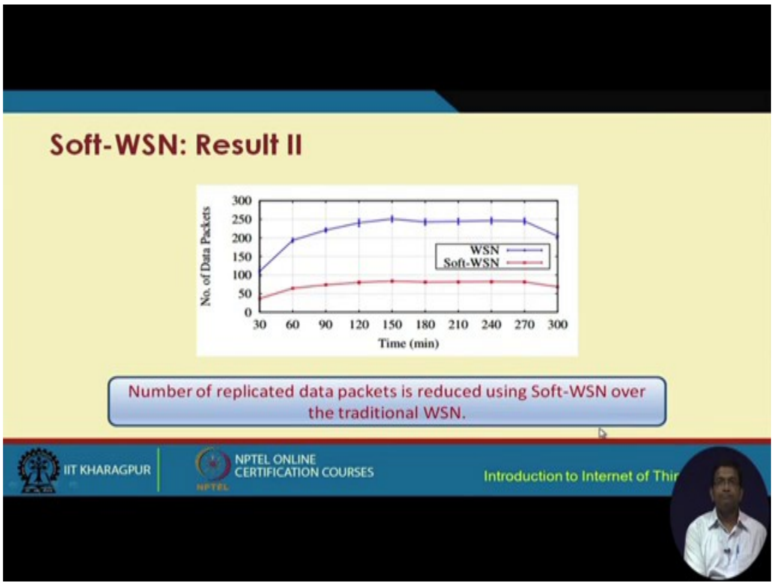
(Refer Slide Time: 11:26)



So, I will just present very briefly some of the results I have taken from that particular paper for example, with respect to the packet delivery ratio. So, this is the packet delivery ratio using soft WSN. That means the proposed solution and and the regular WSN where no protocol is implemented. So, it is a paired pone basic protocol that exists.

So, here that is the reason actually we have observed and that we are able to see much improved packet delivery ratio much improved packet delivery ratio using soft WSN. So, what we see is the packet delivery ratio in the network increases using soft WSN compared to the traditional WSN.

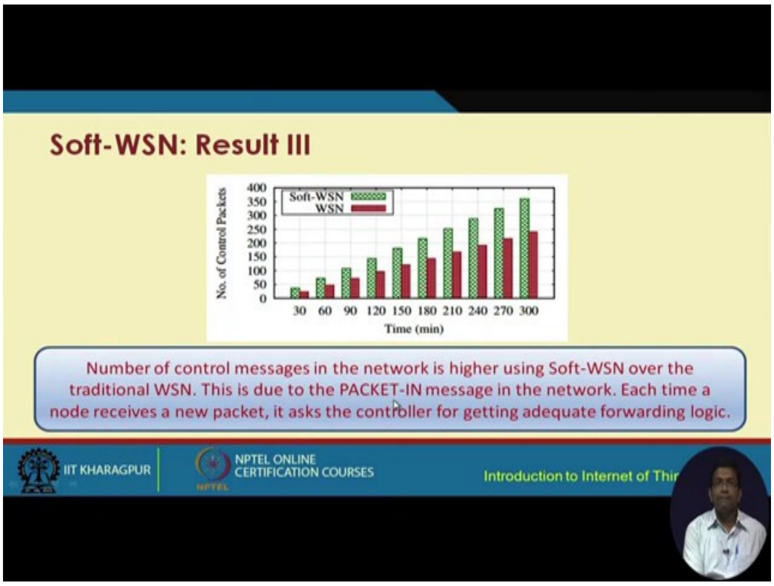
(Refer Slide Time: 12:17)



Here this plot shows the number of data packets that are forwarded and as we can see over here the soft WSN the number of data packets that are forwarded is much less compared to the number of packets in in a regular WSN.

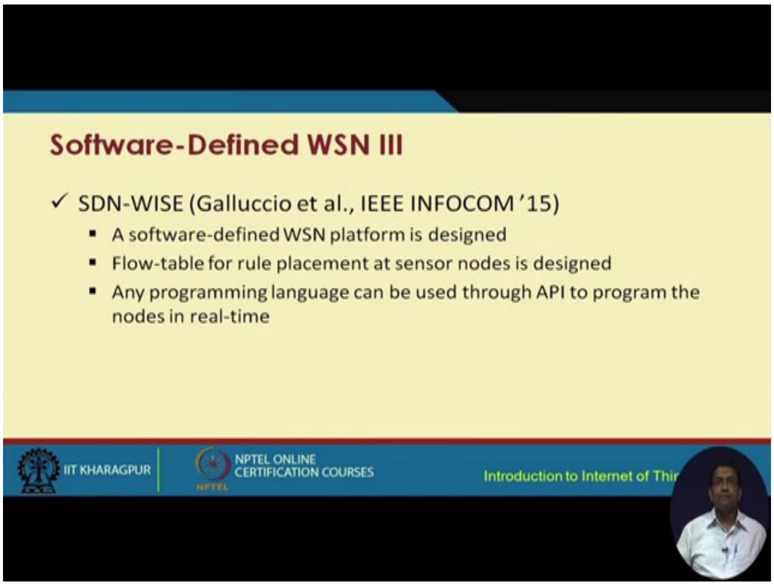
So, the data packet means the replicated data packets. So, I should mention this over here the number of replicated data packets. So, replicated data packets not the number of regular data packets, but the replicated data means this soft WSN basically reduces the number of replications of data packets over the traditional WSN.

(Refer Slide Time: 12:57)



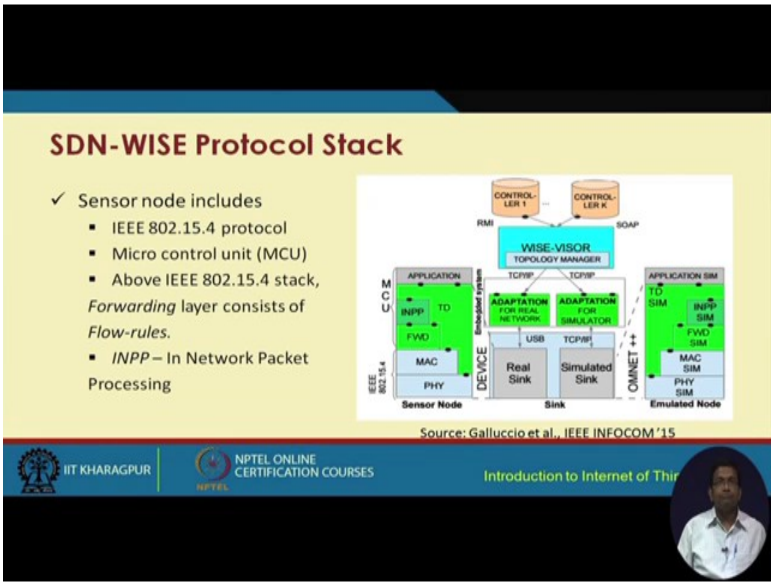
The third result basically shows the number of control packets that are forwarded the number of control packets in the network is higher using this proposed protocol the soft WSN protocol. That means, our protocol over the traditional WSN this is due to that the packet in messages in the network are less each time a node receives a new packet it asks the controller for getting adequate forwarding logic and that is why the number of control messages in the network gets reduced.

(Refer Slide Time: 13:37)



The other solution which has integrated SDN into sensor networks is the SDN-WISE and it was published in the IEEE INFOCOM conference in 2015. So, here it is a SDN you know software defined some WSN platform SDN why is basically proposes a software defined WSN sensor network platform where the flow table for rule placement is is available at the sensor nodes it was designed how the flow table is going to look like and any programming language can be used through API to program the nodes in real time in SDN-WISE.

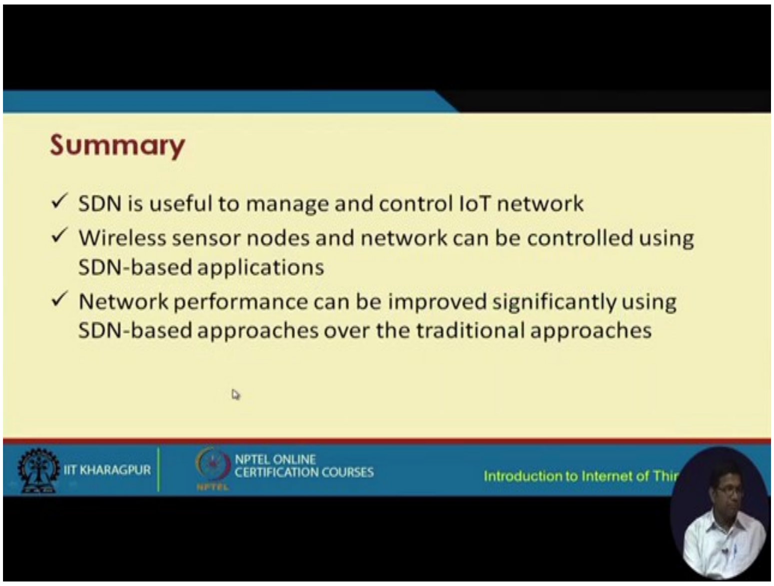
(Refer Slide Time: 14:24)



Very briefly I want to show you the schematic of how SDN-WISE works I do not want to you know discuss this solution in detail, but I just wanted to show you the overall architecture of SDN-WISE. So, what we have are the sensor nodes we have the sink. And we have the emulated nodes and so, as we can see over here we have in the sink we have the real sink and their simulated sink. And these are the different layers the forwarding layer over here and the different other regular layers and how they talk to each other.

So, this part is the emulated part and this part is the real part and this one the sink basically has to both the components the real sink as well as the simulated sink. So, these sensor nodes basically they have they run the 802.15.4 protocol in their work SDN-WISE there is a microcontroller unit and there is a 802.15.4 stack on top of which SDN-WISE basically functions right. And then we have the INPP which is the in network packet progressing processing layer.

(Refer Slide Time: 15:44)



So, in summary we have looked at how SDN is useful to manage and control the IoT network wireless sensor nodes. And network can be controlled using SDN based applications, network performance can be improved significantly using SDN based approaches over the traditional sensor network approaches and we have also seen that there are different protocols.

The latest one that we have seen is the SDN-WISE we have also looked at the soft WSN protocol that was in fact, proposed by us. And we had experimented with real hardware real IoT hardware real sensor network hardware and before that there is there was another solution that was proposed by Low et al and was published in the IEEE communication letters in 2012.

So, basically these are the three main protocols that are available currently there are few other solutions also that might that are also available, but these are the prominent ones and. So, this is basically the state of the art with respect to the implementation of SDN for sensor network.

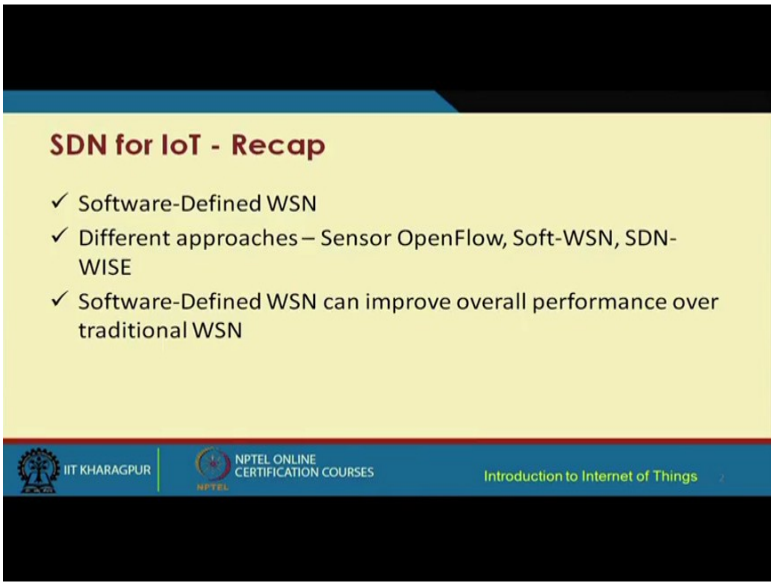
In the next part of the lecture we are going to talk about how IoT devices like mobile devices can exploit the use of SDN to make them efficient. With this we come to an end.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 36
Software - Defined IoT Networking - Part- II

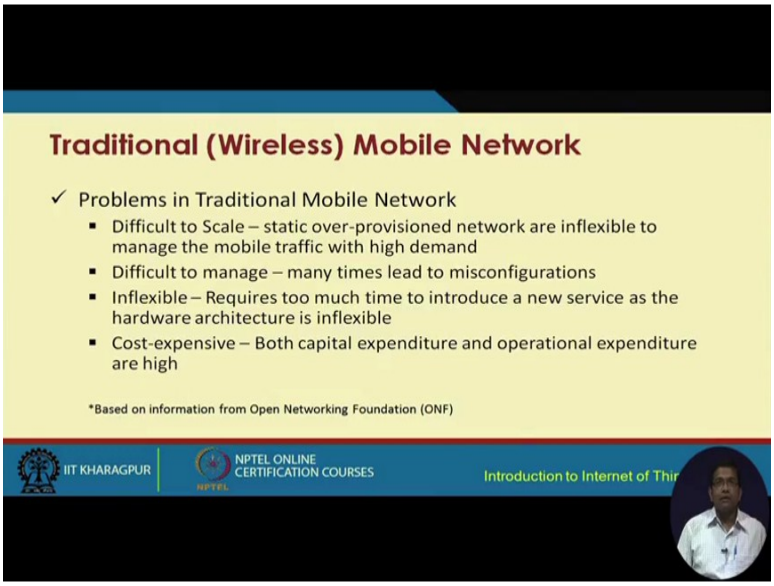
So, now we are going to discuss about software defined networking and and its use in IoT. So, here we are going to talk about how SDN can help in improving mobile networks specifically.

(Refer Slide Time: 00:39)



So, what we have already discussed in the first part of SDN for IoT lecture is that we have. So, a sensor networks and software defined networking can be used to improve the performance of sensor networks. So, we have different SDN approaches for WSN's and different approaches like Sensor OpenFlow, Soft-WSN, SDN-WISE are already available in the literature which can be used. Community can use it if they want to implement sensor you know SDN for WSN and we have also discussed about how software defined WSN can improve the overall performance of the network compared to the traditional WSN.

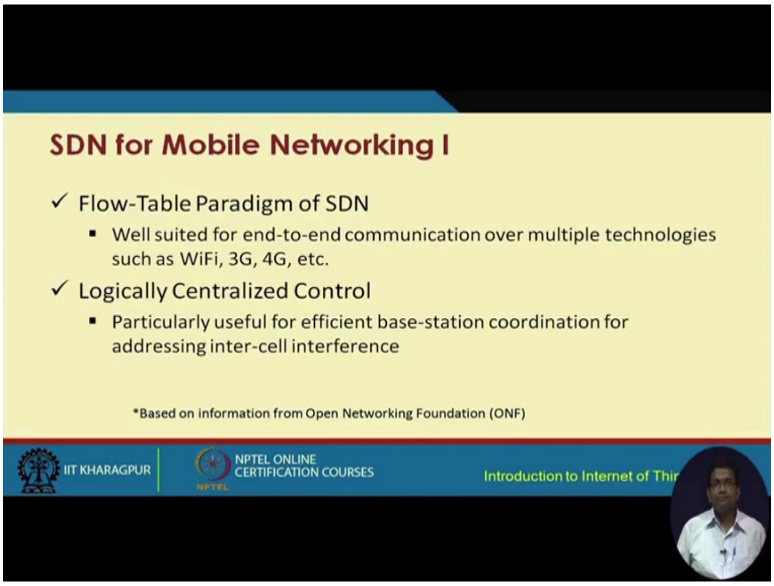
(Refer Slide Time: 01:40)



So, this is what we discussed earlier. Now, let us talk about the Traditional Mobile Wireless Networks. There are different problems in these Traditional Mobile Networks and these networks can be like Wi-Fi based networks. Mobile cellular networks or other mobile networks, the problems are with respect to scalability. So, you know what happens is each of these nodes in the networks if the nodes including the base stations access points etcetera, typically they are statically over provisioned you know. So, there is over provisioning in each of the nodes in these networks and they are inflexible to manage the mobile traffic with high demand.

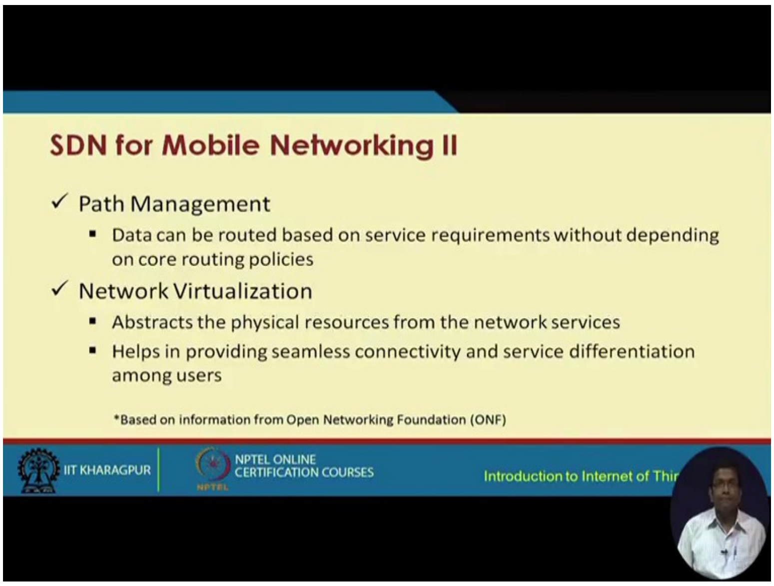
They are difficult to manage many times. This leads to misconfigurations. They are inflexible and requires too much time to introduce a new service as a hardware architecture is inaccessible and they are cost expensive, both in capital expenditure and operational expenditure terms because both the capex as well as the opex are very expensive are very high.

(Refer Slide Time: 02:55)



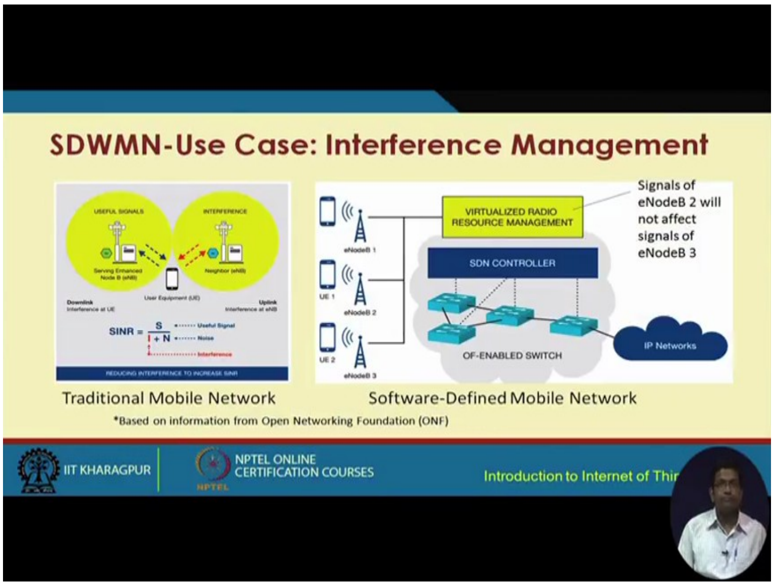
So, two things are important and this is this information has been adopted from the Open Network Foundation. So, two things are important when we want to adopt SDN for mobile networks. One is the flow table paradigm of SDN which is well suited for end to end communication over multiple technologies, such as Wi-Fi, 3G, 4G and so on so forth. The other one is the logically centralized control which is particularly useful for efficient base station, coordination for addressing intercellular interference. So, we are going to talk about each of these in slightly more detail in the next little while.

(Refer Slide Time: 03:41)



Other issues which are also important are path management which concerns basically data that can be routed based on service requirements without depending on the core routing policies and network virtualization which is about abstracting the physical resources from the network services. This helps in providing seamless connectivity and service differentiation among the users.

(Refer Slide Time: 04:07)

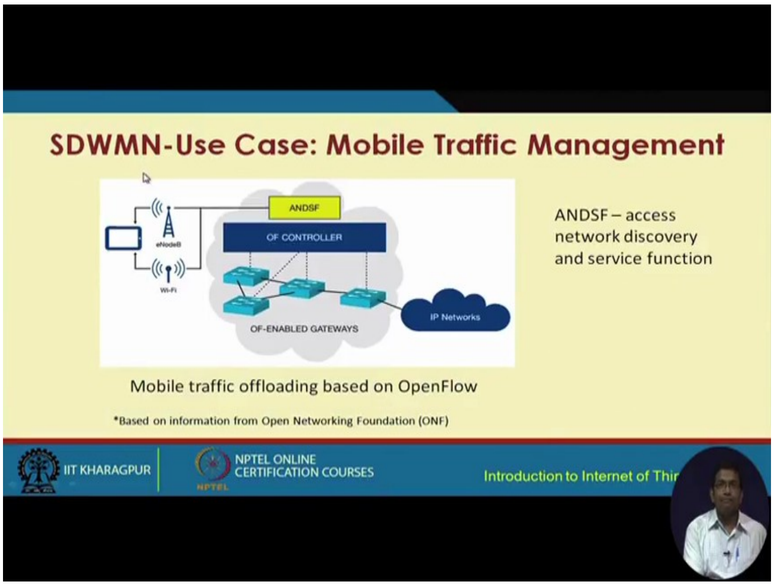


So, in a traditional mobile network, what happens is when a mobile equipment like this operates, it connects with a base station or an axis point for regular data. You know data back and forth between it and that access point and this particular node, it serves this particular access point, sorry this particular user equipment, but while it is doing so, it is also getting, it may also get affected by interference from another node. So, this red colored arrows basically shows the interference and the blue colored ones basically shows the regular data, transfer data communication.

So, there is this solution which is this SDWMN. It tries to address this particular problem of interference through the help of SDN. So, here what we see is the architecture of the software defined mobile network and as we can see over here, we have an SDN controller and the Virtualized Radio Resource Management Unit which basically takes care of interference with the problem of interference. So, this particular unit what it does is, it takes care of issues such as the signals of eNodeB 2 and the signal of eNodeB 3, they do not affect each other. That means, the signal of eNodeB 2 will not affect the signal of eNodeB 3 affect means through interference affecting through interference.

So, this is made possible through this Virtualized Radio Resource Management Unit which has been proposed in this particular protocol or the solution which is SDWMN and with respect to mobile traffic management.

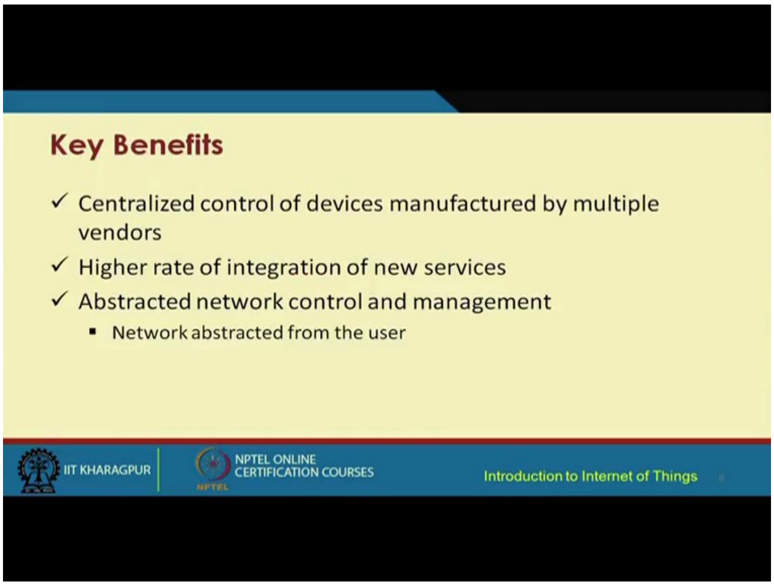
(Refer Slide Time: 06:27)



There is this unit which is the ANDSF, Access Network Discovery and Service Function Unit which basically takes care of it and this is done this way. So, we have the cellular as well as the Wi-Fi and the mobility. So, basically the what happens is when the user is moving, so the user can get first connected to the regular. You know Wi-Fi access point, then you know it might have better connectivity with the cellular network 3G, 4G and so on.

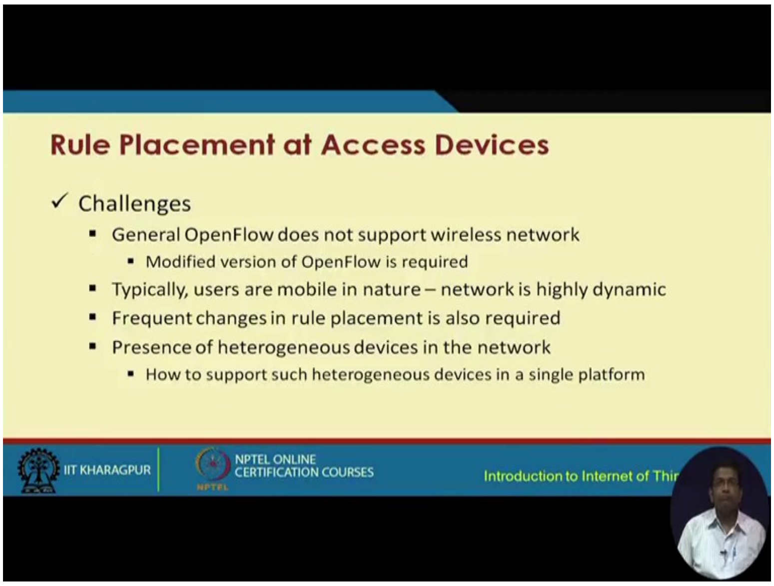
So, basically this particular solution basically takes care of it how to interoperate between these different different when the user is moving and is getting connected with you know and has different signals from different different devices from different networks, Wi-Fi network, 3G, 4G networks etcetera. How it is going to do this switching? So, the SDN basically comes to a rescue to solve this particular problem.

(Refer Slide Time: 07:35)



The key benefits of the solution is that centralized control of devices manufacture by multiple vendors is made possible. It is possible to have higher rate of integration of new services and abstracted network control and management is made possible through this particular solution with that option of SDN in these mobile networks.

(Refer Slide Time: 08:01)



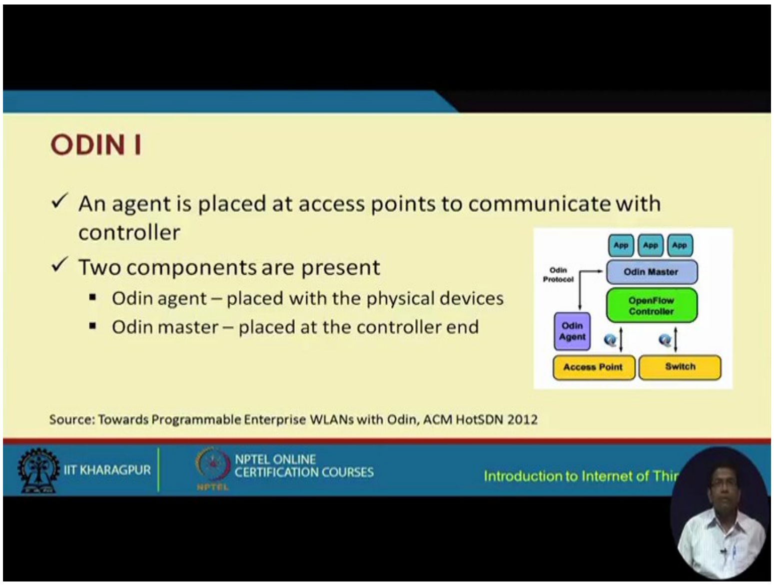
So, how so you know when we talk about SDN and in SDN based solution, it is about rules, flow rules and rule placement controller placement and so on. So, let us now look at how rule placement is made at the access devices in these networks. The challenges that are have to be addressed are that number one, the general open flow does not support wireless network. So, you know because it is general open flow does not do that. Some kind of a modification of the existing open flow is required. Number two, typically the users are mobile in nature and the network is highly dynamic. Third challenge that has to be addressed with respect to rule placement in these networks is that the frequent changes in rule placement is required and the presence of heterogeneous devices in the network might is a reality in these scenarios.

So, basically you know what happened at that last point, what it says the last challenge what it says is different types of heterogeneous devices having different configurations supporting different you know vendor specific solutions and protocols and so on exist in a realistic mobile based IoT network. So, how to support such heterogeneous devices in a single platform? So, these are the challenges that have to be worked upon in order to deal with the rule placement issue.

(Refer Slide Time: 09:36)

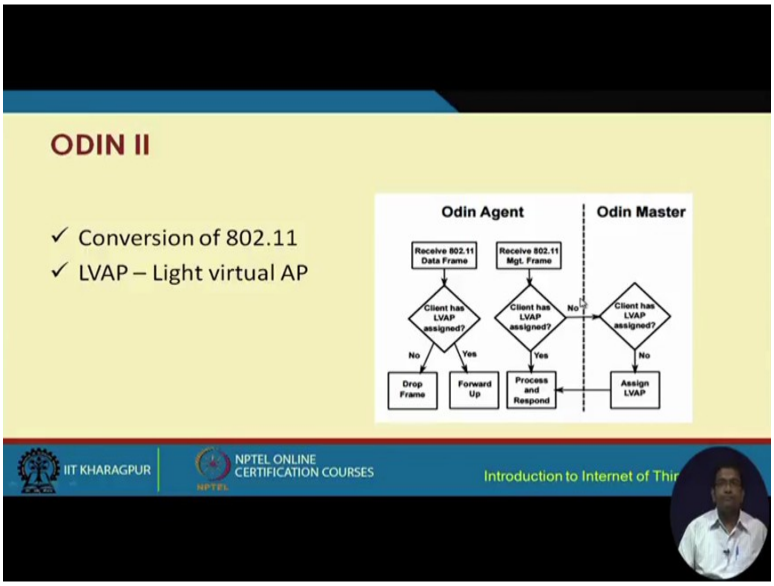
So, there are different approaches or different solutions that have been proposed for it. Number one is ODIN, number two is Ubi-Flow and number three is Mobi-Flow. ODIN basically proposes the use of an agent. It is an agent based solution, agent based architecture.

(Refer Slide Time: 09:48)



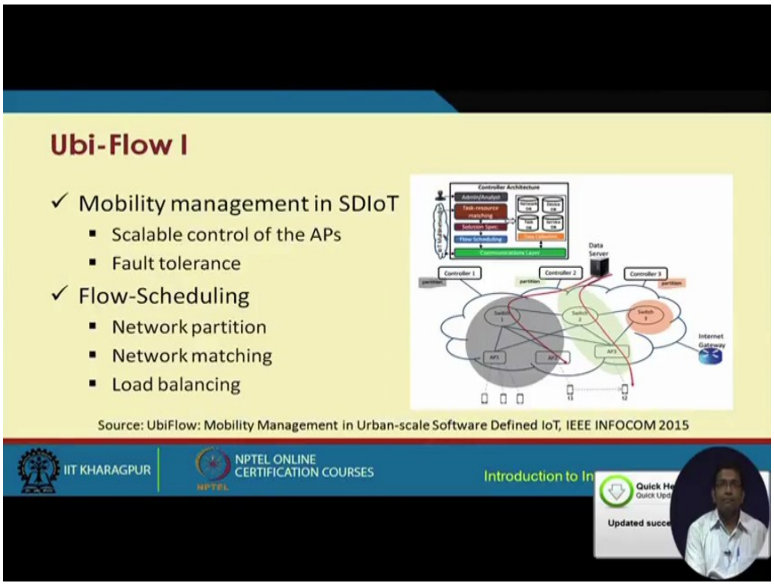
So, here an agent is placed at the access points to communicate with the controller. So, this is the ODIN agent and there is the ODIN master. So, we have the ODIN agent which is placed at the physical devices at the access point. For example, the ODIN master which is placed at the controller and now this is this hand shaking between the communication between the ODIN agent and the ODIN master that is taken care of by this ODIN protocol.

(Refer Slide Time: 10:24)



So, it uses the communication between the ODIN agent and the ODIN master. The corresponding flow diagram, the flowchart is shown over here. We do not need to understand in detail, but it is given for those who might be interested to understand it nonetheless and so, basically it is a handshaking that goes on between this ODIN agent, add the access device and access point and the ODIN master at the controller that makes ODIN function.

(Refer Slide Time: 10:57)



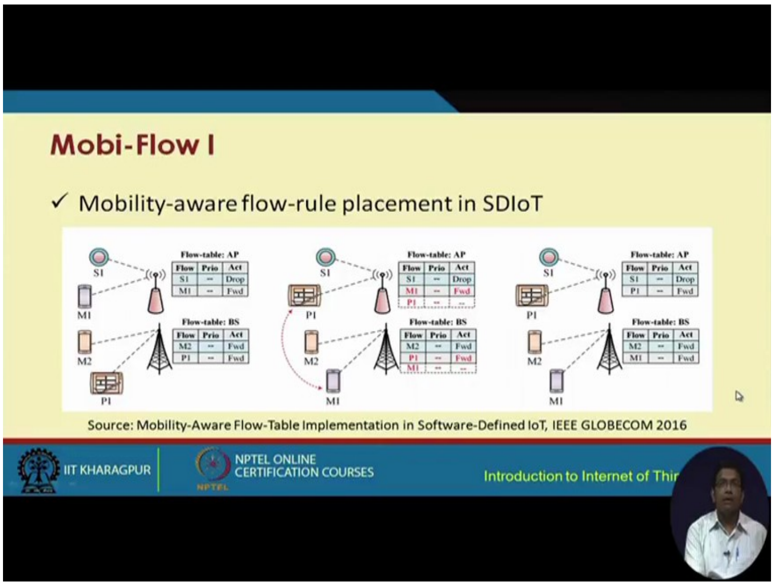
Now, let us look at the second solution, the Ubi-Flow solution which was published in infocom very recently in 2015 only, 2 years back.

So, here there are two main parts of the solution. One takes care of Mobility Management and the other one takes care of Flow Scheduling. Mobility management takes care of issues such as you know how to have scalable control of the access points issues, such as fault tolerance. That means, if some component goes down, then what happens you know how can the network still function and the other one is the flow scheduling which has three parts. First is partitioning this entire network into multiple partitions, no fragmenting this entire network into multiple partitions and over here we have shown those three partitions through three different color shades i.e. grey, light green and orange.

So, we have three different partitions shown over here network partitions and after this network partitioning has happened, then you know network matching has to be done. So, let us say that this particular mobile device receives a particular packet. So, then what it is going to do? It is going to perform, it is going to execute this network matching, network matching algorithm. What that network matching algorithm is going to do is, it is going to check that which of these network partitions should handle this particular packet.

So, then it will be sent to that particular partition for further handling and load balancing basically takes care of it you know. So, you know how the network matching and load balancing will be done together. So, the load balancing is going to take care of issues, such as that one partition should not get too much loaded while the other partition is under loaded and so on. So, this is what the load balancing is going to do.

(Refer Slide Time: 13:09)

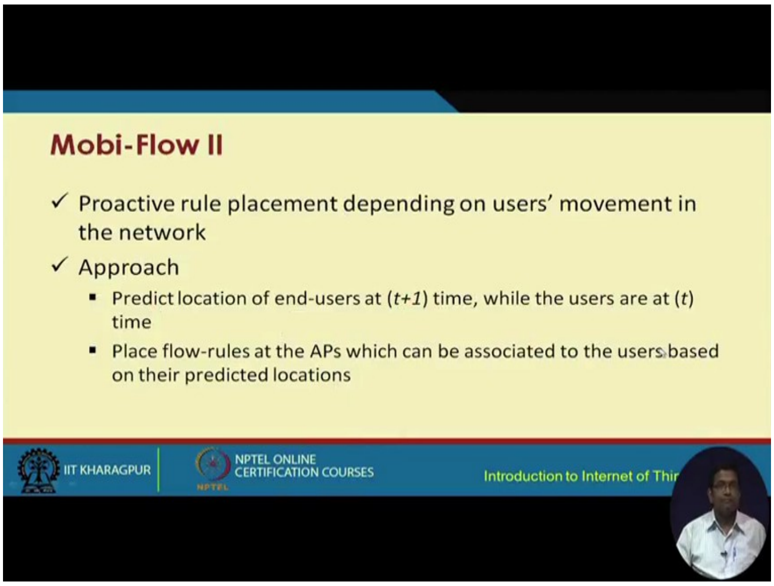


Now, let us look at the third solution that I was talking about the Mobi-Flow and this paper was published in IEEE Globecom, 2016 and this is the solution Mobi-Flow solution was proposed by us in the SWAN group and the mobility. So, Mobi-Flow basically gives a mobility aware flow, flow rule placement for mobile based IoT solutions, mobile place based IoT systems. So, let us look at these three scenarios over here. So, here we have different nodes S1 M1 connected to this particular access point. M2 and P1 connecting to another access point and their corresponding flow tables are shown here, the corresponding flows tables corresponding to this particular access point and this particular access point of the base station, the corresponding flow table is given over here. It is very easy to understand this part.

Now, let us see, let us say that the nodes M1 and P1 have interchanged their positions. Let us assume a very simple scenario, where M1 and P1 have interchanged their positions and the current situation looks like this. So, essentially you know what should happen is, we will have something like this. The another flow rule has to be added in the flow table corresponding to this particular access point and the base station in this particular manner, but at the same time we also know that flow table spaces are very limited.

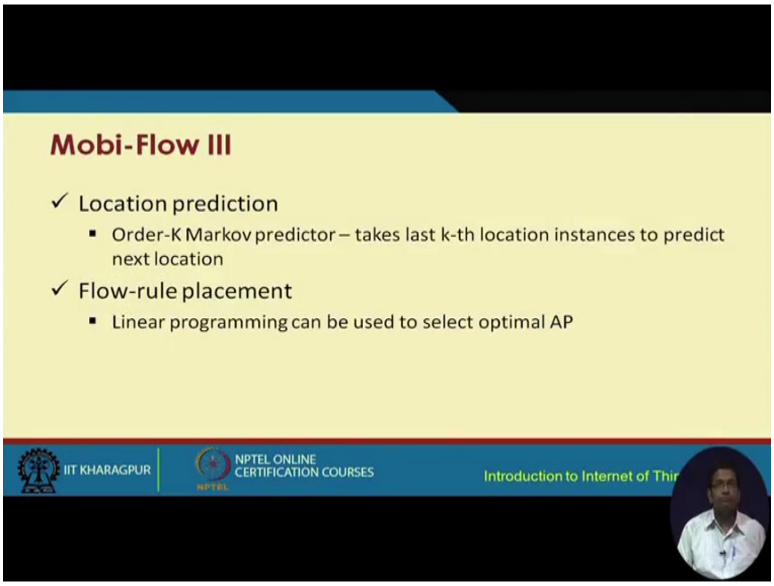
So, we cannot simply have these flow tables grow with the addition of these flow rules. So, you know what essentially has to be done is the scenario like this. So, how can we do it, this is what Mobi-Flow talks about.

(Refer Slide Time: 15:02



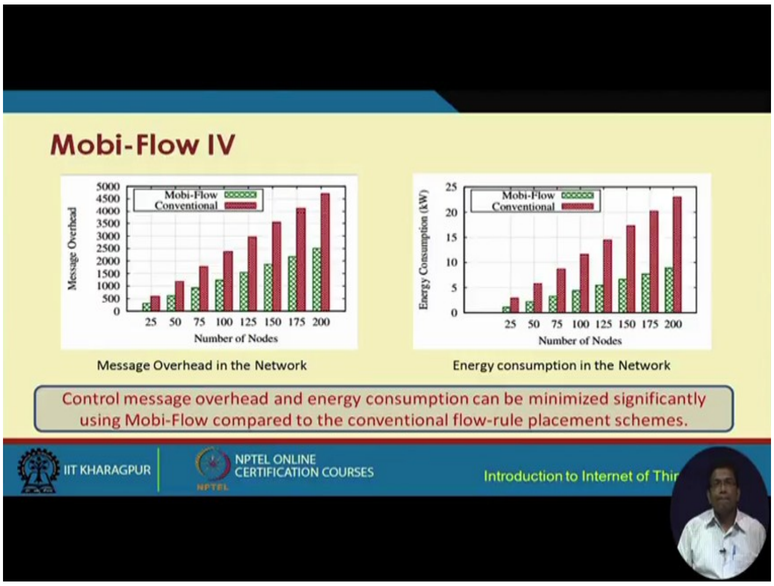
So, Mobi-Flow gives a proactive rule placement scheme depending on the users movement in the network and when we talk about such a scheme, you know what is very important to have some kind of prediction of the location of the end users at the next time instant give you the data of how the user was moving till a particular time instant.

(Refer Slide Time: 15:36)



And then, placing the flow rules at the access points which can be associated to the users based on the predicted locations, location prediction, this is done in Mobi-Flow using something known as the Order-K Markov Predictor which basically takes the last k th location instances to predict the next location and the flow rule placement which basically is a linear programming based solution that is used to select which access point is going to be the optimal one.

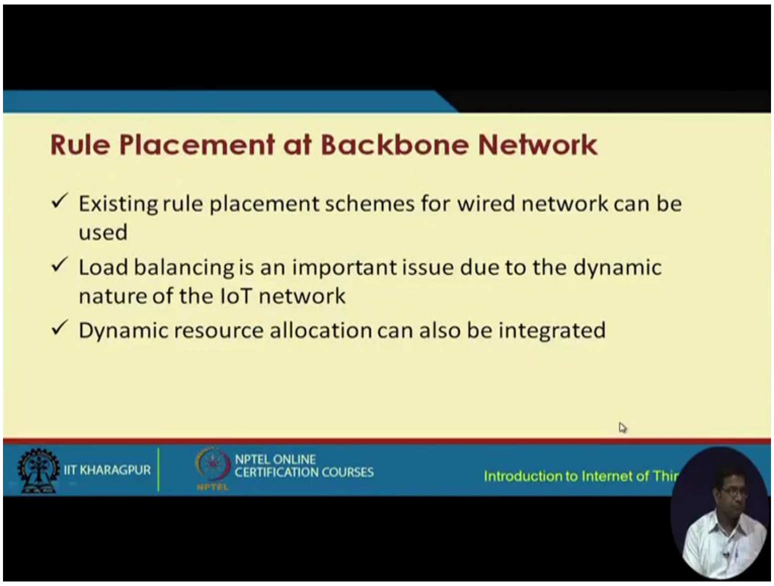
(Refer Slide Time: 16:01)



So, for further details the difference of Mobi-Flow was given in 2016 Globecom paper and if somebody wants to have more insight about how Mobi-Flow works, so one needs to go through that particular paper, but I would like to summarize by giving a a summary of the results of comparison between Mobi-Flow and the conventional solution.

So, what we have is with respect to message overhead and energy consumption, Mobi-Flow performs better compared to the conventional network, conventional solution and this is quite evident from these two plots. So, control message overhead and energy consumption can be minimized significantly using Mobi-Flow compared to the conventional rule placement schemes.

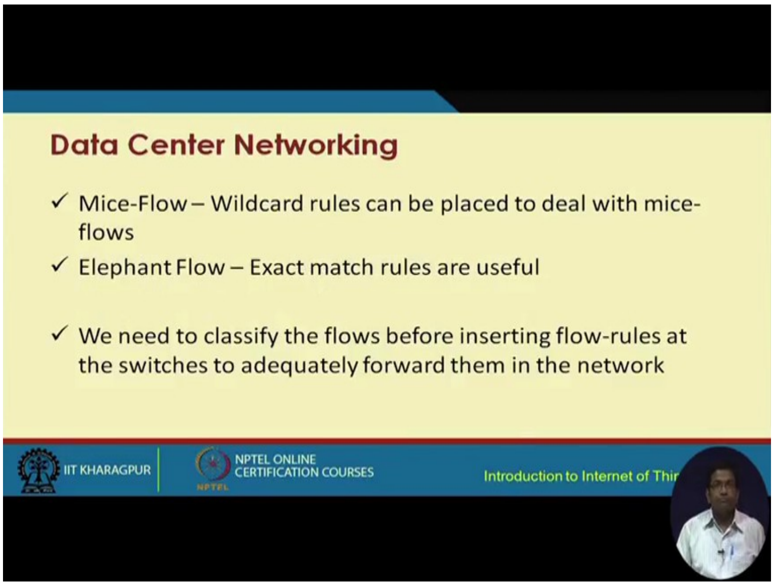
(Refer Slide Time: 16:59)



So, next we have to take care of how to perform rule placement at the backbone network. So, the existing rule placement schemes for wired networks can be used over here because most of the backbone networks are have a topology and the structure. The overall architecture is similar to that which exists for wired networks.

So, we can use the existing rule placement schemes for wired networks over here as well for the backbone network of IoT and the load balancing is an important issue due to the dynamic nature of the IoT network. So, dynamic resource allocation can also be integrated.

(Refer Slide Time: 17:39)

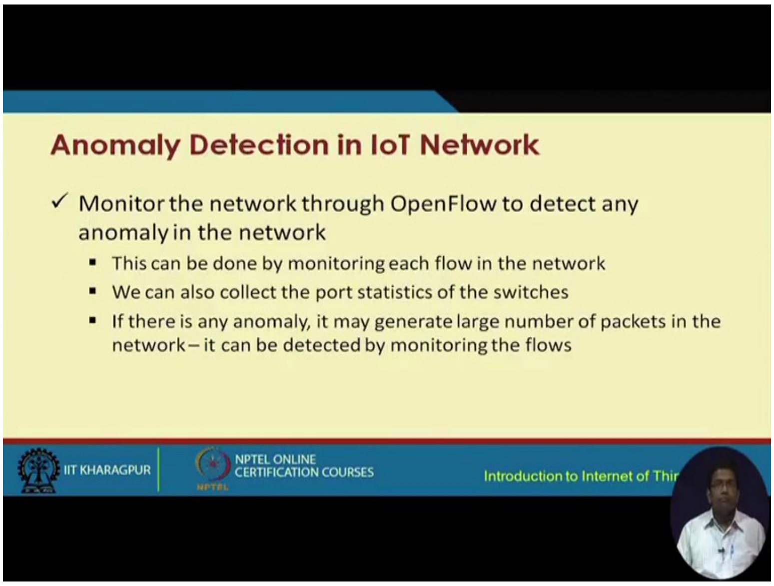


So, another very important thing that we have to remember in this particular context is the Data Center Networking. So, there are two types of flows that occur in Data Center Networks. So, Data Center Networks basically you know here we are talking about implementation of data center networks with the help of SDN.

So, typically two different solutions of adoption of SDN are in data center networks. So, here we have typically two types of flows that are observed. One is the Mice-Flow which are basically you know small flows and the other one is Elephant-Flow which is basically you know large scale flows where big volumes of data are coming, big sized data are coming and so on and small flows, Mice-Flows where small sized data are coming. So, here what is suggested is for the Mice-Flow wildcard rules can be placed to deal with these flows, the wildcard rules and for the Elephant-Flows what is required is to have exact match of the rules.

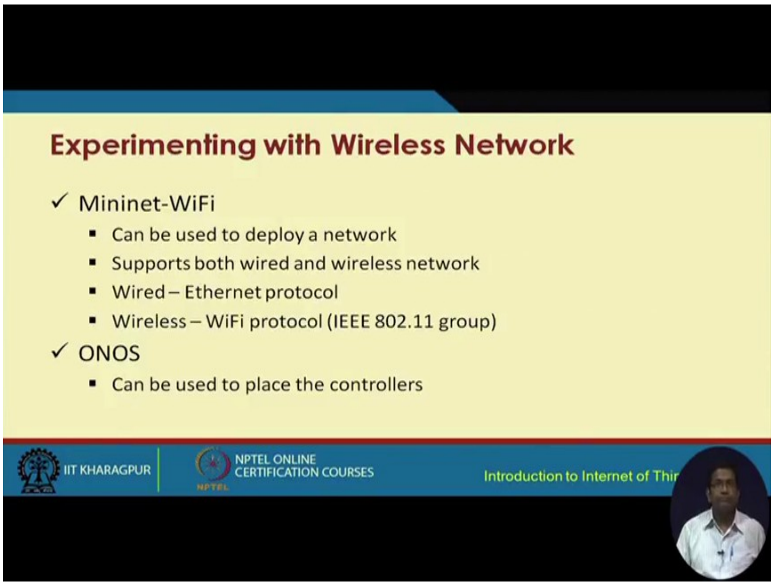
So, we need to classify the flows before inserting the flow rules at the switches to adequately forward them in the network. So, if it is an elephant flow, you know we have to have exact match. If it is a Mice-Flow, we will go for a wildcard match. Anomaly detection can also be performed in IoT network using SDN or open flow.

(Refer Slide Time: 19:07)



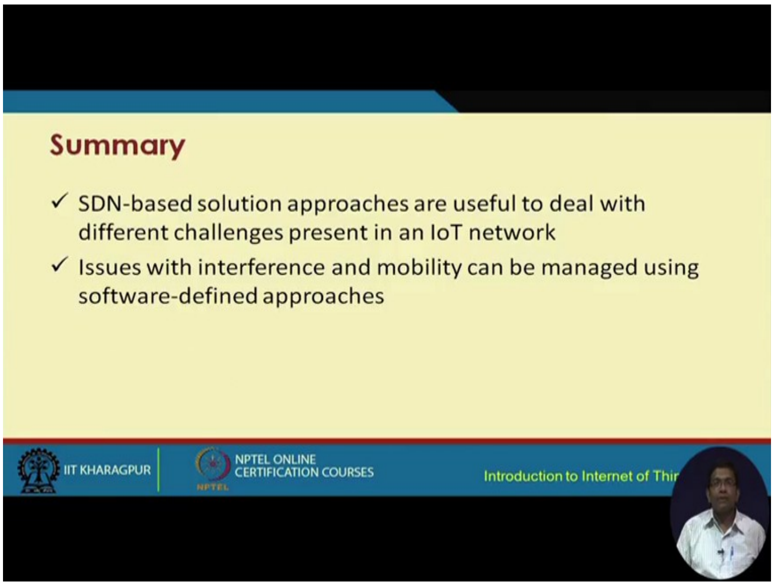
So, here you know it is required to monitor the network through open flow to detect any anomaly in the network which can be done by monitoring each flow in the network. It is also possible to collect different port statistics at the different switches and thereby from these statistics, you know anomaly detection techniques can be implemented and different anomalies can be found out.

(Refer Slide Time: 19:38)



Now, what is required is to experiment with these wireless networks. So, what are the different platform that are available? So, Mininet traditionally did not have any wireless support, but recently there is this Mininet-WiFi that is available which can be used to deploy a network support. Mininet-WiFi can help support both wired and wireless network. Wired implements the Ethernet protocol and Wireless implements 802.11 class of protocols. So, this is one platform that is available. Mininet-WiFi, the other one is the ONOS platform which can be used to place the controllers. ONOS basically helps in placement of the controller.

(Refer Slide Time: 20:21)



So, it helps to solve the controller placement problem. So, again to sum up SDN based solutions are useful to deal with different challenges present in an IoT network and in the first part of it, we talked about IoT in the context of sensor networks and small power, you know small devices, small IoT devices and in the second part, we talked about IoT in the context of mobile networks, mobile devices and so on and we have talked about three different solutions. One is the Ubi-Flow, Mobi-Flow and ODIN. These are the three different solutions that are available recently to support SDN for mobile IoT networks.

So, there are different issues of interference and mobility management which have to be taken care of in these SDN based approaches to SDN based approaches to IoT. So, interference is a very common thing, a very important problem that has to be addressed so and mobility as well because mobility is something that occurs in any IoT network and particularly the mobile based IoT networks.

So, with this we come to an end and we will stop here for the, we have understood that how SDN can be used for implementing IoT networks and making the IoT networks much more efficient.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 37
Cloud Computing- Fundamentals

So this lecture is on Cloud Computing, and this is the first lecture on the series of cloud computing. So, the first one will be on fundamentals. So, here in this lecture I am going to speak about some of the basic motivation behind cloud computing, particularly from the use of cloud computing in internet of things. Then about some of the basic models of cloud that are popularly used and also how the cloud can be deployed in different environments and the models there of. So, this particular lecture is focused on these specific issues.

So, before we start I would like to mention a few different things. So, the first thing is that why do you need cloud. So, let us try to understand this thing why do we need cloud and the second thing that will try to understand is why do we need cloud specifically for internet of things and that will basically justify why we are devoting a few lectures on cloud computing in a course on IoT. So, the second one will come next, but let us first look at what is cloud. So, cloud computing is all about using computing as utility

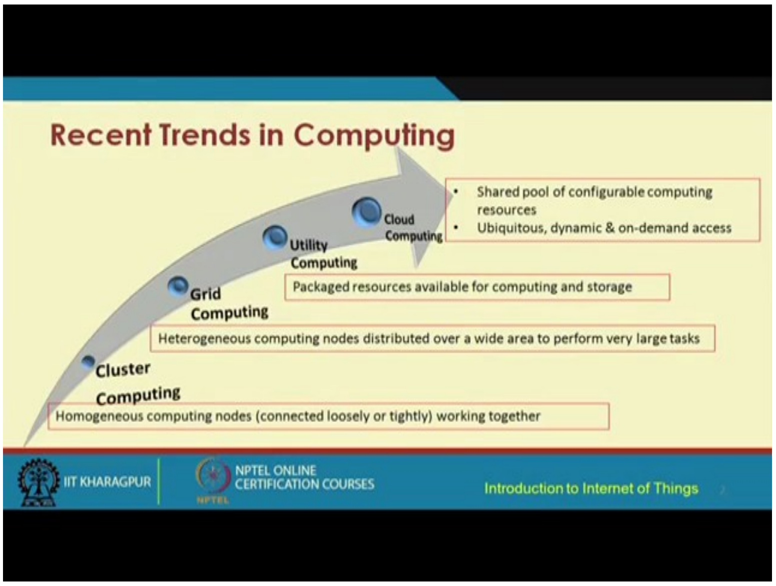
So, we all are users of different utilities; utilities such as electricity, utilities such as water resources and so on and so forth. So, electricity water supply etcetera are utilities which we use first of all we have to subscribe to those utilities then some connections will be given at our home for those utilities. Then there will be some meter which is going to measure how much units of electricity or water we are using at our home and based on our units of usage we are going to be finally built at the end of the month for the use of these resources.

So, what did we see that if I have to use electricity at my home if I have to use water at my home it is not required for me to be bothered at all about deploying the necessary infrastructure for generation of electricity for the transmission of electricity similarly the pumping out of water from river or ground or the distribution of the water I do not I do not really have to be worried at all about this.

So, I subscribe to these utilities I will be given a connection at my home for these utilities then based on the units of usage of these resources electricity water etcetera at the end of the month I will be billed for this I will be billed for this. So, what did we see that I do not really have to bother about how the electricity or water was generated or pumped out how it was distributed? So, I do not need to be worried about all I need to be worried about is whenever I required I will be using it and at the end of the month I should be paying for the units of usage.

So, this basically can serve as a motivation behind why cloud computing is required in the same way as water is a utility, electricity as a utility people thought about can we have computing as utility what does it mean computing as utility computing means what computing means hardware resources like servers workstations which again include processors which can do certain computations etcetera memory storage and so on. So, these computational resources hardware plus software resources plus development platforms; so, all these things offered as utility why do we need, because that will have some business value that will save some cost and it also has certain advantages and this is what we are going to learn in this particular lecture.

(Refer Slide Time: 05:02)

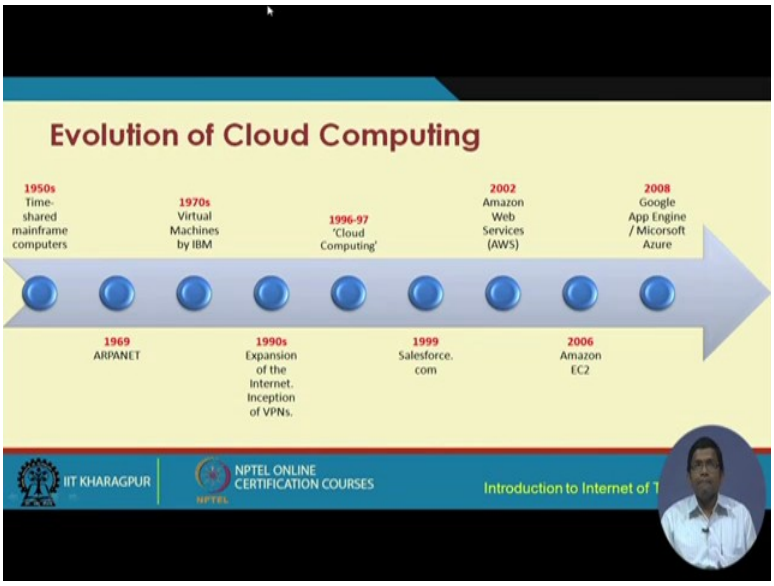


So, first let us have a quick glance through how computing evolved over the years. So, you must have already heard about cluster computing, grid computing at least these 2 you must have heard about. So, cluster computing is basically you know having some kind of computing nodes connected together in the form of a cluster. So, the cluster as a whole which can be loosely or tightly connected the cluster as a whole would be accomplishing some computational job which will be; it will be executing some computational job. So, this is cluster computing grid computing is sort of like a wide area kind of heterogeneous computing platform which will be performing large volumes of tasks or tasks which are large in size then we have the utility computing where this resources the computational resources are packaged for delivering as utility for use by consumers as utility.

So, this is the whole premise of how utility computing evolved and then we have this cloud computing which was basically sort of like an integration of the concepts from all these com cluster computing distributed sorry grid computing and utility computing their advantages put together in order to have this new model of computing which is known as the cloud computing. So, in cloud computing we have shared pool of configurable computing resources shared pool of resources and whenever it is required wherever it is required dynamically these resources will be offered will be offered to the users as service on payment.

So, this is like a scalable kind of model that that has been conceptualized over all these cluster grid and utility computing models.

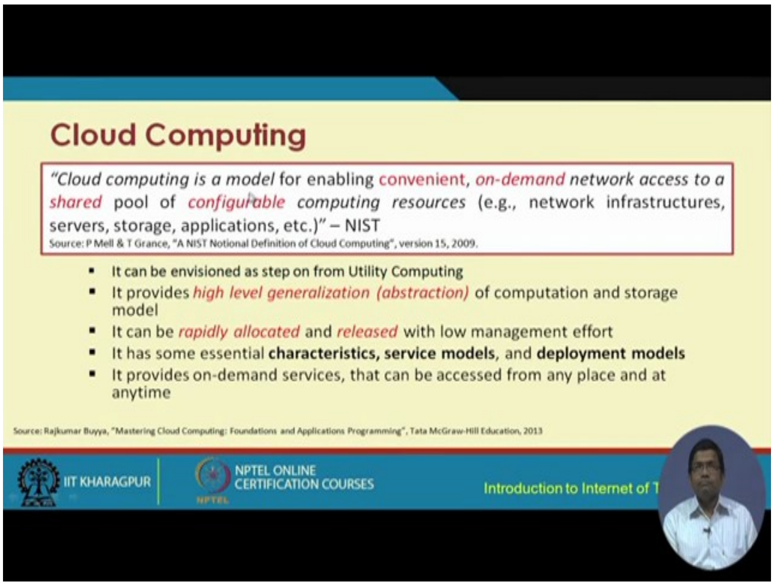
(Refer Slide Time: 07:24)



So, you know cloud is more or less a very recent kind of phenomenon it started in the mid 1990s and in the last few years it has become even more popular there are different commercially available cloud platforms that are there people are still using it companies are subscribing to these cloud services, but going back in the 1950s people were more concerned about time shared mainframe computers in the 1960s ARPANET and the like oriented network based services became popular virtual machines became popular in 1970s; 1990s the internet was expanded virtual private networks were formed.

And in the late or mid 1990s onwards cloud computing came into being popularity has been more in the last couple of years of cloud computing different platforms offering software you as utility platform as utility infrastructure, as utility are offered by different companies such as sales force dot com, Amazon web services, Amazon EC2, Google app engine and so on. So, these are the different companies which are basically daily offering these different services as utility.

(Refer Slide Time: 08:57)



Now when we talk about cloud computing NIST has done quite a bit of work on in cloud computing it. In fact, has some literature and as per that literature of NIST cloud computing is defined in this particular way I will read it out for you it is there in front of the slide in front of you in the slide and for the benefit of everyone. Let me read it out for you cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources example network infrastructure servers storage applications etcetera.

So, there are few key words that will drill down for the convenient network access. So, whenever it is required for me at any time of the day at any time of the month whenever it is required conveniently I should be able to get network access to the to these different resources that we just went through that we just gone have gone through on demand on demand means that whenever it is required I should be able to on my demand I should be able to get access to these resources. And there is a shared pool of resources which are configurable shared pool. That means, that these servers storage etcetera, etcetera, which will be shared all across and the computing platform is configurable with respect to these network infrastructure you know servers, etcetera.

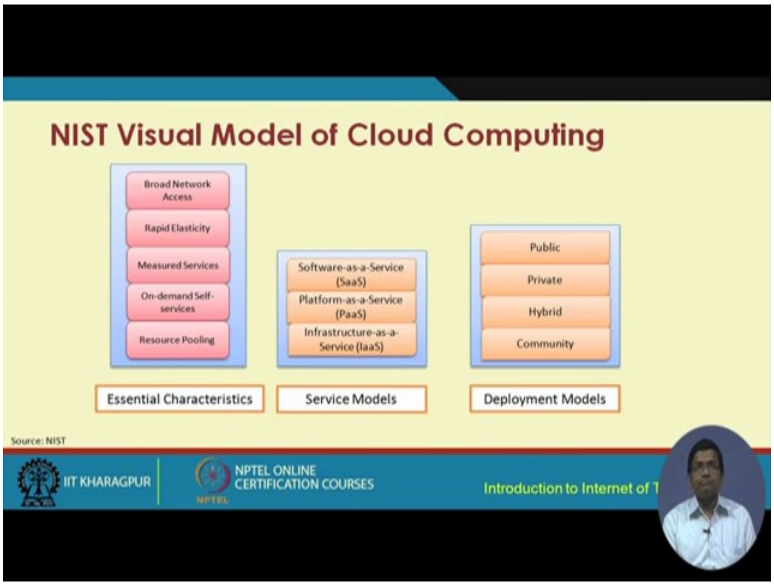
So, basically it might so, happen that you know as a user my job as a cloud user my you know computational job is getting executed to me it I will get a feeling that it is get getting executed at my dedicated machine that has been given to me by the cloud platform, but in actuality physically maybe there are multiple servers which are geographically separated from one another which are together being pooled to execute different parts of my job. So, this is basically you know to me it is like a single entity which I am using, but in the back end there is so much of seamlessness that is there that I would not be able to understand that how and where and when things are getting executed.

I in fact, do not need to be worried at all about it of course, I would tell you that it is not that I do not need to be completely worried cloud computing also has some privacy security concerns as well. So, will you know for this course we are not going to understand what are these issues, but there are indeed certain issues, but we will consider that you know there is no such issue and you know I do not really need to be worried about how when and where my computation job that I have is getting executed, but to me I will get a feeling that I am paying for it and it is getting executed at my end actually it is not happening that way it is because of virtualization that I am getting such a feeling.

So, I will talk about it in more detail later on. So, cloud computing is sort of like a step ahead of utility computing it provides abstraction or high level generalization of the computation and storage software platform etcetera from and this kind of abstraction is made available to the end users for use on a paper use basis the resources are in a cloud platform rapidly allocatable and they can be also released whenever it these resources are no longer required and that can these can be done with low management effort.

So, there are some essential characteristics something called the service models and the deployment models which we are going to go through of cloud computing. So, what are these essential characteristics broad network access is one.

(Refer Slide Time: 13:20)

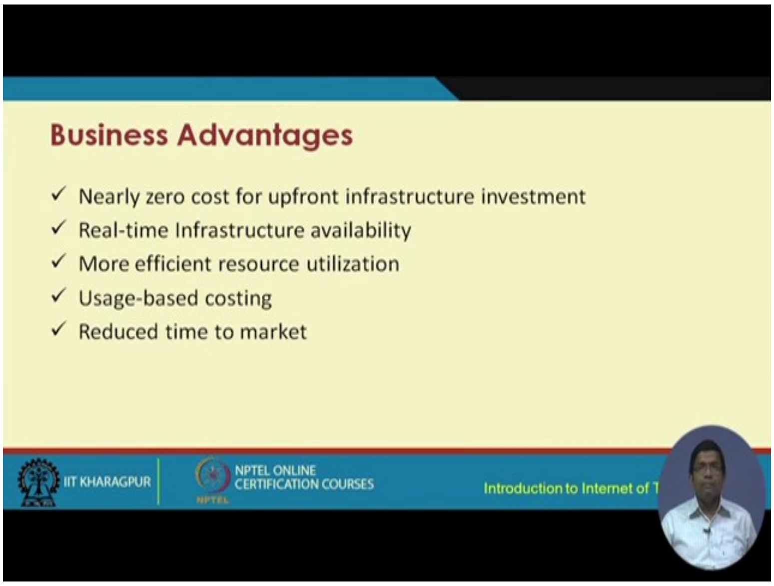


So, this network you know access is offered in such a way that from anywhere and from anywhere in the world geographically even if I am distributed at different locations my company has different. So, I would still be able to get access to these cloud resources. So, these computational resources rapidly elasticity means that as and when required you know if I require more I would be able to scale up. And I should be able to get these computational resources if I require less I should be able to scale down. So, this dynamic scaling has to be made possible through cloud.

Third is measured services paper use you know. So, I would be paying for the units of utility cloud utility. That means, the computational utility that I am using on demand self services. So, whenever required I should be able to subscribe to and be able to get access to these services resource pooling means that you know if a particular server is not able to physically. You know physically give the services as per requirement then the services can be a can be obtained from other servers, other physical computers by pooling resources from them. So, these are some of these essential characteristics of cloud computing and there are different service models the very popular software as a service platform as a service and infrastructure as a service in short these are popularly termed as SaaS; SaaS, PaaS and IaaS and in terms of deployment there are different models like the public cloud, private cloud, hybrid cloud and the community cloud.

So, we will talk about each of these service models and deployment models later on. So, what are the businesses advantages I told you that cloud has certain business advantages.

(Refer Slide Time: 15:30)



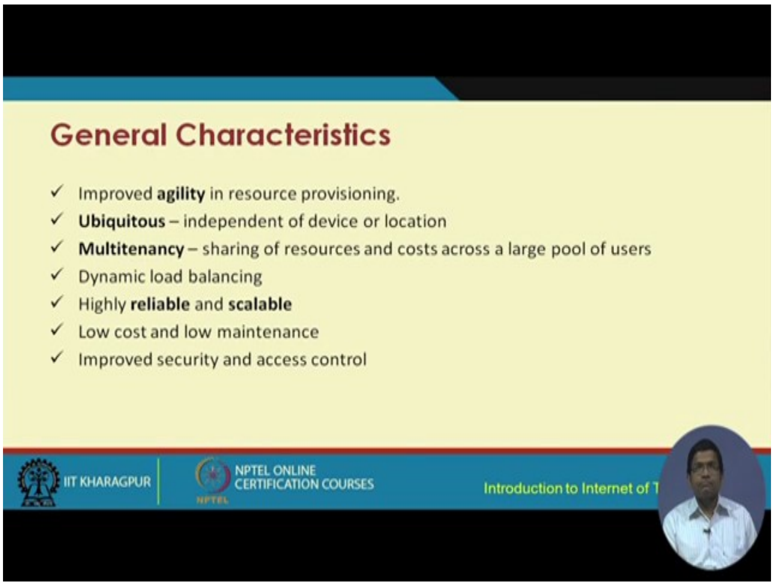
So, without any upfront infrastructure investment a company who has computational requirements they do not have to go and buy their own servers for instance and use them, but within almost 0 cost of infrastructure investment in terms of procurement deployment etcetera the you know they should be able to get access to this computing resources on demand on whenever it is required in a ubiquitous manner.

Real time infrastructure able ability means that the infrastructure is going to be made available for real time use at any time the resources are going to be made available and will be made available for real time access more efficient resource utilization. So, these resources will be utilized in a more efficient manner usage based con costing is another thing. So, usage based costing means based on how much I am using these resources I would be billed for those units only reduce time to market, because you are not basically investing time.

And of course, money for procurement for initiating the procurement for process tendering, then you know getting all the infrastructure buying them the delivery time etcetera, etcetera and then starting to use. So, you are cutting down on the time to market of the product that the company is building, because whenever you require you are getting access to your computational resources over the internet at any time.

So, basically we have not you through the use of cloud computing we have not spent too much of time on the procurement of these computational resources, which otherwise traditionally used to happen and that would kill significant amount of time in business.

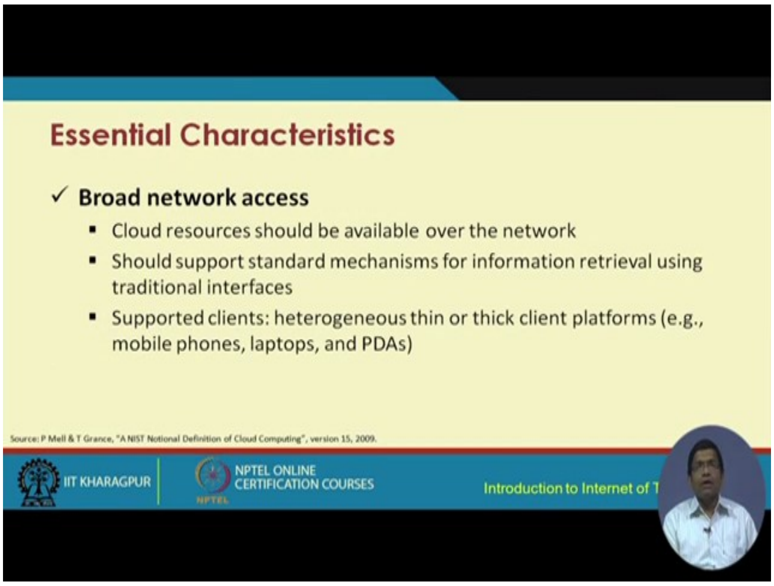
(Refer Slide Time: 17:47)



Some general characteristics improved agility in resource provisioning is one this I do not need to explain explain further ubiquity independence of device or location multi-tenancy which basically talks about sharing of resources and costs across a large pool of users. Dynamic load balancing means that the computation or even communication load it would be it is possible through the cloud model to be able to dynamically balance the load throughout the entire cloud platform cloud system. This cloud model is highly reliable, because physically if some network some computational resource has gone down or is broken or is not available for whatever reason there are other resources which can be easily pooled into and be made available to the users.

So, it is highly reliable and is scalable likewise. So, for the same reasons this is scalable as well and cloud also comes with low cost and low maintenance for the company the users of the company which is investing on in which was traditionally investing on infrastructure and improved security and access control as well. So, you know. So, these are some of the different characteristics of cloud computing.

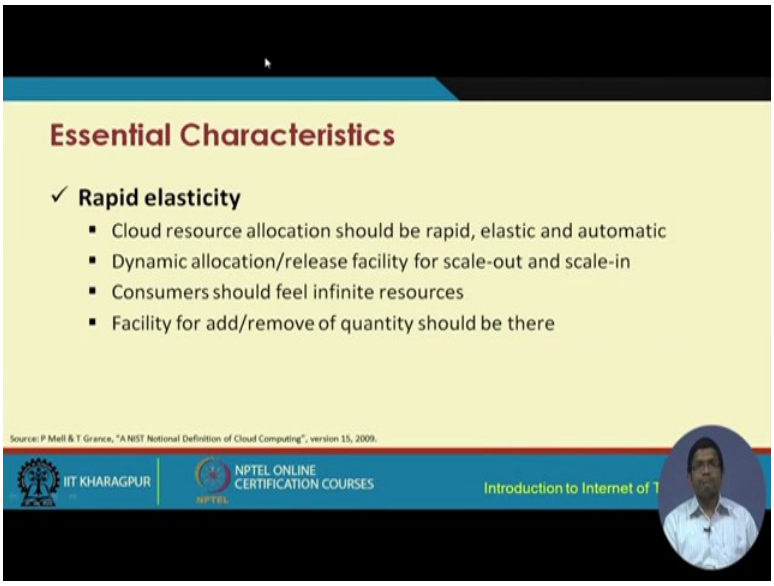
(Refer Slide Time: 19:11)



So, let us start with the essential characteristic the first one is the broad network access cloud resources should be available over the network and this is what is happening over the internet the cloud resources are man made available. And it should support the standard mechanisms for information retrieval using traditional interfaces. For example, different clients could be used different types of clients whether thick client the thin clients or mobile phones laptops etcetera these all are supported in a cloud platform.

So, basically what is going to happen you can very easily you can use thin platforms and it is like a bare basic terminal which will be you can simply have to you have to buy those low cost cheap bare basic terminals the thin clients etcetera. And the computation, the resources are going to be made available to you through the cloud platform you simply need to have some network access the broad network access in the form of internet or the like and should be able to connect to the cloud in order to get access to those resources.

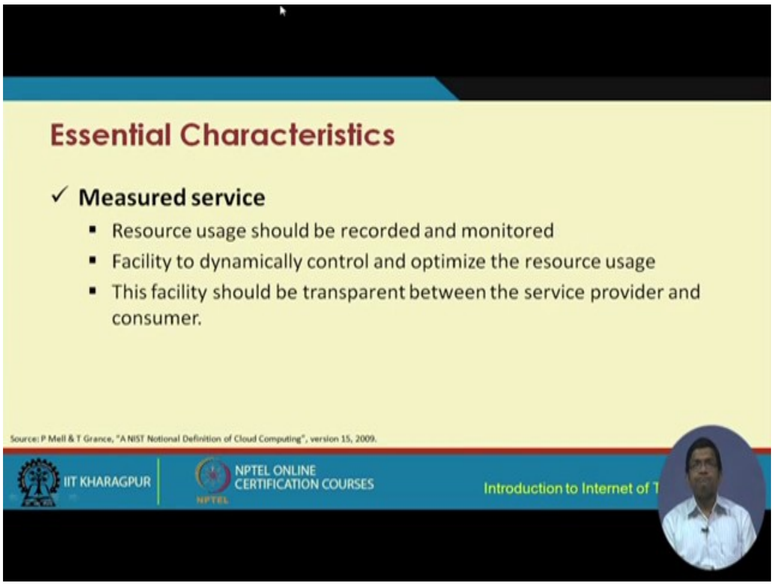
(Refer Slide Time: 20:23)



Rapid elasticity; so, cloud resource allocations should be rapid elastic and automatic dynamic allocation and release of facility for scaling in and scaling out of resources should be made possible. So, whenever additional resources are required you know it should be able to you know the cloud should be able to scale out. That means, increase the scalability of these resources. And whenever it is no longer required scaling in should be made possible by the release of these resources to the consumers. Consumers feel that it is a highly elastic system seamlessly things are integrated in such a way that the consumers feel that they have access to infinite resources and the and there is facility for adding or removing of quantity should be there in cloud.

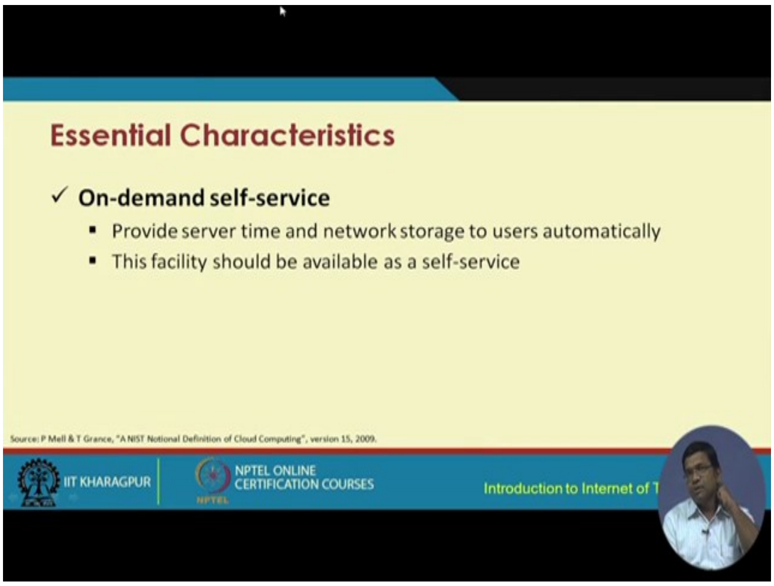
So, whatever you know if you need more quantity or if you need less quantity the addition or the release of resources to reduce the number should also be made available and this is the property of rapid elasticity. So, elastically we should be able to expand. Elastically we should be able to reduce and release resources through the cloud model.

(Refer Slide Time: 21:47)



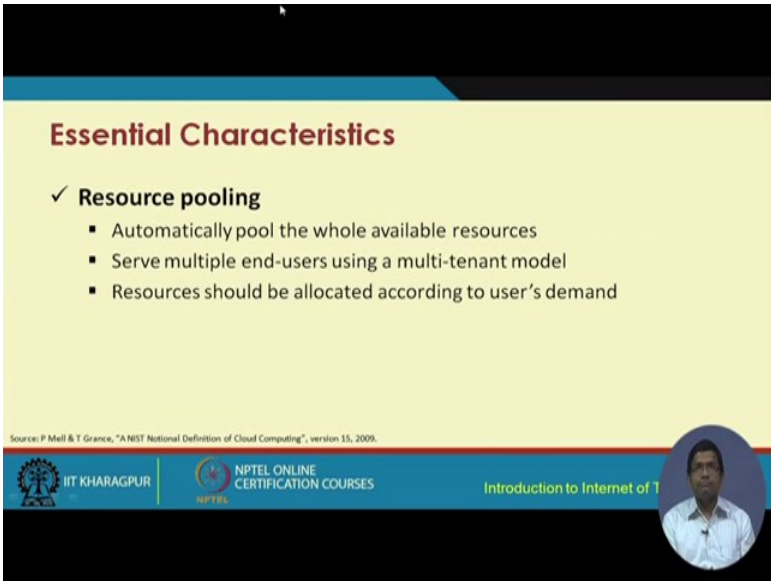
It is a measured service resources and their uses would be recorded and monitored. So, the use of these resources should be recorded and monitored and at the end of a particular time duration maybe a month. So, the cloud service provider is going to send out a bill to the end user in order for them to be able to pay for it. So, this can also be done at the same time you pay immediately, and then get access to your resources immediately as well. So, there should be facility to dynamically control and optimize the resource usage and this facility should be transparent between the service provider and the consumer.

(Refer Slide Time: 22:34)



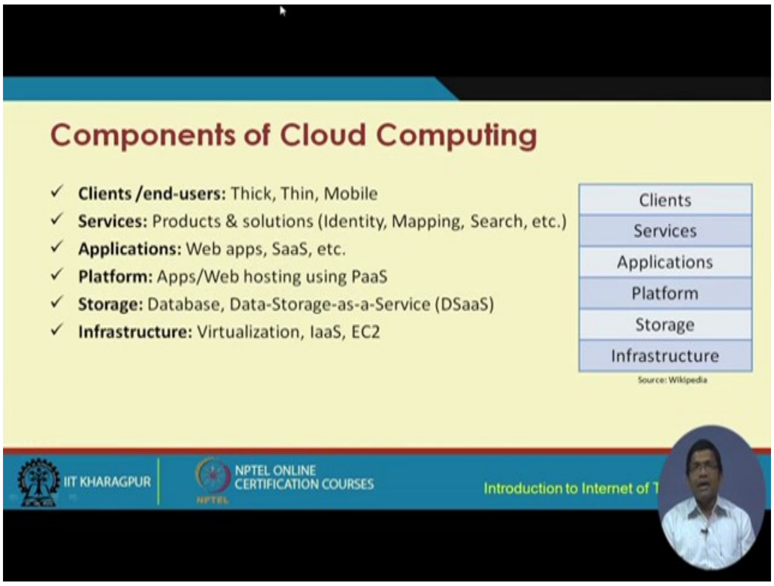
On demand self service, self service means whenever required the user should be able to get access to this resources through a self service manner. And cloud should be able to provide the server time and network storage to users automatically on demand whenever it is required.

(Refer Slide Time: 22:55)



Resource pooling means that it is sort of like a multi-tenancy model, where there are multiple end users and automatically as per the requirement the whole available resources would be made available will should be made automatically available. And should be pooled from all these available sources the resources should be allocated according to the users demand.

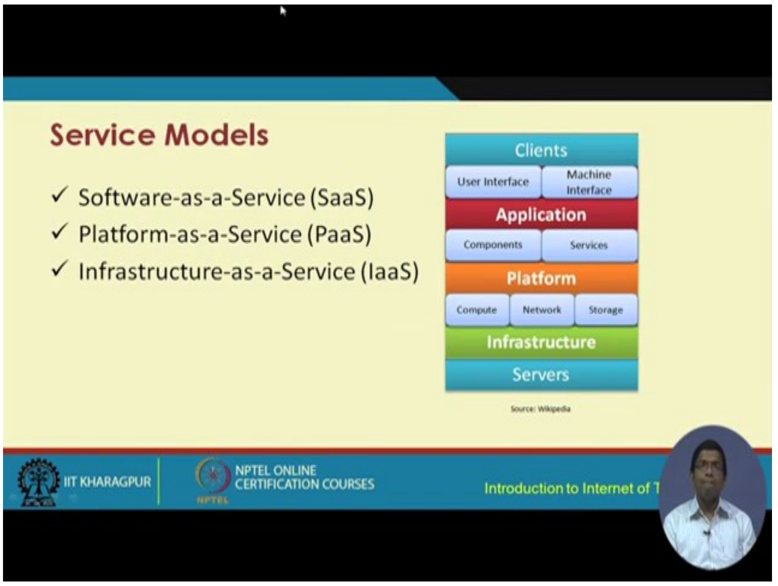
(Refer Slide Time: 23:23)



There are different components of cloud computing from the user end you have these clients and the end users which may who may use thin clients which are very popular in a cloud model. So, which are low cost as well they could be using the thick, the traditional thick clients as well. Or the mobile devices as clients services product solutions applications like web apps you know software service platforms such as web hosting platforms, application hosting platforms, should be made available through the cloud computing storage.

For instance, different databases then data storage as a service are components of cloud computing and infrastructure lastly which is very important should be virtualized and be made available in the form of infrastructure as a service model. And I am going to talk about that shortly.

(Refer Slide Time: 24:26)

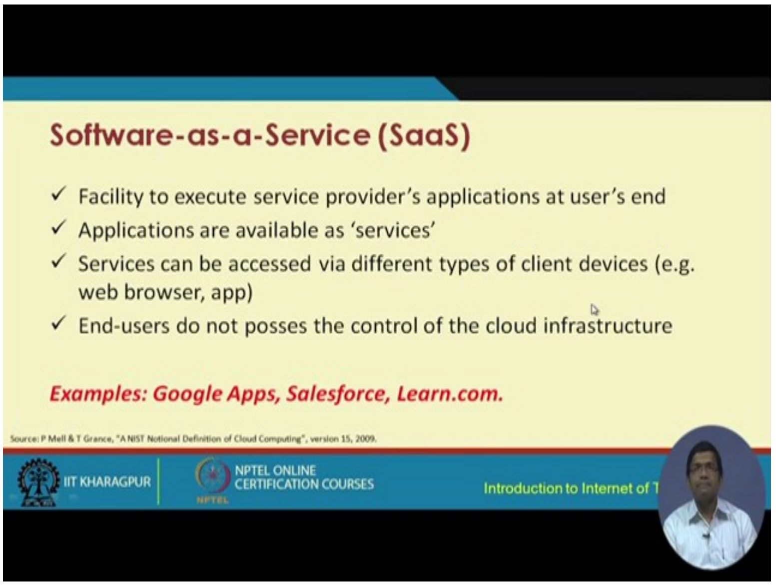


So, different service models include the software as a service, platform as a service and infrastructure as a service, these service models have been very popular. Since, the last few years I mean from the time cloud computing became very popular these service models are core service models of cloud computing, but mind you that at present people are also talking about different other types of service.

So, not just software platform and infrastructure as a service, but also something like x as a service where x could be anything, some people are talking about hardware as a service, some peoples people are talking about sensors as a service like that database as a service security as a service, people are talking about all different types of service models made available through cloud.

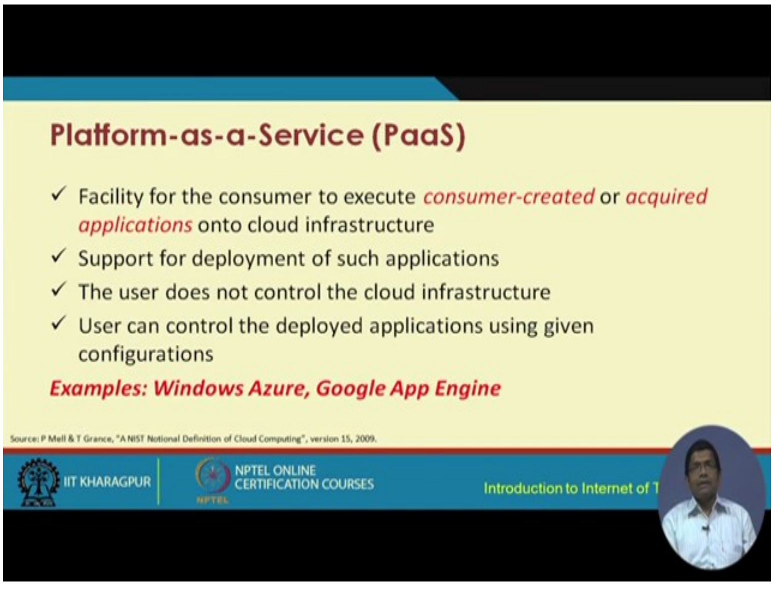
So, if you look at this particular figure we have all these cloud models. So, we have the servers underneath then infrastructure as a service platform as a service and application as a service, clients are getting access to each of these different computational resources through different interfaces.

(Refer Slide Time: 25:39)



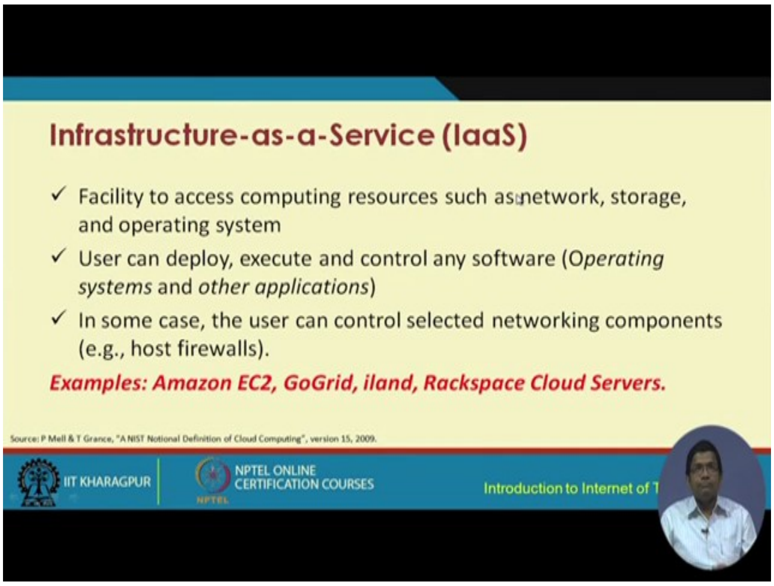
So, we have the first one which is software as a service the commonly used software as a service platforms available commercially is the Google apps the sales force learn dot com and so on. So, as this name suggests software as a service basically gives you facility to execute service provider's applications at the users end. So, applications are available as services; services can be accessed via different types of client devices example web browsers apps different types of apps and so on.

(Refer Slide Time: 26:20)



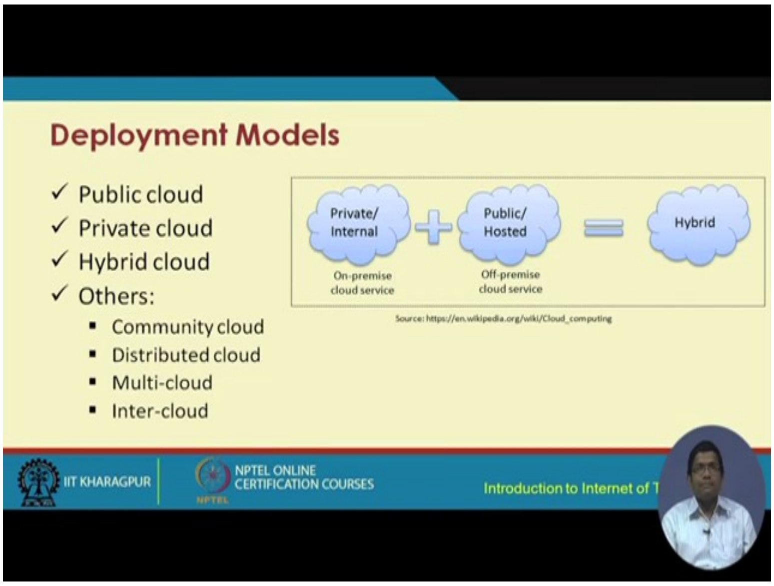
So, end users do not basically possess the control of the cloud infrastructure platform as service examples include the commercially available Windows Azure, Google app engine and so on. So, here basically the development platform is basically made available to the consumers as facilities to execute consumer created and acquired applications on to the cloud infrastructure.

(Refer Slide Time: 26:43)



Infrastructure as a service basically talks about most of this computing infrastructure like network storage operating system to be made available as facilities through the internet accessing these facilities as computational resources dynamically, whenever it is required on a paper use basis operating systems other applications can also be made available through this facility. So, popular examples of infrastructure as a service include the Amazon EC2, GoGrid, iland, Rackspace Cloud Servers and so on.

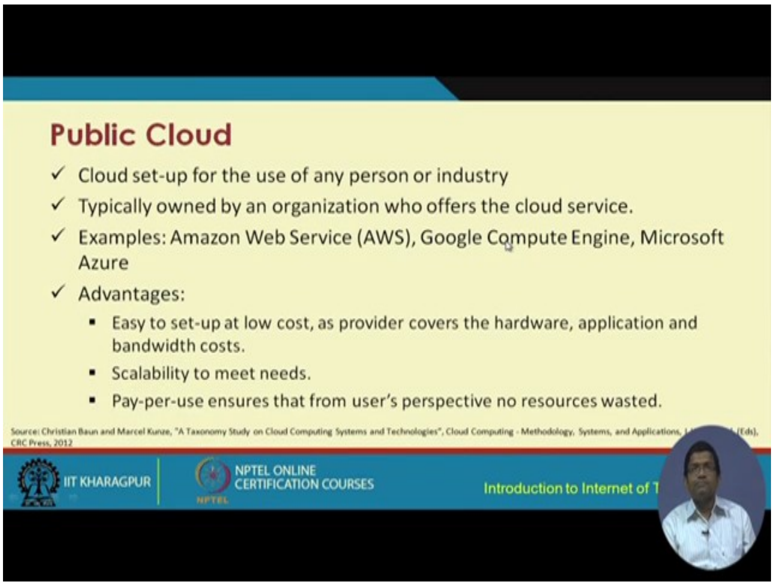
(Refer Slide Time: 27:19)



Now let us talk about having spoken about the different service models software as a service, platform as a service and infrastructure as a service let us now talk about how cloud is deployed typically what are the different deployment models that are available in cloud computing we have number one the public cloud, the second is the private cloud, the third is the hybrid cloud. And there could be other types of cloud like community cloud, distributed cloud, multi cloud inter cloud and so on. So, you know private cloud is internal to an organization and these cloud resources are made available to the users within the institution only. For example, in IIT; Kharagpur we have our own private cloud which is known as the Meghamala.

So, like that different organizations have their own private cloud, but there are some publicly hosted cloud facilities which are available off campus, off premises and these are made available by different companies like Amazon like TCS and different other companies who are sort of like service providers of these cloud. So, these are public clouds that are that are available. Hybrid clouds basically is sort of like an integration of some features of private cloud and some features of the public cloud.

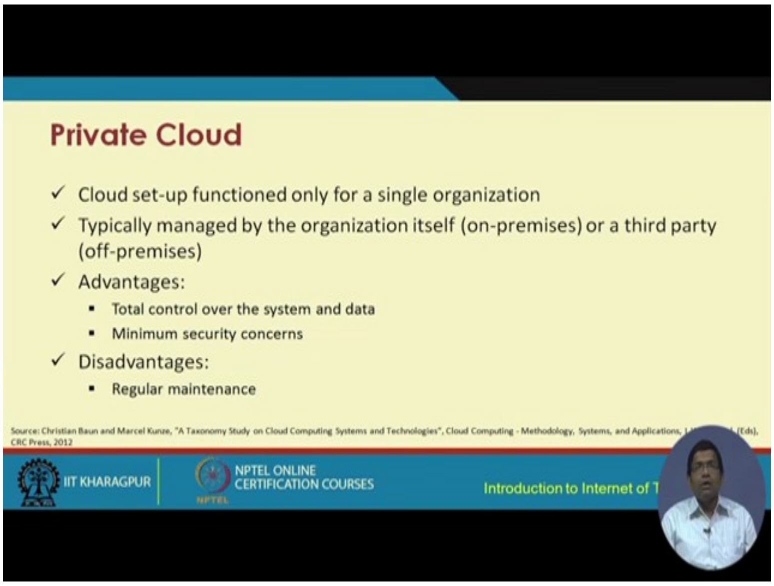
(Refer Slide Time: 28:52)



So, the public cloud is set up for the use of any person or industry typically it is owned by any organization who offers the cloud service examples include Amazon web services, Google compute engine and Microsoft azure the advantage is that this is easy to set up at low cost as the provider covers the hardware application and bandwidth cost or any other cost that is made that is in available to them.

So, this basically is a highly scalable model you just pay for the resources that are being used and there will be lack of wastage of resources.

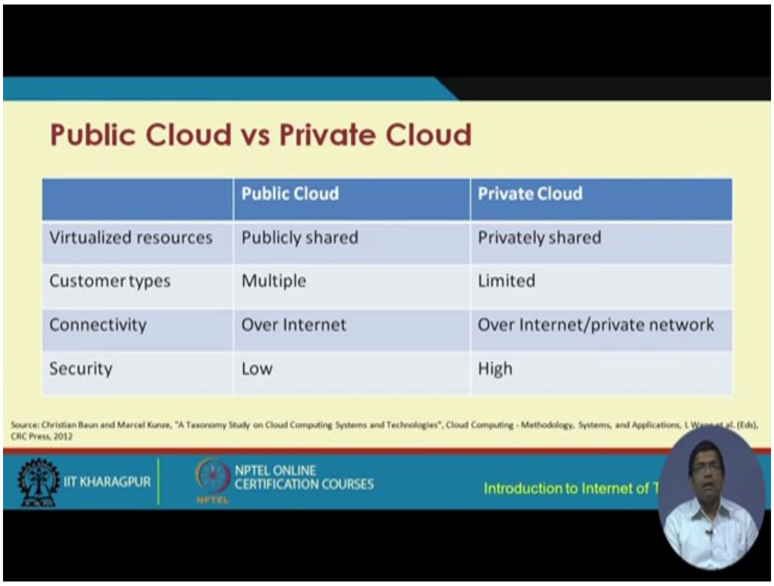
(Refer Slide Time: 29:37)



So, it is a highly scalable model that can be made available on a payment basis. Private cloud is typically restricted to a single organization the cloud functionalities are made available only within the organization typically these are managed by the organization itself or a third party. And the advantages are that there is total control over the system. And the data in such a private cloud being deployed; of course, there is some initial investment in setting up the cloud.

But once it is done then this model is quite advantageous it is low cost and these resources can be made available to the users of the organization on on their requirement basis. The disadvantage is that you have to be bothered too much about the regular maintenance, you need to have a group which will be regularly performing the maintenance tasks in a private cloud.

(Refer Slide Time: 30:37)



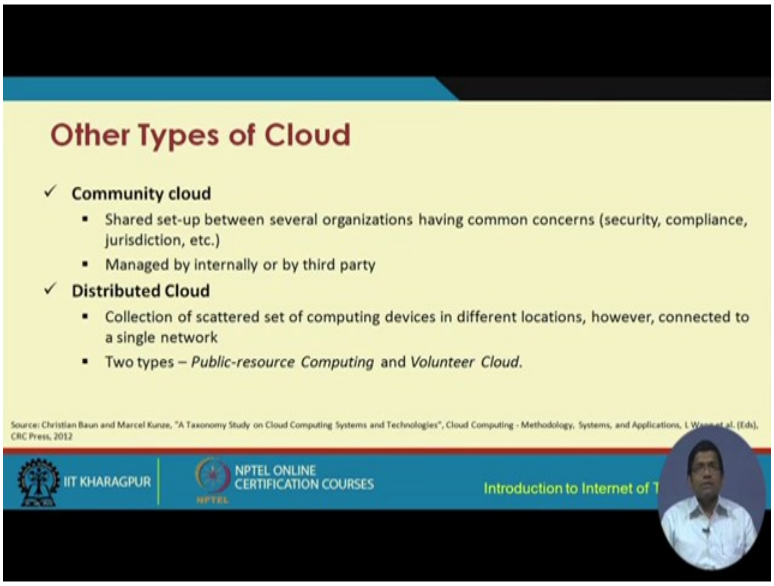
So, comparison wise public cloud and private cloud in terms of the virtualized resources in public cloud these resources are publicly shared, in a private cloud this resources are privately shared, customer type in a public cloud is basically multiple customers. And in a private cloud only a few customers who are typically limited or users of the organization like the employees of the organization.

Or the students of an organization are basically users of they serve as the customers of the private cloud in terms of connectivity public cloud is made available over the internet and private cloud. Over the internet as well as through the private network of the organization in terms of security public cloud security is much lower compared to the security issues in a private cloud.

(Refer Slide Time: 31:33)

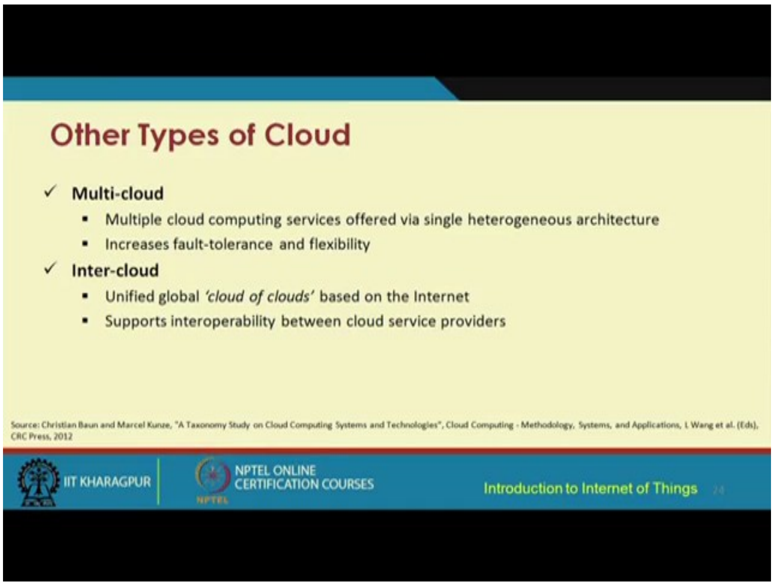
And there is a hybrid cloud as I said before with basically combines the facilities of 2 or more types of unique cloud types. For example, private community or public cloud the resources in this case are pooled together by standardized tools some resources can be pooled from a private infrastructure some from the public infrastructure and together this cloud model basically offers different services to their inducers.

(Refer Slide Time: 32:03)



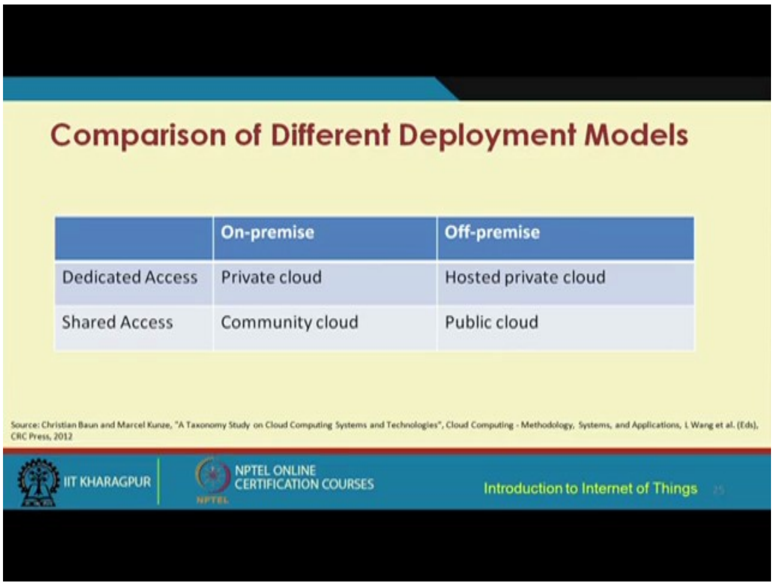
Then we have this community cloud typically this is restricted to certain communities like medical community, hospital community, security community, compliance. So, only the users of that community would be able to get access to the services of such a cloud. So, this is known as the community cloud and then we have the distributed cloud which comes in different flavors where there is collection of the scattered set of computing devices in different locations. However, connected to a single network and there are 2 types of distributed cloud- the public resource computing and the volunteer cloud. So, we are not going to go through it in the interest of time.

(Refer Slide Time: 32:42)



Multi cloud basically it is you know heterogeneous architecture single architecture combining multiple different cloud platforms together to increase the fault tolerance and flexibility of the system inter cloud is basically cloud of clouds. So, you have multiple different-different clouds which are put together unified through the internet and these basically would interoperate between each other between the different cloud service providers. And that giant cloud of cloud services is going to be made available to the users. So, these are the different models of cloud deployment.

(Refer Slide Time: 33:22)



So this comparison of this private public and this community cloud are as follows. So, in this particular table as you can see that private cloud is on-premise and offers dedicated access the privately hosted cloud is off-premise and has dedicated access as well and the community cloud is on-premise and offer shared access and the public cloud is off-premised offered offers shared access.

So, with this we come to an end of the lecture on the fundamentals of cloud computing. So, we have a series of three more lectures on this particular topic of cloud computing we have already understood at the outset of this lecture about why cloud computing is being very popular in the internet of things community cloud is I will talk about it later on as well.

But cloud you can understand that it is one of the most important enabling technologies or if core building block for internet of things development, because you have to deal with heterogeneous resources offering different types of data collecting different type of data which has to be processed quite fast without much in you know infrastructure involvement. That means, this infrastructure should be taken care of quite automatically I do not have to really buy this infrastructure and waste time and money for it. I should be able to get access to these resources and I should be able to enjoy the computing facility on a paper use kind of modeled.

So, this is all about cloud computing. In the next lecture we will talk about some more details of cloud computing.

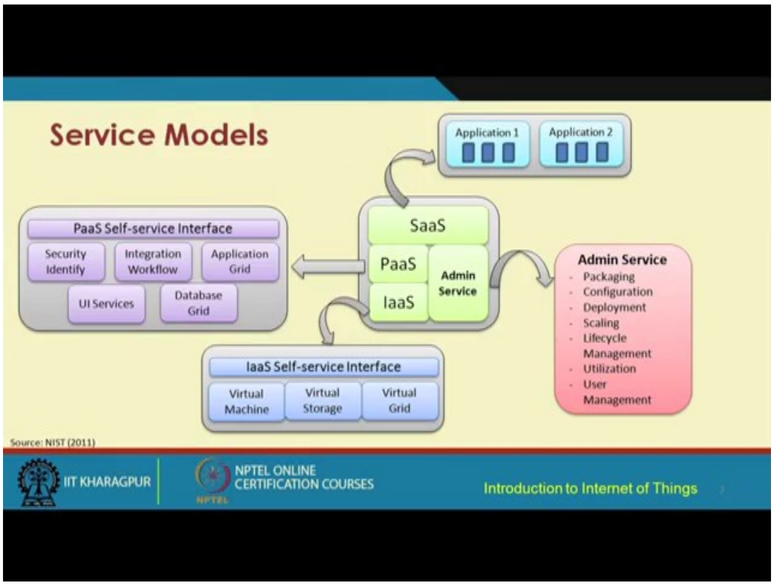
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 38
Cloud Computing - Service Models

So, the next lecture on the series on cloud computing for internet of things is on the service models. So, we briefly in the previous lecture have gone through the different types of service models we have seen that there are 3 core service models that have been popular since the inception of cloud computing. The first one is software as a service, the second one is platform as a service and the third one is infrastructure as a service. So, let us try to go through the details further of each of these clouds cloud models.

(Refer Slide Time: 00:51)

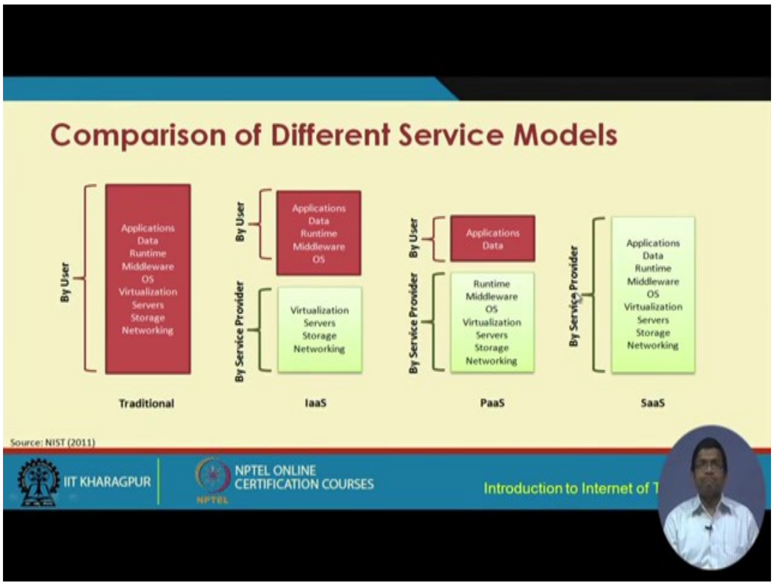


So, as we can see over here we have these different applications which have to be served and for service serving these applications we need to take help of the software resources the platform and the infrastructure.

So, what we have we have software as a service, we have platform as a service and we have the infrastructure as a service. So, infrastructure is surface on top of virtual machines virtual storage and virtual grid. So, we have this infrastructure as a surface made available and then we have the platform as a service which includes security identification integration workflow application grid user interface services database grid and so, on and then we have this software as a service which we serving different applications as well. In fact, all these service models are serving different applications are serving different customers and so on and then we have these administrative services which are in addition.

So, these administrative services include things like packaging configuration deployments scaling lifecycle management utilization user management and so on.

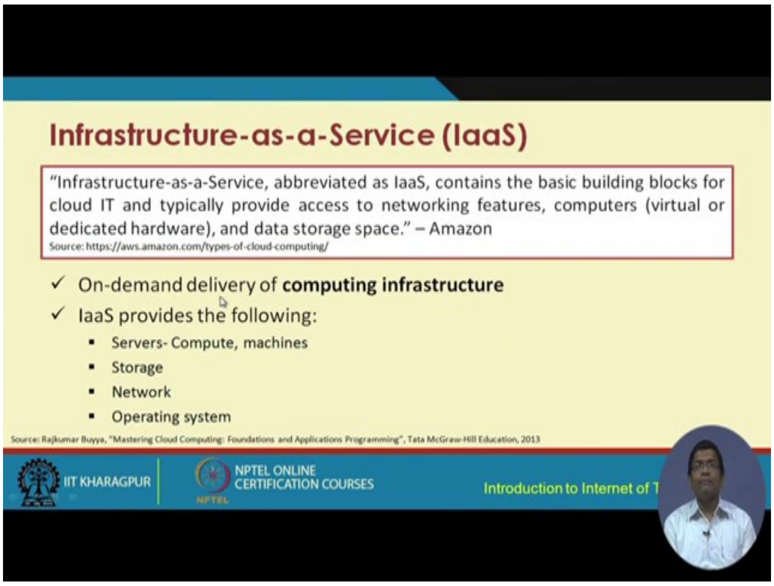
(Refer Slide Time: 02:07)



So, when we compare that the these 3 service models the serve the software as a service the platform as a service and the infrastructure as a service with respect to the traditional computing computing paradigm then we see we observe a few things. So, whereas, traditionally starting from applications data runtime middleware operating system virtualization service offerings storage networking all these things would have to be done by the user himself, in the case of infrastructure as a service concerns about or issues of applications data runtime middleware and operating system are done at the user end whereas, virtualization server storage Networking are taken care of by the service provider.

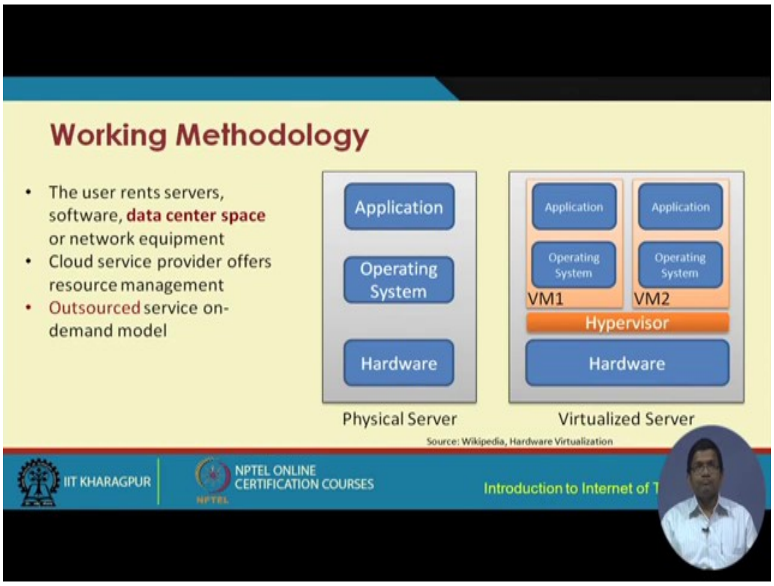
So, as you can see over here in this model the operating system is at the user end. In the platform as a service as we can see compared to infrastructure as a service where the OS was as part of the user here only 2 things applications and data are taken care of by the user the rest of the other things are taken care of by the service provider end and in software as a service everything is taken care of by the service provider.

(Refer Slide Time: 03:42)



So, this is a side by side comparison between infrastructure as a service platform as a service software as a service and the traditional computing methodology. So, we start with each of these service models and try to understand what is inside. So, as per the definition of Amazon, infrastructure as a service which is appreciated as IaaS contains the basic building blocks for cloud it and typical typically provide access to Networking features computers which are virtual or dedicated hardware and data storage space. So, we have this computing infrastructure which has to be made available on demand to the different users through some kind of virtualization mechanism. So, infrastructure as a service provides the following features it has servers for computation and the different machines are also made available like different workstations etcetera. So, so servers and machines then we have the storage we have Network we have the operating system.

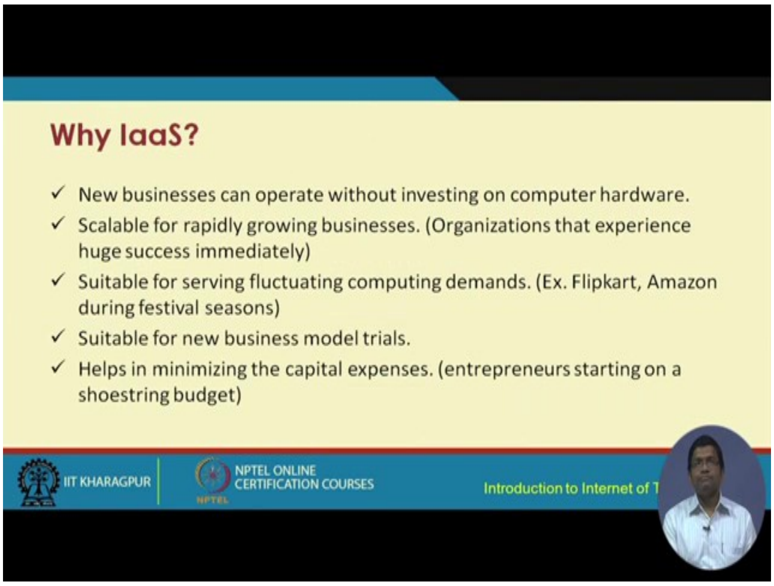
(Refer Slide Time: 04:44)



The working methodology is like this we have a physical server and then we have this virtualized server the users rent the servers the software and the data center space or Network equipment the cloud service provider offers the resource management and the outsourced service on demand is made available for use. So, this is the physical server here we have the hardware on top of that on top of hardware we have the OS and the apps and in comparison in the virtualized server we have hardware as before then we have some virtual machines. So, these virtual machines VM 1 and VM 2 would include the operating system and the application layers.

So, we have on top of the hardware multiple virtual machines executing and there is the concept of hypervisor which basically manages this show by sitting between the hardware layer and the VM layer. So, the VM layer basically contains the VMs the hardware layer the actual physical hardware and the hypervisor is sort of playing some kind of a managerial role in between these 2.

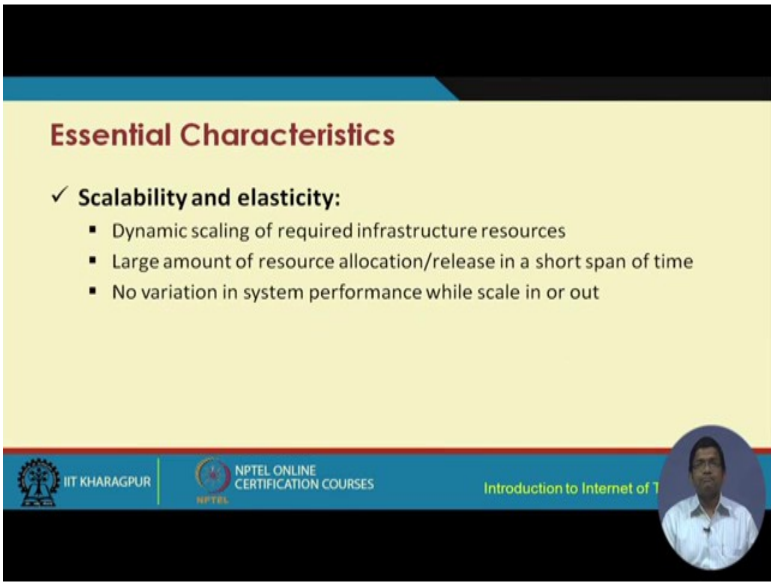
(Refer Slide Time: 06:16)



So, why do we need infrastructure as a service? So, basically new businesses can kick start without basically having to invest on vine computing hardware and this is a scalable model by which rapidly whenever the businesses need some resources they can subscribe pay for and start using the resources and whenever they do not required they will not waste the resources and will stop utilizing them.

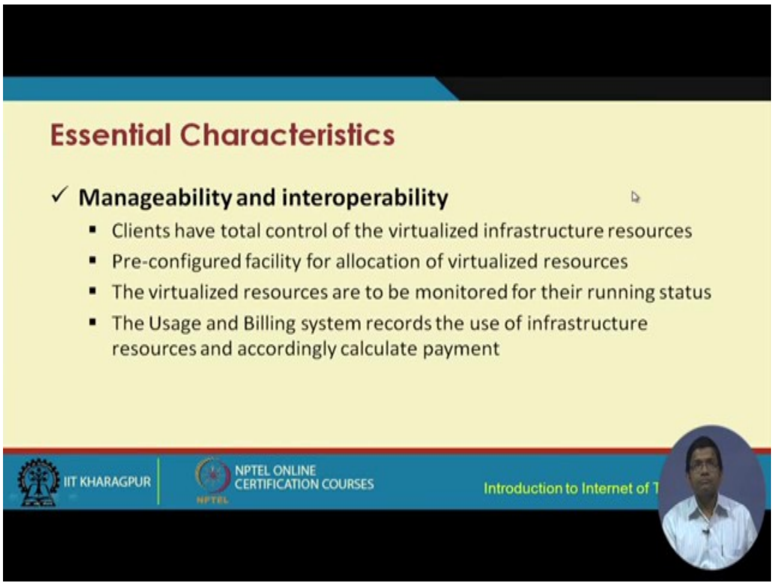
So, it is suitable for serving fluctuating computing demands example Flipkart, Amazon, etcetera during festive seasons you know they need more infrastructure during festive seasons because of the obvious you know obviousness due to the up search in the business. So, you know, but at the other times of the year they do not need this.

(Refer Slide Time: 07:25)



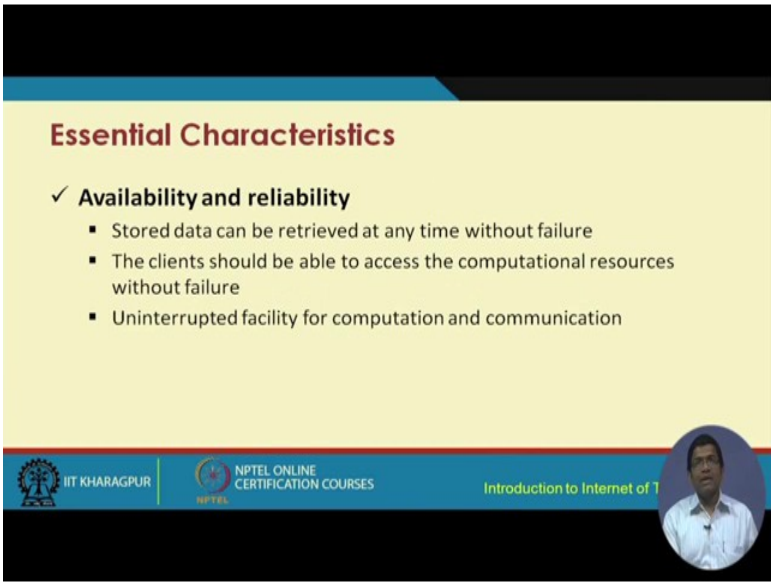
So, as you can see that there is fluctuating computing demand and whenever required you use those resources whenever not required you release the resources and so on. So, it is suitable for new business model trials it helps in minimizing the capital expenses. Scalability issue and elasticity dynamic scaling of required infrastructure resources is made possible through infrastructure service having large amount of resource allocation or release in a short span of time is possible in the infrastructure as a service model and there is no variation in system performance while scaling up or down.

(Refer Slide Time: 07:49)



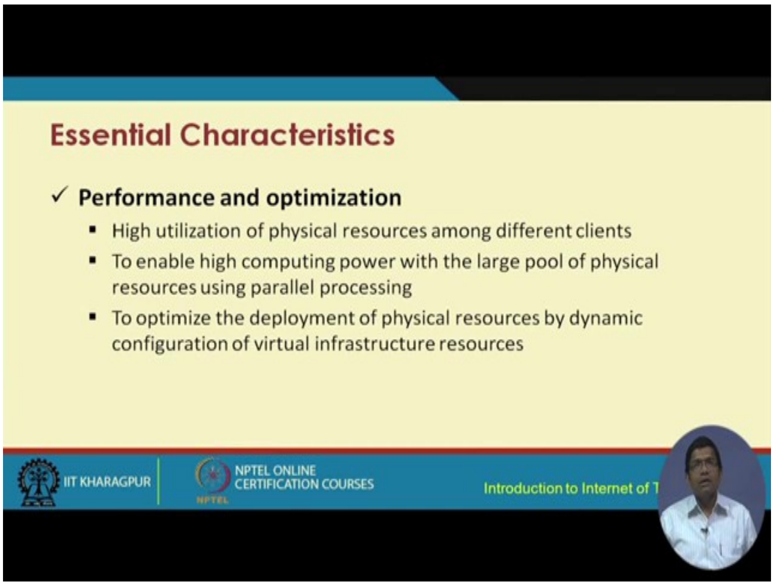
Manageability and inter probability clients in this particular model have total control of the virtualized infrastructure resources they can do whatever they want with the resources that are offered to them.

(Refer Slide Time: 08:21)

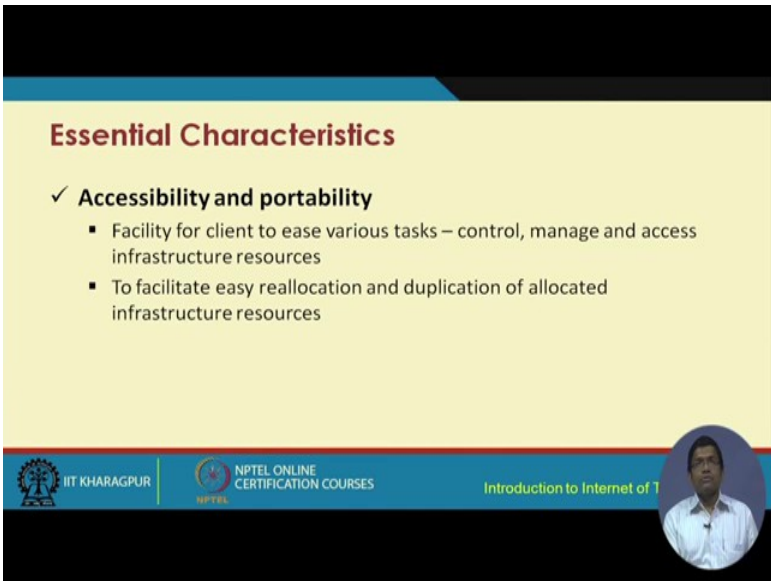


So, they can preconfigured they can preconfigured the facility for the allocation or can virtualize the resources and these virtualized resources are to be monitored for their running status the overall health and so on and the usage and the billing system records the use of the infrastructure resources and accordingly calculates the payment availability and reliability. So, storing of the data and the retrieval of the stored data can be made possible at any time without any failure of any any kind whatsoever; whatsoever be the failure. So, it is not possible you know the resources can be made available reliably and be made available at anytime anywhere the clients should be able to access the computational resources without failure and there should be uninterrupted facility for computation and communication in terms of performance.

(Refer Slide Time: 08:55)

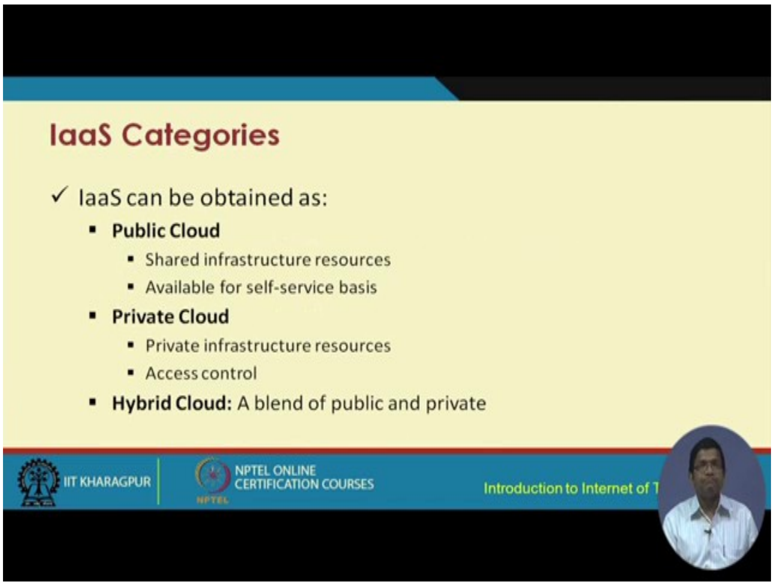


(Refer Slide Time: 09:21)



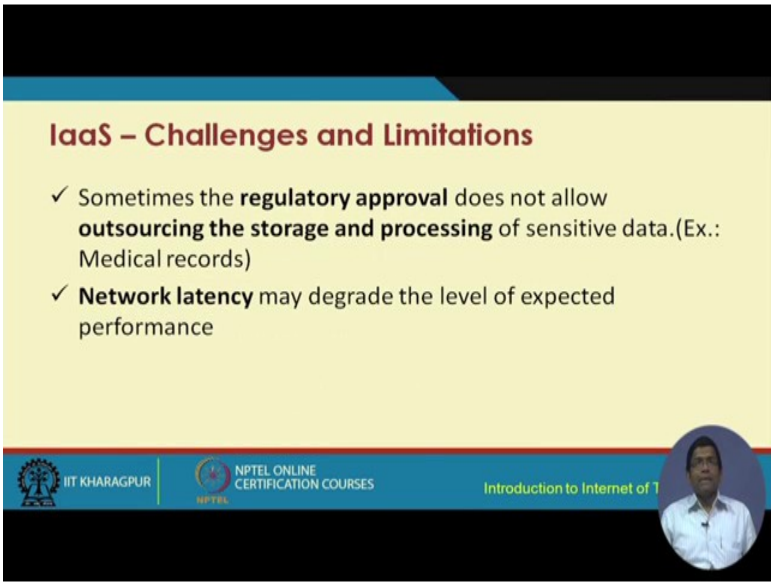
And optimization high utilization of physical resources among the different clients is possible through the use of the infrastructure as a service model; it is also possible to enable high computing power with the large pool of physical resources using parallel processing. And it is also possible to optimize the deployment of physical resources by dynamically configuring the virtual infrastructure resources in terms of accessibility and portability this basically provides the facility for client to ease out various tasks with respect to control management access infrastructure access and so on and to facilitate the easy reallocation and duplication of the allocated infrastructure resources. IaaS can be obtained as a pub public cloud a private cloud.

(Refer Slide Time: 09:44)



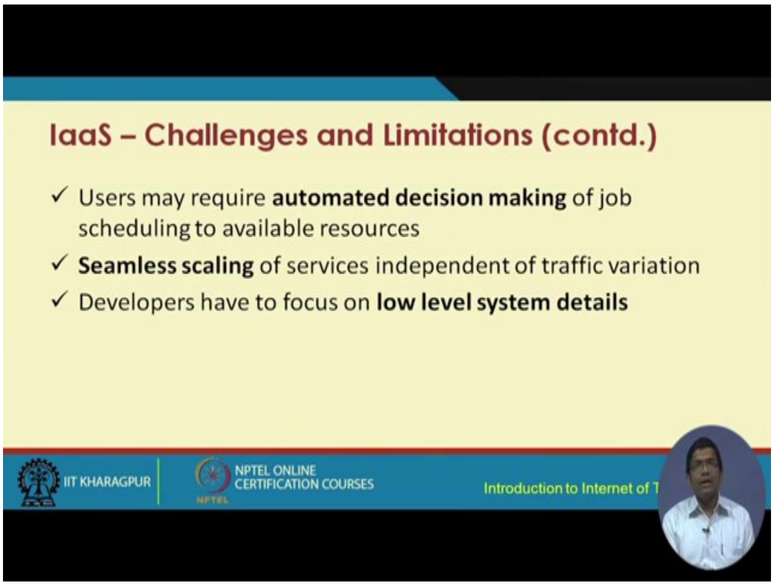
And the hybrid cloud and each of these we have already discussed in the fundamentals lecture on cloud computing for IoT.

(Refer Slide Time: 09:56)



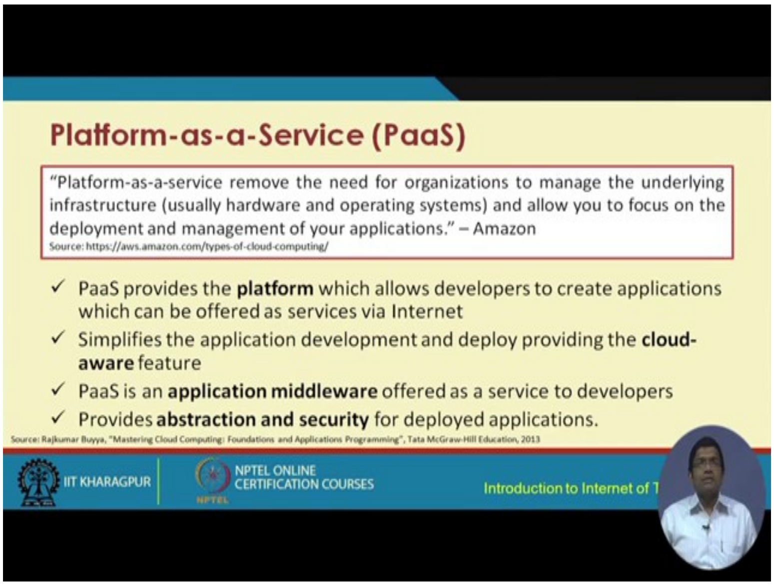
So, the challenges and limitations of infrastructure as a service includes that there is sometimes in certain places regulatory approval that is required for the use of outsourcing outsourced storage.

(Refer Slide Time: 10:19)



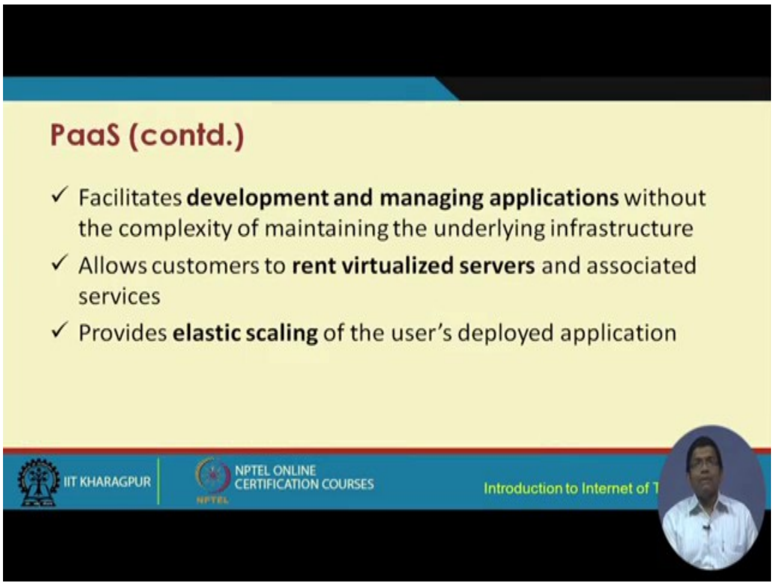
And outsourced processing through the cloud model and Network latency may degrade the level of expected performance as well users may require automated decision making of job scheduling to available resources and seamless scaling of service services independent of traffic variation and developers have to focus on low level system details these are some of these limitations of infrastructure as a service.

(Refer Slide Time: 10:38)



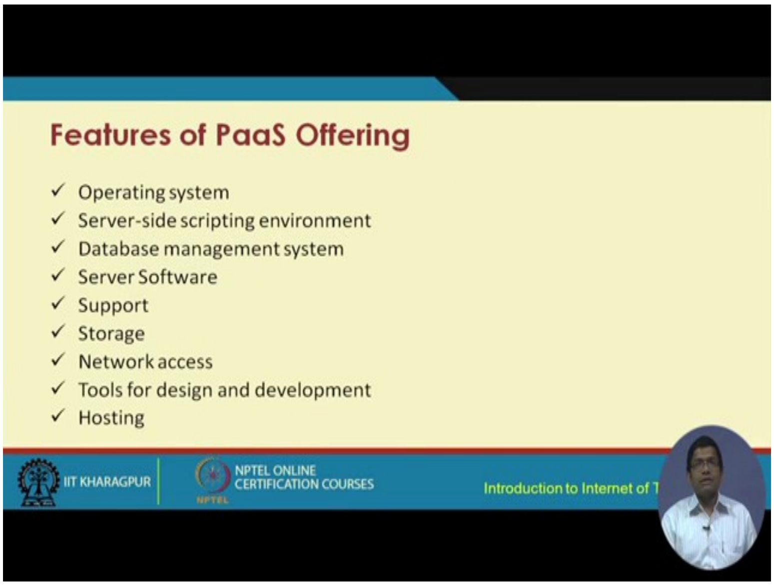
Next comes the platform as a service. So, here I will read out the definition for you platform is a service removes the need for organizations to manage the underlying infrastructure which is usually a hardware and operating system combination and allows you to focus on the deployment and management of your application. So, as you can understand application development firms would be strongly benefited through the use of platform as a service. So, platform as a service provides the platform which allows the developers to create applications which can be offered as services via the internet it basically makes the applications you know easy to develop it simplifies the application development and deploy and deployment by providing the cloud aware features. Platform as a service is an application middleware.

(Refer Slide Time: 11:36)



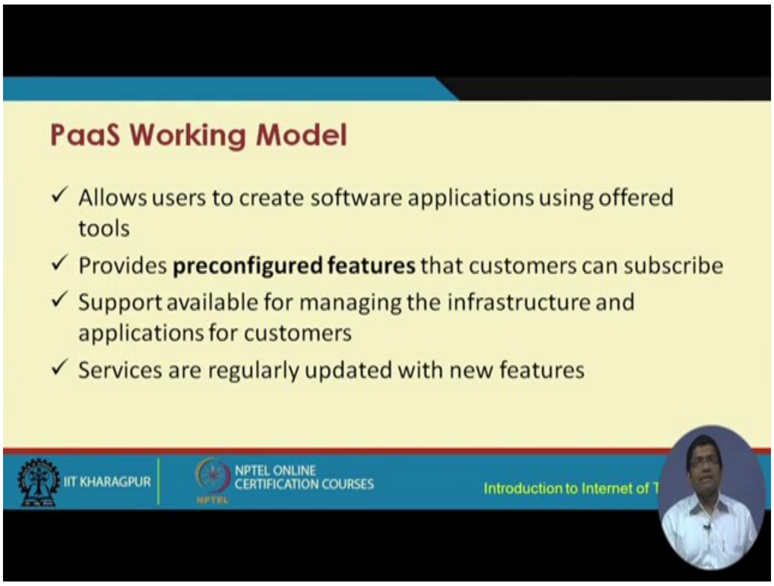
Which is offered as a service to the developers it provides the abstraction and security for the developed applications, it facilitates the development and management applications without the complexity of maintaining the underlying infrastructure it allows customers to rent virtualized these servers and the associated services.

(Refer Slide Time: 11:53)



And provides elastic scaling of the users deployed application. There are different features of platform as a service in terms of operating system you know operating system can be made available through the platform as a service based on the choice of the in the developers or the users server side scripting is possible, database management is possible server software support net storage, Network access offering different tools for design.

(Refer Slide Time: 12:27)

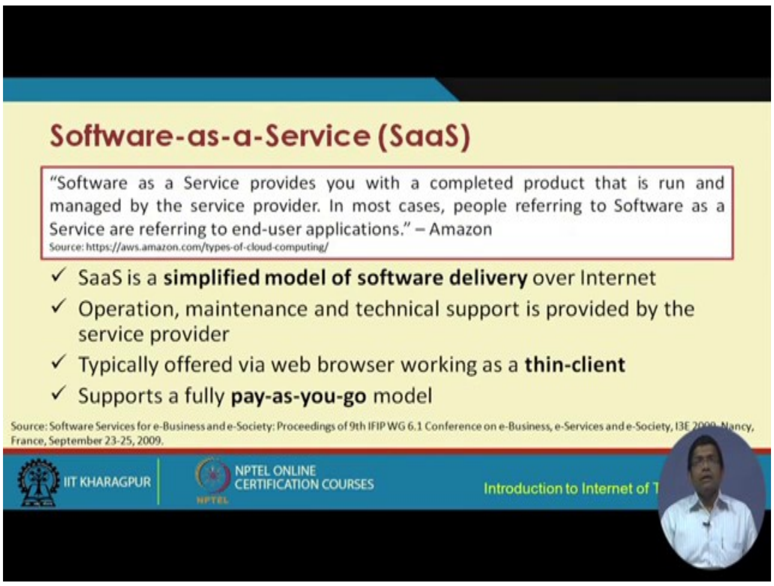


And development of software and hosting these are all made available as different features of platform as a service the working model is like this that it allows the users to create the software applications using offer tools and it provides the preonfigured features that the customers can subscribe it supports the available it support supports availability and management of the infrastructure and applications for customers and the services are regularly updated with new features.

(Refer Slide Time: 12:50)

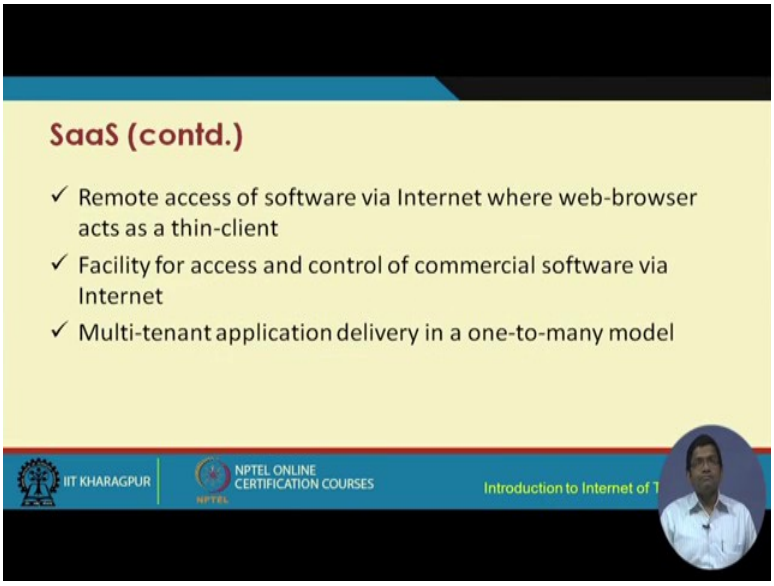
The business advantages are with respect to the middleware service support the development and deployment tools the easy access to them and also the freedom for managing development and deployment tools individually.

(Refer Slide Time: 13:06)



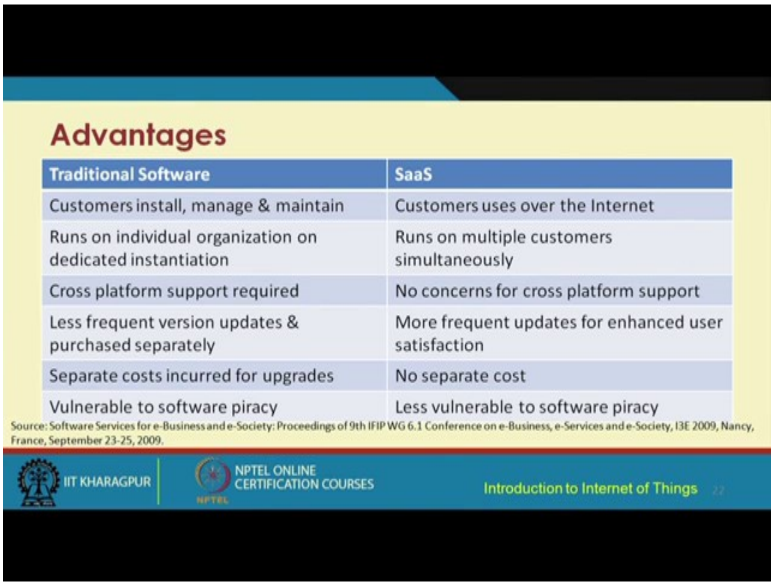
And finally, the software is a service. Again the Amazon definition I will read out software is a service provides you with a completed product that is run and managed by the service provider in most cases people referring to software as a service are referring to end user applications.

(Refer Slide Time: 13:36)



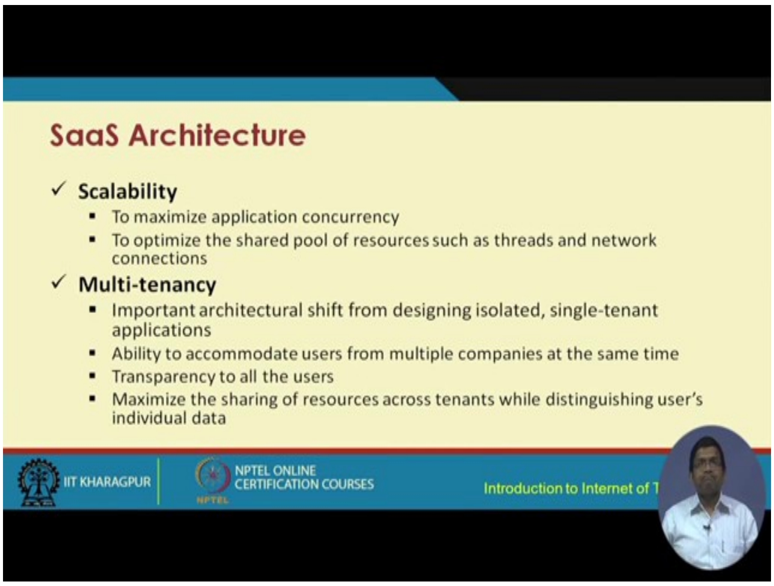
So, SaaS is a simplified model of software develop delivery or over the internet it typically uses web browser working as a thin client and supports a fully pay as you go model it also has some additional features for example, remote access of software is possible via the internet where the web browser acts as a thin client, it also has facilities for access and control of commercial software via the internet. And also this multi tenancy application delivery to multiple people at the same time multiple tenants at the same time in one to many model is made possible through software as a service.

(Refer Slide Time: 14:05)



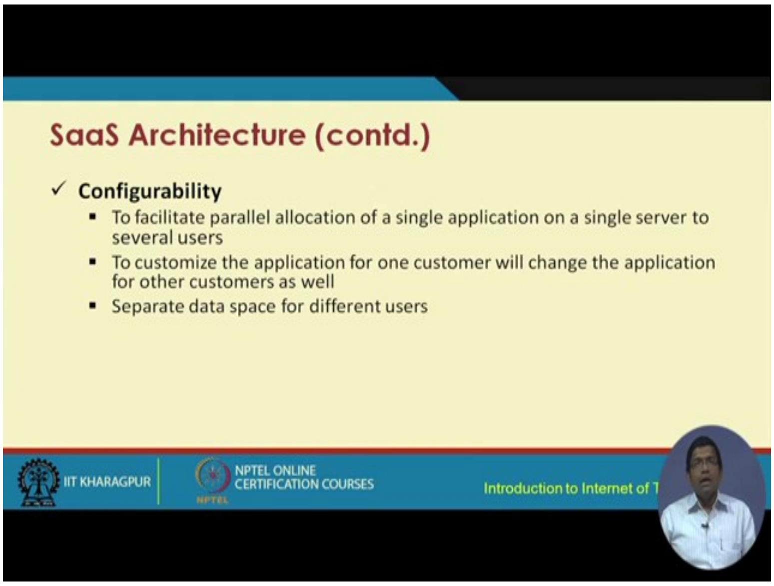
Compared to the traditional software the comparison with software as a service is given in this particular table the advantages include for example, with respect to traditional software customers have to traditionally install manage and maintain the application the software. Whereas, in software as a service the customers simply use all these over the internet the traditional software runs on individual organization on dedicated instantiation whereas, software as a service runs on multiple customers simultaneously clock sorry cross platform support is required in traditional software.

(Refer Slide Time: 14:59)



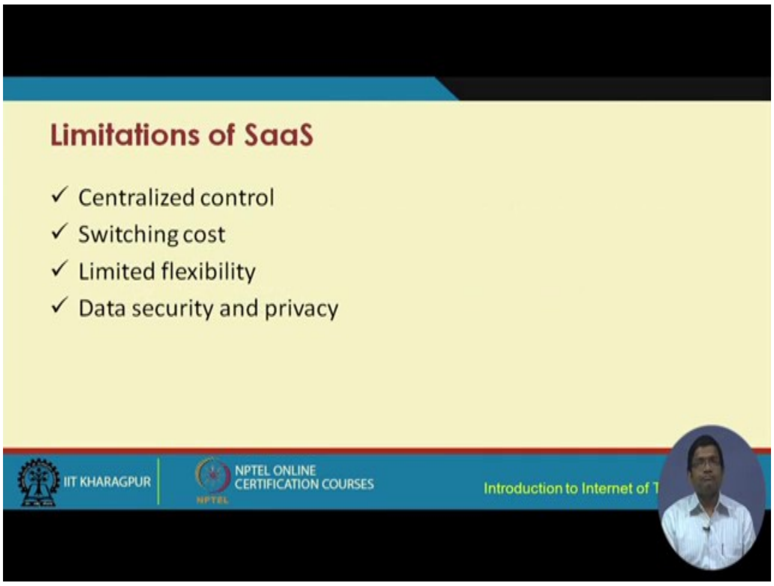
Whereas in software as a service there is no concern for cross platform support like this; there are different other advantages of software as a service over the traditional software scalability is to maximize the application concurrency to optimize the share resource share resource pool such as threads and Network connections multi-tenancy it is an important architectural shift from designing isolated single tenant applications to supporting multiple tenant applications it has the ability to accommodate users from multiple companies at the same time.

(Refer Slide Time: 15:36)



And there is transparency that is improved by the use of this model amongst all the users in terms of configurability it is about to facilitate it; it facilitates parallel allocation of a single application on a single server to several users to customize the application for one customer.

(Refer Slide Time: 15:54)



While changing the application for other customers as well. The limitations of SaaS include supporting centralized control. So, that is not a very good thing it is a limitation switching the cost. So, switching cost rather switching cost between different software limited flexibility it has immediate flexibility and there are data security and privacy concerns in this model. So, these are the 3 main models of cloud the software as a service, platform as a service and infrastructure as a service and we have gone through the different advantages and limitations of each of these models and as we will see later on that these models coupled with few other concepts are required in order to meaningfully develop and deploy IoT services maybe for Smartphone applications or maybe for smart cities applications.

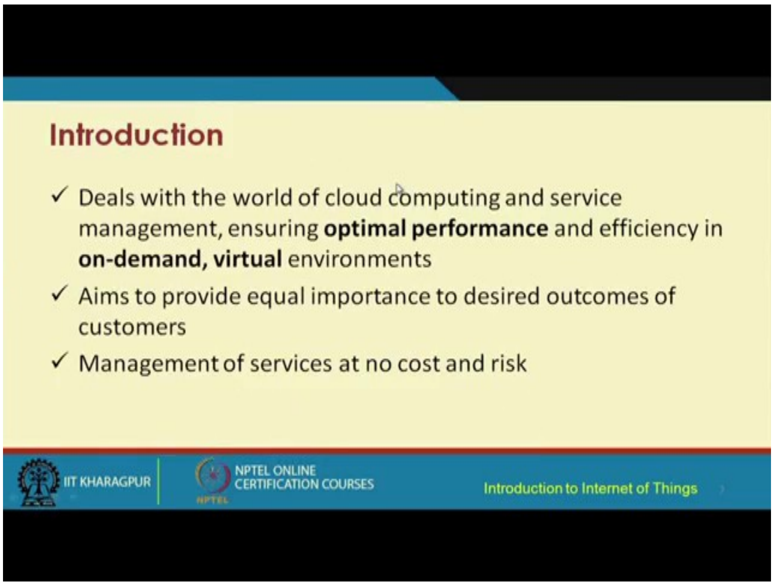
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 39
Cloud Computing - Service Management and Security

In this lecture which is the third in the series on cloud computing for internet of things we are going to specifically focus on issues of service management and security. So, we will look at some of the issues with service management and security in this lecture and we will not specifically get get too much deep into how to offer the service management and how to secure the systems that will be basically you know out of the scope of this introductory course on internet of things. So, we will simply try to focus on the issues that are there and which have to be taken care of while dealing with cloud computing and particularly more specifically of cloud computing for IoT.

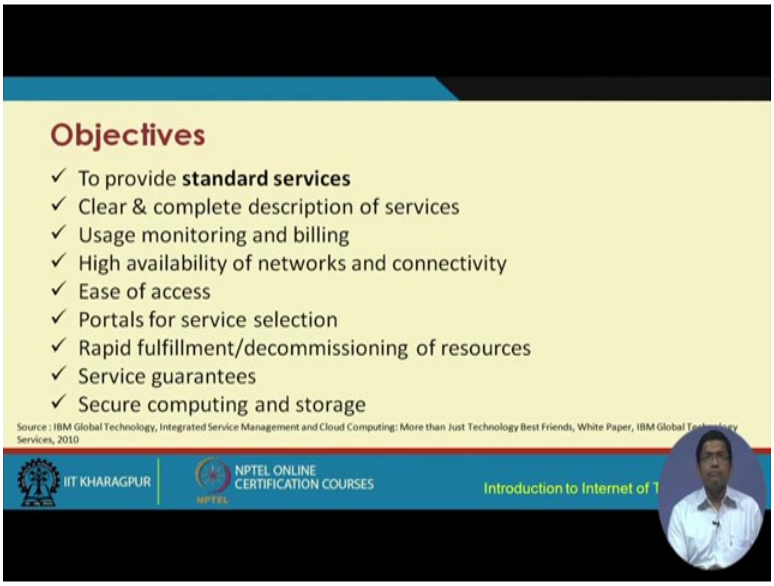
(Refer Slide Time: 01:13)



So, let us look at some of these different issues. So, before that we have to be careful about few things. So, when we are talking about cloud computing we are essentially talking about service offerings computing services being offered and when we talk about service offerings we have to ensure that there is optimal performance that is delivered to the intended customers or the end users and there is on demand whenever there is required, the services are offered in an efficient manner in a virtual environment because as we saw in the previous lectures on cloud computing these are environments which are virtual. Cloud is essentially a virtual environment where you know computing resources are offered through the through the use or through the help of virtualization technologies.

So, basically the aim is to provide equal importance to desired outcomes of customers through service management. So, that the customers are satisfied and so, that there you know the customers get the services in an; in you know in a good way at no extra cost and with minimum risk. So, minimum risk means I will give you an example over here cost is understandable, but risk basically refers to that let us say that customer was using some computing resource and if due to some reason that resource becomes unavailable there should be the risk mitigation technique should ensure that there is some additional physical resource which will be mapped to the virtual one that the customer was using.

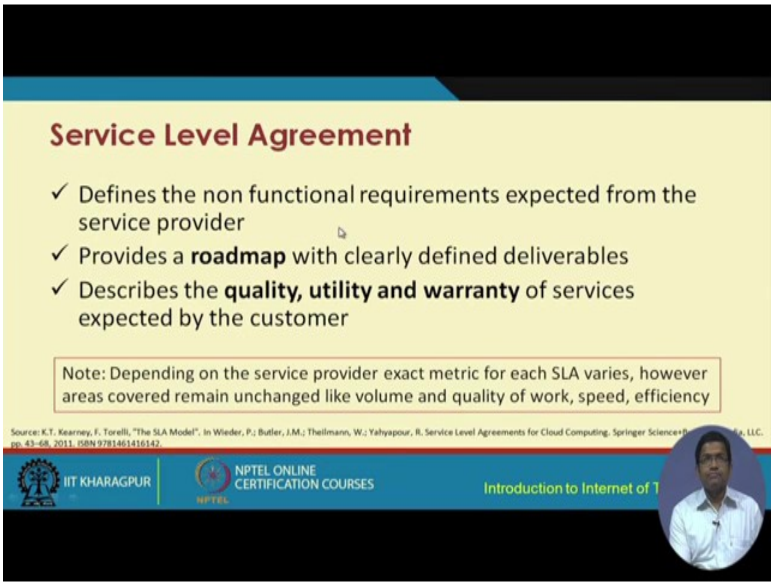
(Refer Slide Time: 03:19)



So that provisioning has to be done dynamically and the customer should not feel that something was has had gone wrong and because of which this change happened in the background. So, basically it is required to offer different types of services and services including usage monitoring and billing there should be complete description of clear and complete description of the services that the customer is going to get. Then issues with respect to availability of networks and connectivity and it should be available continuously high availability of networks and connectivity should be there; there should be ease of access to these resources and and it should be managed the services should be managed in such a manner that the customer will not be able to get any get any feeling of any under or you know underperformed computing environment.

There should be portals for service selection there should be service guarantees and rapid fulfillment of resources or decommissioning of resources should should be there and it should be a secure environment where securely computing and storage facilities are made available to the users.

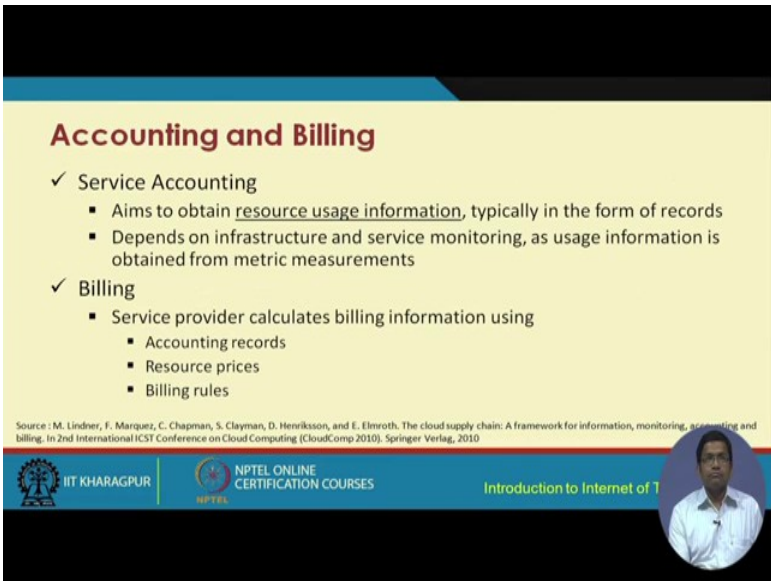
(Refer Slide Time: 04:34)



So, what is this service level agreement? So, service level agreement as per definition is about non functional requirements that are expected from the service provider more specifically the cloud service provider and this service level agreement in short in the industry it is known as SLA this SLA basically is required to provide a roadmap which will give clearly defined deliverables

So, this SLA will typically describe the quality, the utility, the warranty of services that are expected by the customer. So, this SLA will be some sort of an agreement and handshaking platform between the service providers and the customers.

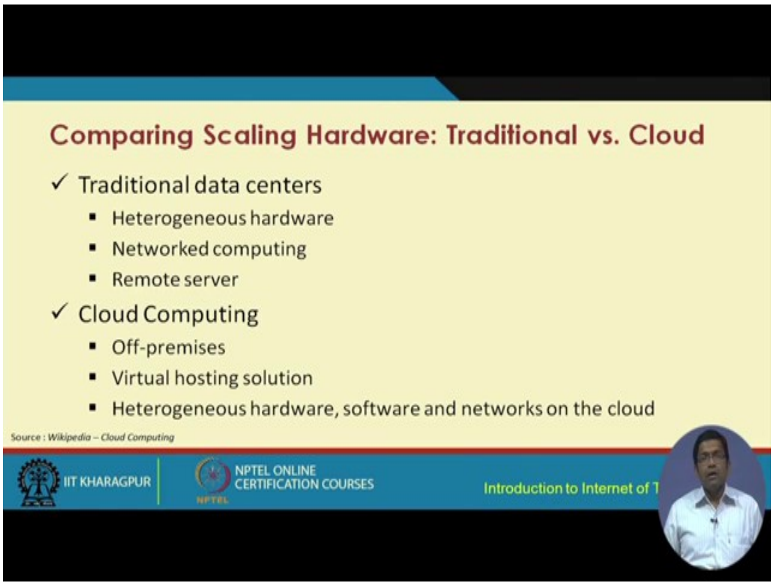
(Refer Slide Time: 05:35)



So, that the customers know what level of services the customer is going to get from the service provider. Accounting and billing which go hand in hand are very important. So, basically based on the resources the use of the resources and the information about such an such use it is required to bill the customers it is required to bill the customers and keeping track of this information about the resource. Resource use which is typically in the form of records the customers will be billed and the customers will be having you know it they will billed based on the accounting records, the resource prices and the billing rules. There has to be some rules based on which the customer is going to be billed maybe this much unit of resource consumption will lead to this much you know billing rate a higher amount will lead to another higher rate and so on.

So like this there has to be slabs or some billing policy some billing rules which has to be agreed upon by between the customers and the service provider. So, accounting records which has to be kept track of which is a core component of the accounting module the resource prices; that means, you know what is the unit cost of each of these different resources and the billing rules; that means, what is the policy by which the customer is going to be billed. So, all these taken together will be used for billing purpose.

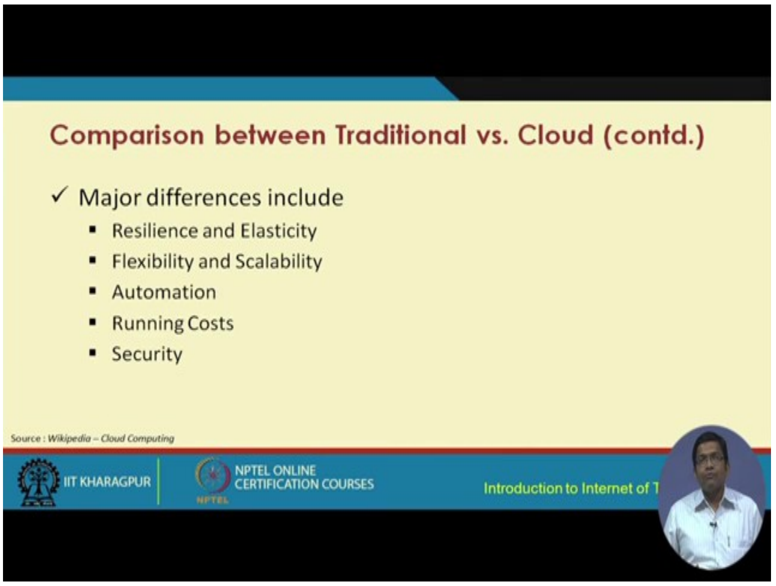
(Refer Slide Time: 07:21)



Now traditionally data centers were used or even simple IT infrastructure used to be used in the companies in the organizations now we are talking about replacing such things or supplementing such traditional regular IT infrastructure based or data center based platforms with cloud. So, we are talking about that. So, let us compare with respect to different criteria now for example, with respect to the hardware the traditional data centers used to use heterogeneous hardware different types of hardware purchase through different means you know different groups purchasing and so on and so forth heterogeneous hardware with network computing and remote server.

So typically what would happen through a remote environment these remote network environment these heterogeneous hardware would get access to a server get access to the server and that used to be the traditional way of getting access to different computing resources getting access to remote server. Means like data centers would be hosted remotely and through this hardware and the network environment the users are going to get access to the servers and computing needs etcetera, etcetera that used to be traditional in cloud computing we are talking about off-premise resources with virtually hosted solutions with heterogeneous hardware software and networks everything available on the cloud whenever things are required, whenever users have requirements they can easily scale up or down the resources the resources are going to be made available to the users as per the requirement through a virtualized platform.

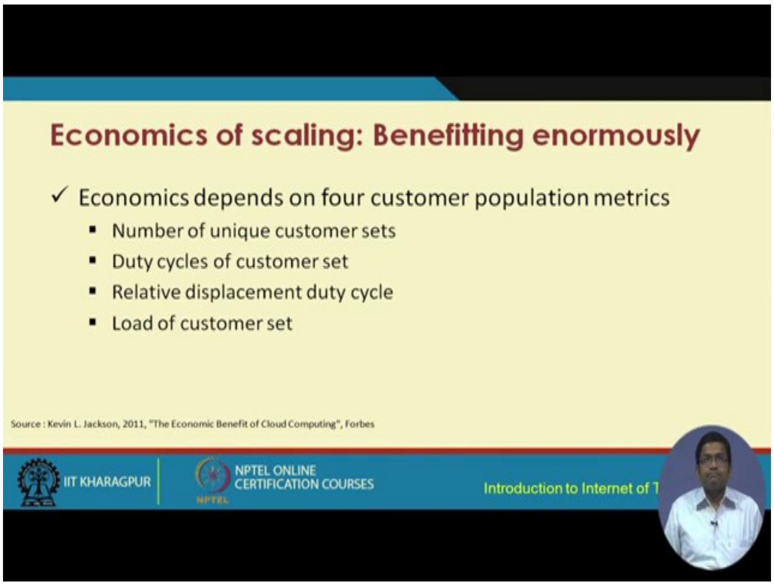
(Refer Slide Time: 09:39)



So, there is some difference as you can understand between the traditional data centers traditional IT infrastructure in the companies and the cloud computing environment there are different other differences as well which we have already understood in different perspective in the previous 2 lectures on cloud computing. One is the differences in resilience and elasticity you know. So, cloud resources cloud platforms are available you know in an elastic manner resilient manner resilience means that something going wrong users will not have a clue of it you know and it is taken care of the problem is taken care of its resilient to different kinds of failures and so on.

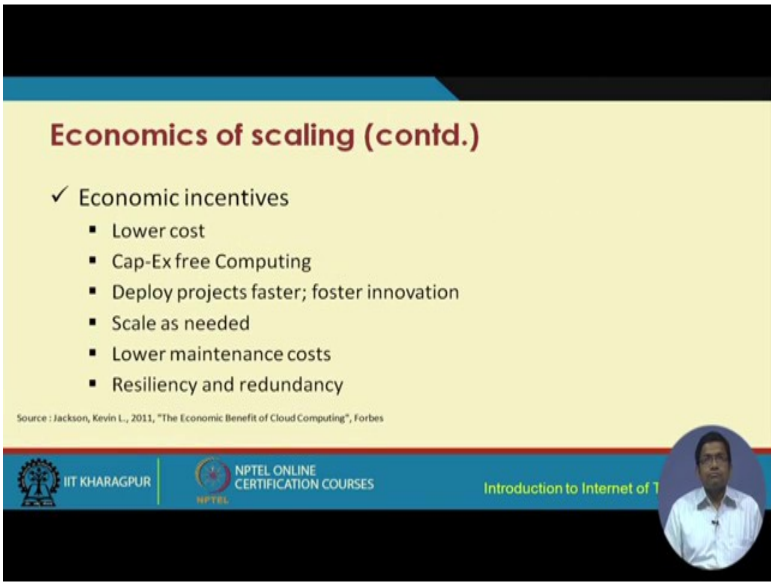
Flexibility and scalability you know you need more resources you just pay for it you have the resources with you whenever you need automation is understood running costs security; security is very important security is you know in the cloud environment you have more security compared to the traditional data center or regular IT infrastructure based environment and with respect to running costs I have already explained before. So, I do not need to explain further. So, the running you know. So, here actually you have running costs compared to the traditional onetime cost or periodic costs in on the traditional data center environment. So, here you have running costs. So, you need you need more resources you pay for it you need even more you pay even more and so on. So, running costs have to be taken care of in the cloud computing model.

(Refer Slide Time: 11:07)



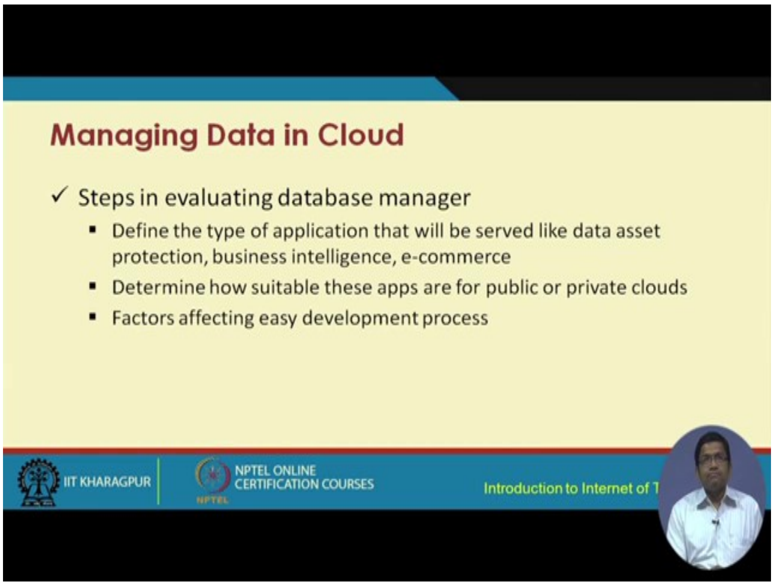
Now the economics of scaling which basically benefits the users enormously and the economics basically depends on 4 customer population metrics number one the number of unique customer sets, number 2 is the duty cycle of the customer set, number three is the relative displacement duty cycle and number 4 is the load of the customer set. So, all these basically factors all these factors basically help in coming up with ideas of economics of scaling.

(Refer Slide Time: 11:47)



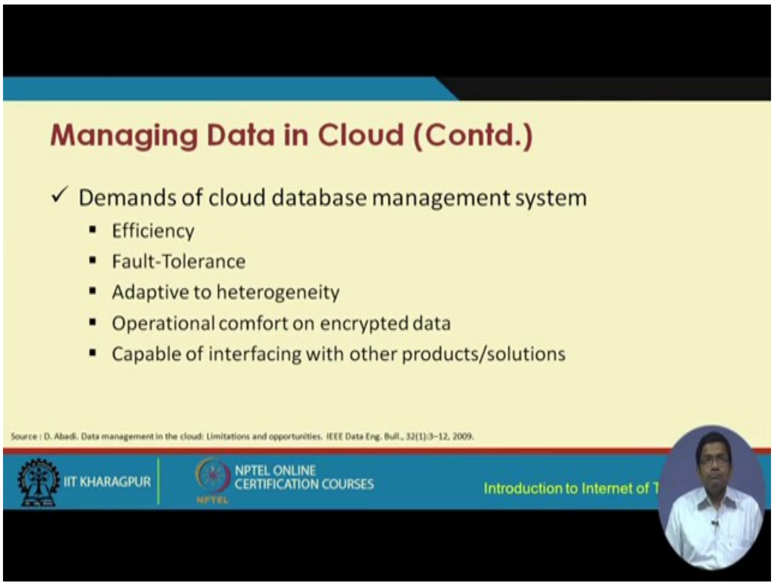
There are different economic incentives for cloud computing lowering the cost behind infrastructure and computing required in the organization then you know cap-ex free computing you know cap free computing you know exclusively made available to the customers deployment of projects faster that will foster innovation as well then you know scaling up or down as an when required lower maintenance costs resiliency and redundancy.

(Refer Slide Time: 12:21)



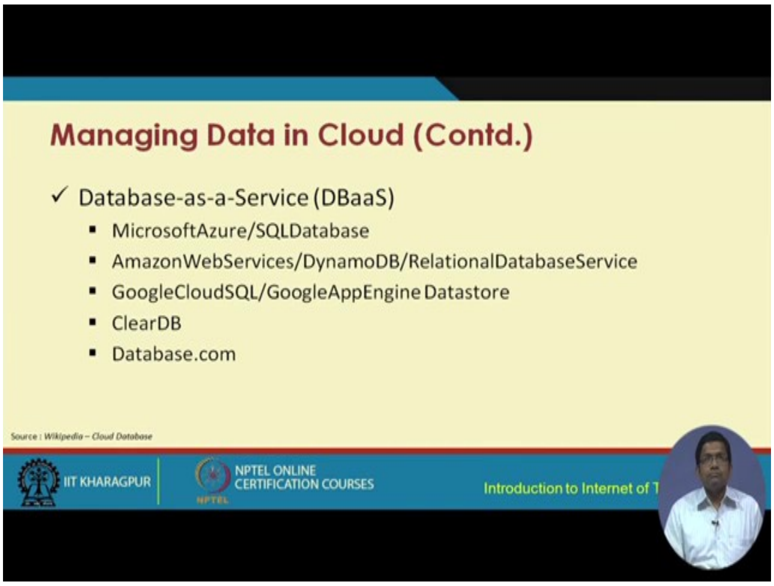
Steps in evaluating the database manager; so, database management is very important you need to manage the data in the cloud. So, there are different ways of doing it. So, will not get into too much of thing, but we need to understand the saliency behind this particular issue. So, it is required to define the type of application that will be served like the data asset protection, business intelligence, e-commerce etcetera and determine how suitable these applications are for public and private clouds and the factors that are affecting the easy deployment process.

(Refer Slide Time: 13:01)



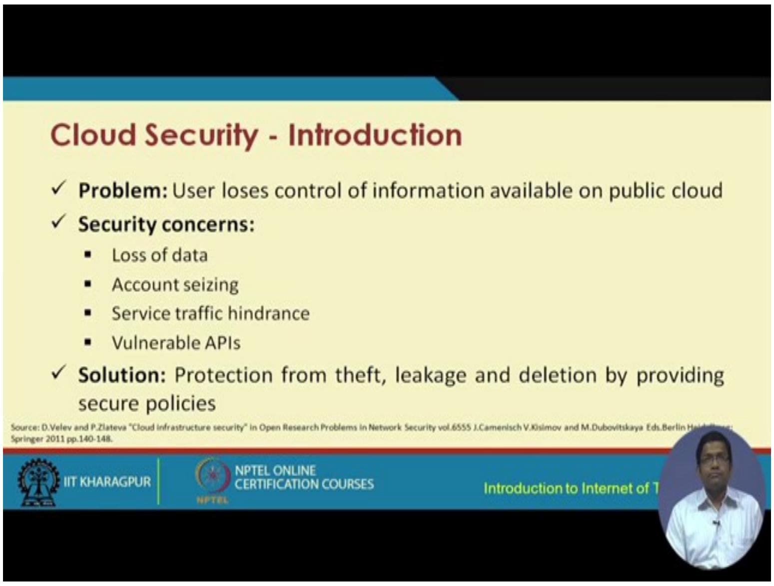
The demands of cloud database management system include efficiency fault tolerance adaptive; adaptivity to heterogeneity operational comfort on encrypted data and keep and the ability of interfacing with different products and solutions.

(Refer Slide Time: 13:32)



So this basically is quite you know explicit it is quite understandable each of these. So, we do not need to really dig into them in further detail. So, for managing data in the cloud we need some kind of service like database as a service DBaaS we need something like that and that has to be integrated with the cloud platforms like Microsoft azure or SQL database. So, SQL database basically comes with Microsoft azure or with Amazon web services with the help of DynamoDB relational database service and so on or in the case of Google cloud SQL taking help of database as a service like platforms like Google app engine data store, clearDB database dot com and so on.

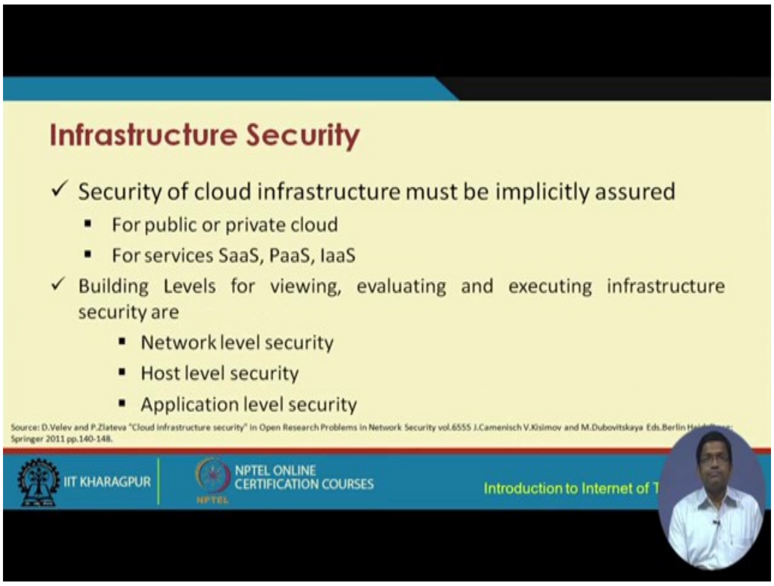
(Refer Slide Time: 14:29)



So these are the different platforms database as a service platforms that are available through commercial or open source mechanisms for use with cloud. Now let us come to the issue of security which is the second part of the lecture and here basically we have to be careful because when you are talking about cloud you are essentially handling different types of data and not only different types of data this data are going to be stored in different servers different platforms which may be geographically distributed without the cloud user even having a clue about what is going on behind the scene where physically the data is going to decide the cloud user does not know. So, data security is very important and overall the security of the cloud platform is very important because otherwise the customers will have lot of concerns which will affect directly or indirectly their use of cloud services.

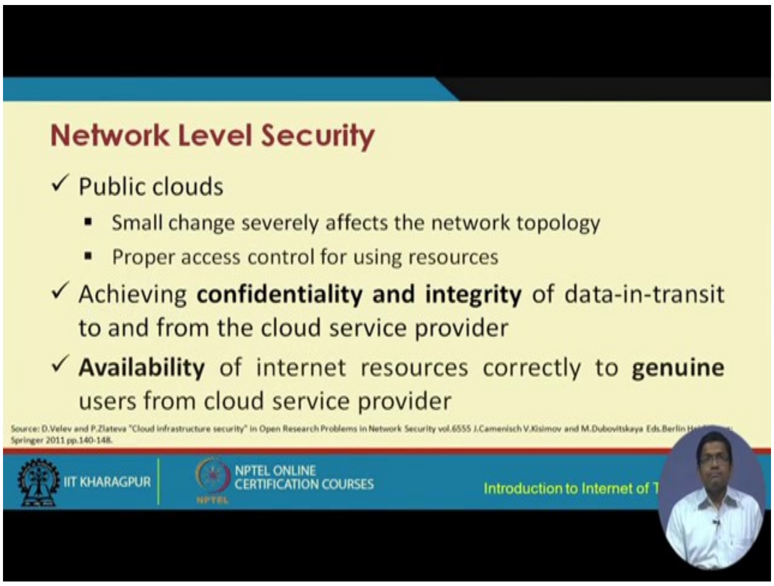
So, the problem is that the user in a cloud platform would essentially lose control of the information that is available on the public cloud. So, concerns more specifically about the loss of data seizing of the account service traffic hindrance vulnerability of APIs are paramount in the case of cloud and the security of cloud. So, these security concerns have to be taken care of in addition to any other IT security issues that you already know. So, the solution is to have counter security solutions, platforms APIs you know applications software etcetera, etcetera which will protect from theft leakage of data deletion of data accidentally by providing security policies by providing security policies.

(Refer Slide Time: 16:32)



So, security of cloud infrastructure must be implicitly assured for public or private cloud for services such as SaaS, PaaS and IaaS building levels of viewing evaluating and executing infrastructure security include network level security host level security and application level security.

(Refer Slide Time: 16:54)



In the case of public cloud we have to ensure that the small change does not severely affect the network topology and there has to be proper access control for using resources. So, this is a network level issue and that has to be ensured. Second thing is achieving you know character traits like confidentiality and integrity of data in transit to and from cloud service provider.

So confidentiality of data see as you know that data confidentiality integrity availability and non repudiation are very much important issues in the context of security. So, achieving at the network level achieving confidentiality and integrity of data in transit data flowing into the cloud and coming out of the cloud has to be insured by the cloud service provider and the security rather the confidentiality.

(Refer Slide Time: 18:13)

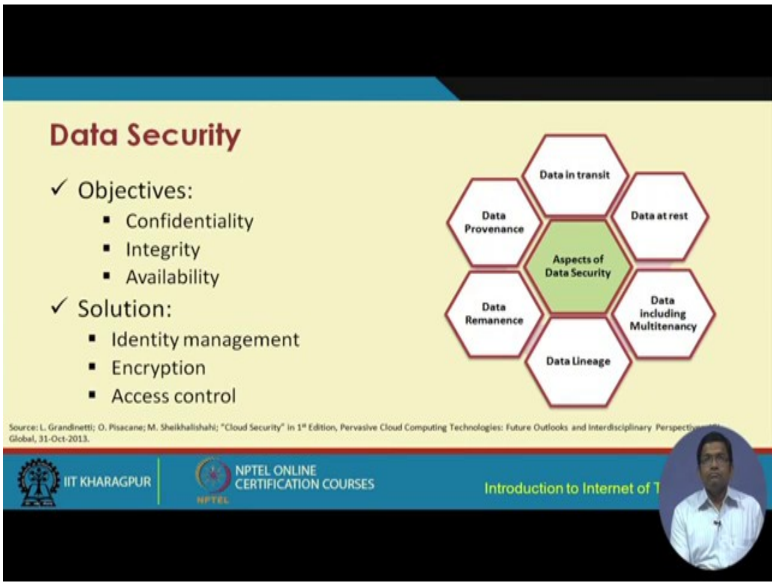
And integrity of it availability of internet resources correctly to genuine users from the cloud service provider is another issue of concern at the network layer at the host layer issues particularly at the PaaS and the SaaS level include hiding the host operating system from the end users and ensuring to delegate security responsibilities to the cloud service providers. Host security at IaaS level include the objective of securing the allocated hosts with the help of different software etcetera to ensure that attacks such as the blue pill attack on the hypervisor which is a core component of IaaS platforms is mitigated or is taken care of blue pill attack as you may be already aware is a specific type of attack on the hypervisor and hypervisor is what I have already explained in the previous lecture on cloud. So, hypervisor you know the virtual machines sit on top of the hypervisor; hypervisor is tasked to manage these virtual machines.

(Refer Slide Time: 19:31)

So, blue pill attack is a very popular form of attack on the hypervisor and that kind of threat has to be taken care of at the host level. At the application level both the CSP and the customer are responsible for security at the application level. So, it is you know here specifically the application at the application level not just the CSP the customer also has to take care.

so if it is a SaaS provider SaaS cloud service provider taken care of the security of deliverable applications is there you know should be their main focus from a security perspective from for PaaS providers security of the PaaS PaaS platform; that means, the platform which is offered as a service for development it is a Google app engine kind of environment you know its security etcetera has to be taken care of and the deployed customer applications security of the deployed customer applications. So, that is also another concern at the IaaS level IaaS providers level the application level security is not provided by IaaS customers arrange for the security mechanism themselves.

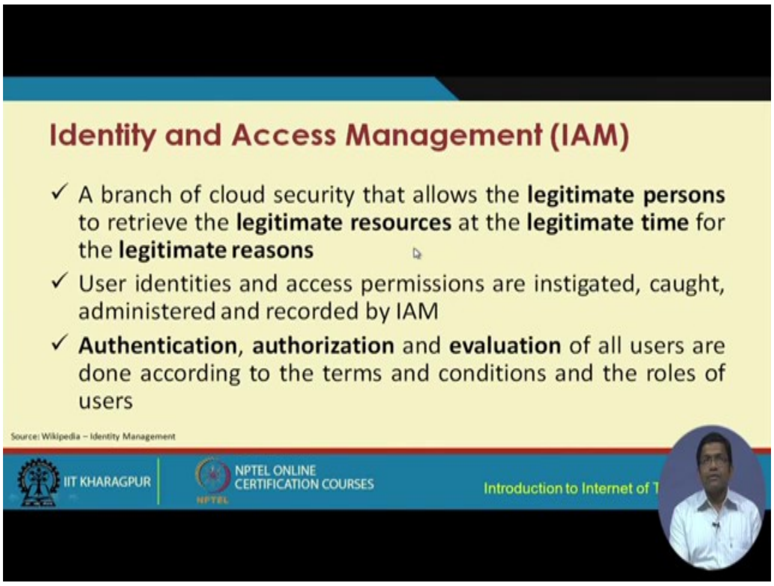
(Refer Slide Time: 20:47)



So customer has to take care of the security themselves data security has different objectives and the corresponding issues objectives include confide ensuring confidentiality of the data integrity of the data and availability what does confidentiality means that the data should be confidential and should be made available to only the intended stakeholder integrity means that the data should not be tampered with in between. That means, when it is flowing into the cloud or coming out of the cloud and availability means that the data should be made available as per the service level agreement to the intended customers in a secured manner.

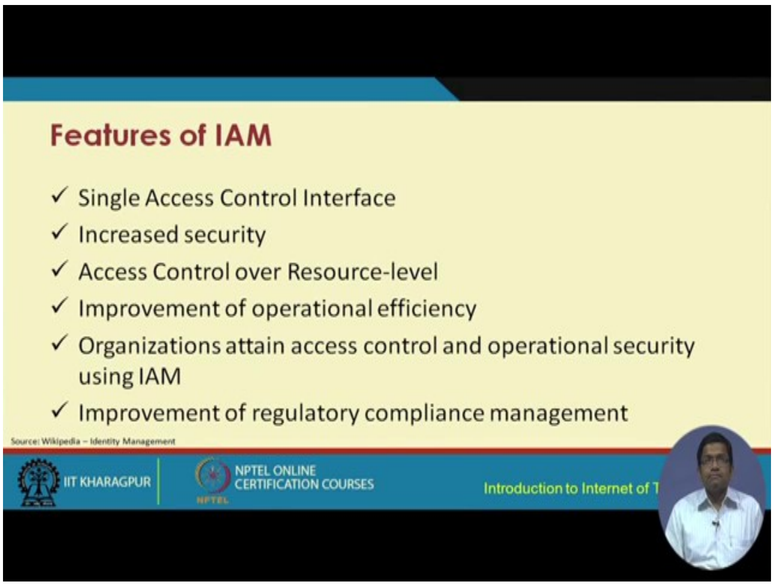
So that different solutions include you know using identity management techniques encryption access control and so on. So, there are different aspects of data security data provenance, data in transit, data at rest data at rest means the data that is used for long term use that is data at rest I mean which does not change to fast and it will be there in the server for long term use you know in the future and so, on data including multi tenancy and the data lineage. So, data lineage means data lineage data remanence and data provenance these are the issues with the data. So, data lineage means like from the start you know the from the source till the data is used you know ensuring the security of it and you know similarly the data remanence basically takes care of that whenever the residual data etcetera, etcetera you know securing that data you know keeping track of the data that basically has to be taken care of.

(Refer Slide Time: 22:45)



So like these actually these are the different issues of data security. So, let us first talk about identity and access management IAM which is basically a branch of cloud security that allows the legitimate persons to retrieve the legitimate resources at legitimate time for legitimate reasons. So, legitimate persons retrieving legitimate resources at legitimate time for legitimate reasons is basically the issue the main issue behind identity and access management in cloud security here the users the user identities and the access permissions are instigated caught administered.

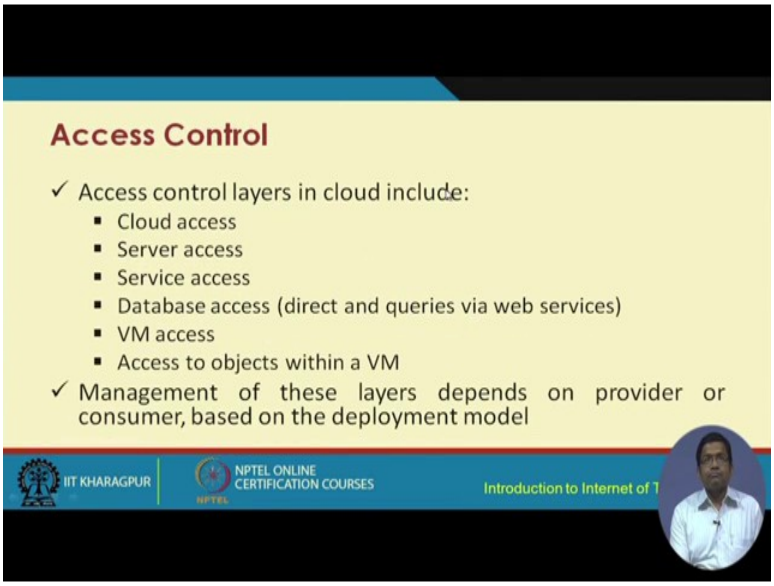
(Refer Slide Time: 23:38)



And located recorded by IAM; that means, the identity and access management module authentication authorization and evaluation of all resources are done according to the terms and conditions and the roles of the users.

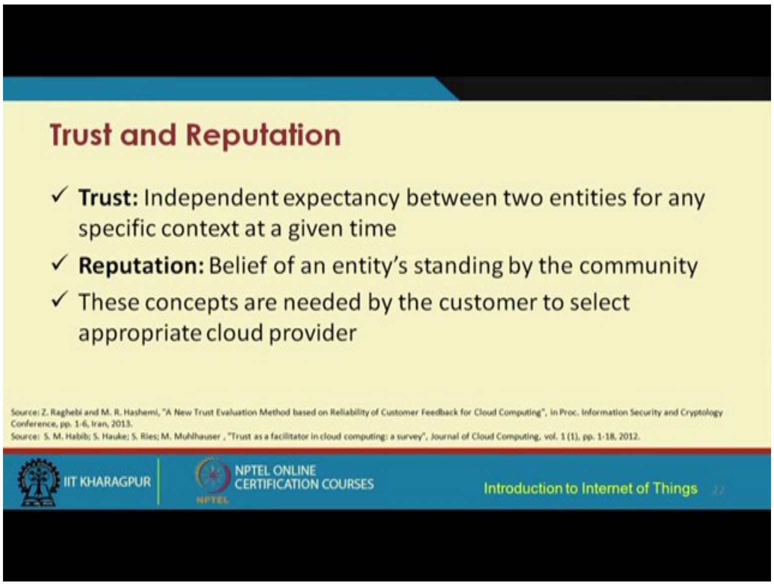
Features of this module include single access control interface, increased security, access control over resource level, improvement of operational efficiency organizations attaining access control and operation security using this module and improvement of regulatory compliance management access control is very important in cloud.

(Refer Slide Time: 24:02)



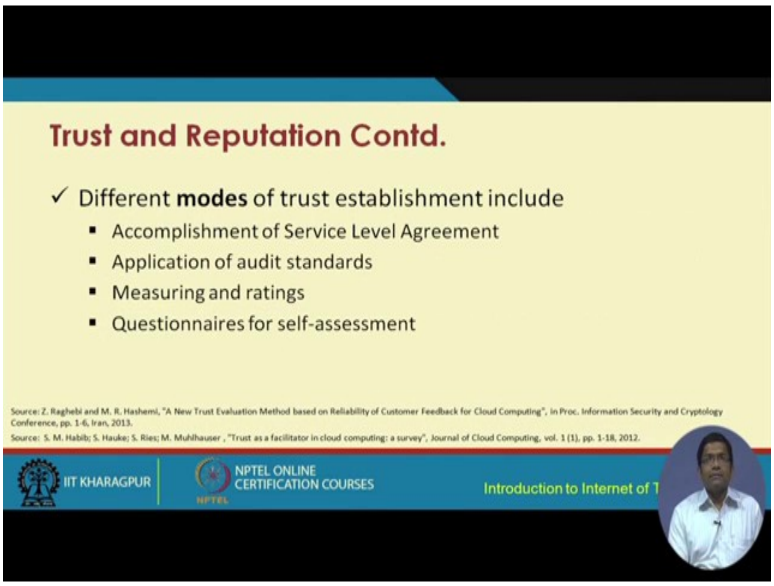
So, service providers have to take care of it explicitly. So, access control layers in cloud include cloud access server level access service level access database access both directly and indirectly directly the queries should be sent via web services. So, taking care of that and VM access virtual machine level access to objects within a virtual machine.

(Refer Slide Time: 24:49)



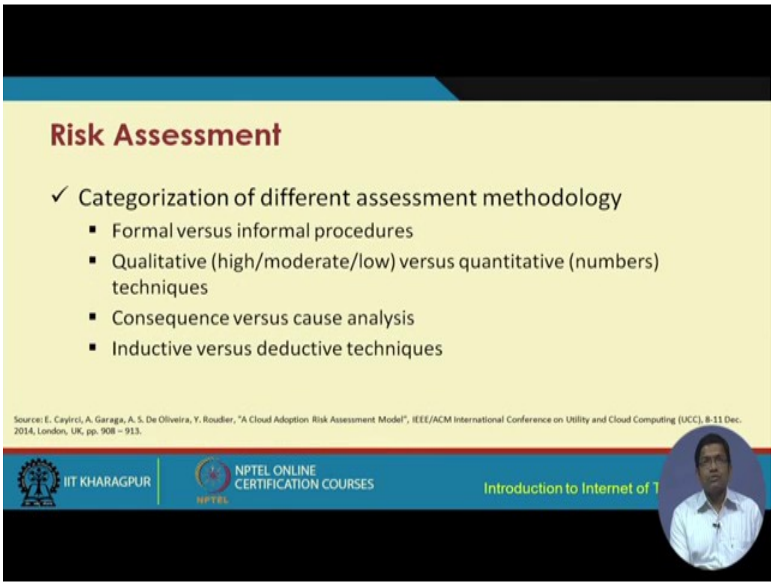
So these are the different levels of access and the control of access to these differently layers has to be taken care of management of these layers depends on the provider or the consumer based on the deployment model. Trust and reputation are very important trust basically takes care of issue of independent expectancy between 2 entities for any specific context at a given time independent expectancy; expectancy between 2 entities. So, they have to trust each other and at the same time hand in hand comes the issue of reputation and reputation is about the belief of an entity; entities standing on the community you know what does the entity have you know what is its reputation in the community.

(Refer Slide Time: 25:37)



So these are the 2 different issues that that goes hand in hand. So, these concepts are needed by the customer to select appropriate cloud provider. So, there are different models or sorry rather different modes of trust establishment. So, these include accomplishment of service level agreement. So, whatever service level agreement exists you know accomplishing it then application of the audit standards that are out there you know whether the audit standards have been adequately applied or not measuring and rating and questionnaire for self assessment.

(Refer Slide Time: 26:11)



So, these are the different levels of trust access trust establishment that has to be there there. Risk assessment categorization of different assessment methodology formal versus informal procedures of risk assessment qualitative versus quantitative methods of risk assessment qualitative means that high risk moderate risk low risk versus quantitative means numeric risk figures consequence versus cause analysis. So, whether the risk is due to a consequence of something or what is the cause behind the risk and inductive versus deductive techniques.

(Refer Slide Time: 26:50)

So, these are the different categories of risk assessment in cloud authentication in cloud computing user authentication. So, there are different aspects like what where user authentication process which takes care of the user authentication process between the new users and the service provider when during the authentication the properties and the safety of process which can be invaded by attacks causing severe damages and where the user authentication is done at the PaaS layer and the consequence is threat to authentication process can lead to divulge; divulge divulgation divulging of confidential data to a fake user.

So, with this we come to 2 broad main issues in cloud computing one is taking care of the service management with the help of SLAs between the customers and the service providers, number 2 is this issue of security; security of infrastructure, security of the platform, security of the software and the data security data security is very much important. Customers did not know really that where their data is going to reside how the data is going to flow around in the system and that has to be assured to the customer that their data is going to be safe. So, taking care of measures to ensure that there is enough security of the data and the parties can trust each other you know that also has to be ensured through the process of some kind of reputation tracking and ensuring that those reputation measures are basically disseminated for you know developing trust between these different parties. So, these all these things have to be ensured in order to meaningfully use cloud in a commercial or any any kind of environment.

Thank you.

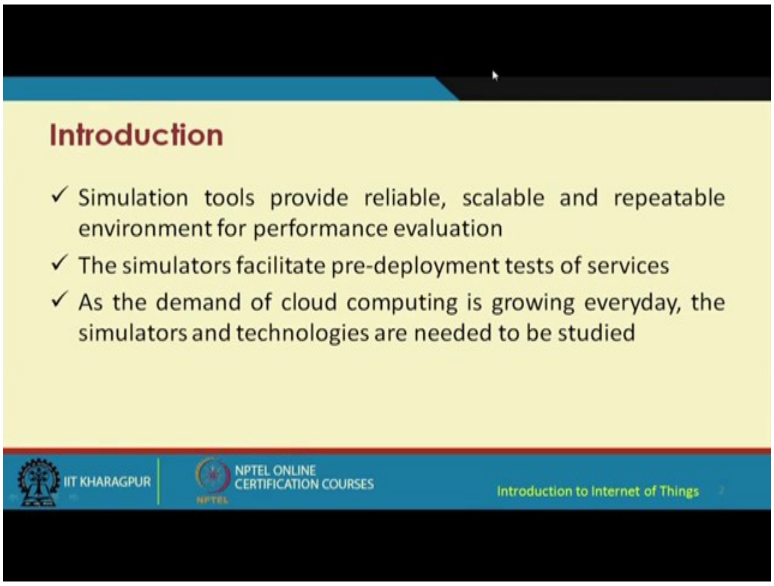
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 40
Cloud Computing- Case Studies

The current lecture on cloud is on some case studies and more specifically case studies related to the available cloud platforms and including the Cloud Simulation platforms. So, we are going to go through some of them. So, before I start I would like to mention that you know before even before the adoption of cloud whether it is for R and D purpose or whether it is for actual use in a business it is required to assess this particular technology the different solutions that are offered by this technology it is required to assess. So, how can we assess one of the ways is through simulations. So, there are different simulations platforms that have been that are made available by different community groups. So, we can use those in order to assess how cloud is going to perform what are the different modules what are their implications on the overall performance of the system and so on. So, that is a very important aspect of cloud computing.

So, I will go through some of these different Cloud Simulation platforms, but before that I would like to make you understand some of these issues of simulation. So, first of all the simulation tools would be required to ensure reliability, scalability and repeatability for of performance evaluation.

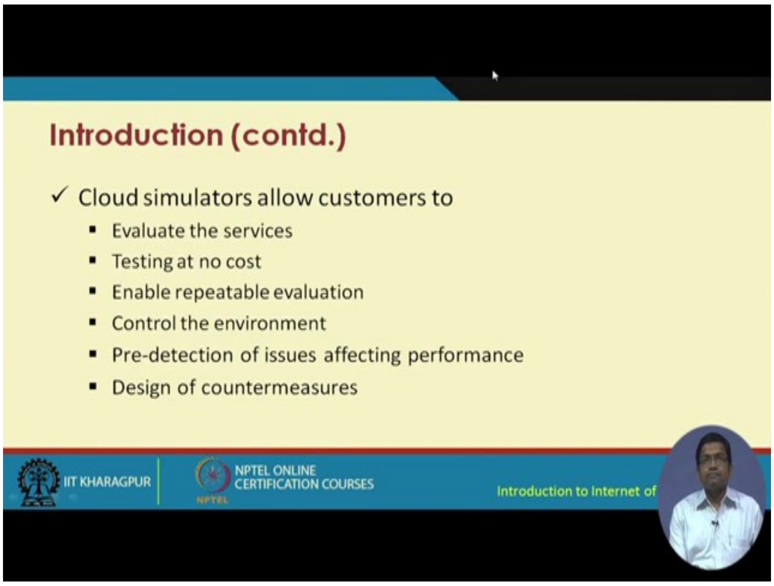
(Refer Slide Time: 01:52)



So, you know we have to ensure that the system is reliable even before it is used it is scalable and the data that we are getting you know that is repeatable. So, we have a repeatable environment which will give you the same or similar kind of data even if you rerun the same simulation over time you know you run in you know at different instants of time you know you have a repeatable environment which will give you similar kinds of data. So, that is very much required for performance evaluation.

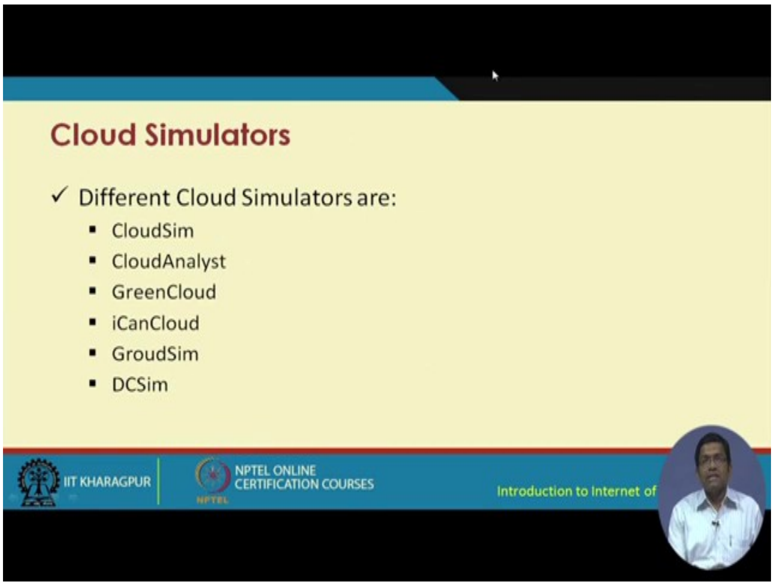
The simulators basically facilitated pre deployment tests of services then that is basically quite generic as well I mean not just specific to cloud any simulator even mean what a simulator does is even before you deploy the infrastructure the services is the platform as a whole you need to test how it is going to work. So, this is another purpose of the simulator and the third is as the demand of cloud computing is going every day the simulators and technologies are needed to study how things how different features which are going to be enabled which are going to be added additionally how they are going to perform in the cloud environment.

(Refer Slide Time: 03:15)



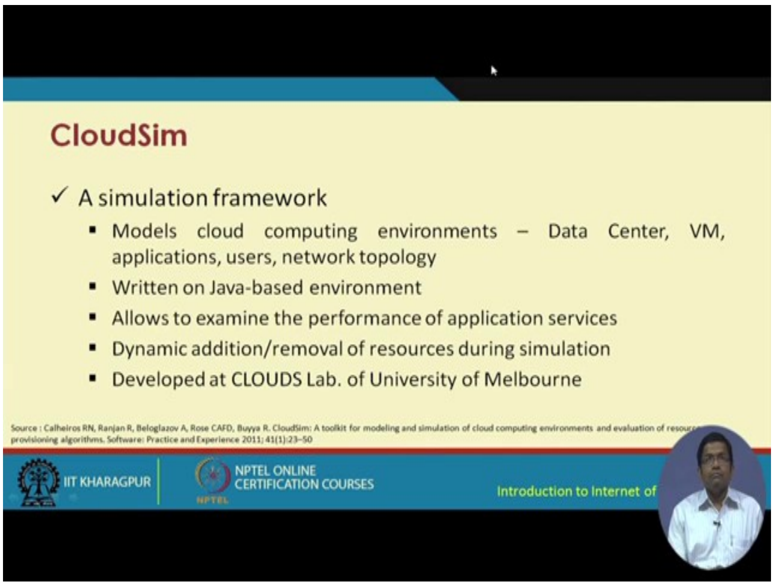
So, Cloud Simulators allow the customers to evaluate the services to test the services and the platform at no additional cost because no additional infrastructure is going to be taken enabling a repeatable evaluation repeatability I have already mentioned to you controlling the environment pre detection of issues affecting performance pre detection means even before actually the cloud is deployed you want to pre detect what are the issues that are going to be there which would be affecting the performance of the cloud environment and that has to be done even before the deployment is going to take place. So, Cloud Simulator will help you do that and designing of the countermeasures in the case of you know the performance degradation due to some issues or you know certain things going wrong.

(Refer Slide Time: 04:07)



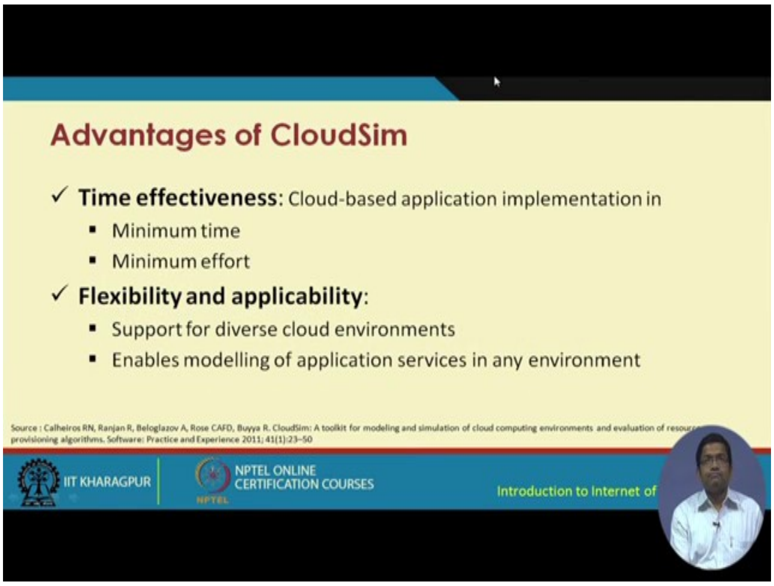
So, what are the counter measures that have to be taken and you know designing that and evaluating those aspects different Cloud Simulators that are available include CloudSim which is probably one of the most popular you know simulation platforms that is available in the community CloudAnalyst is another one third is green sorry, GreenCloud. Next is iCanCloud, the next one is GroudSim and the last one is DCSim in this particular list. So, these are some of the some of the CloudSimulators that are available for use if you want to simulate cloud before actually deploying cloud.

(Refer Slide Time: 04:52)



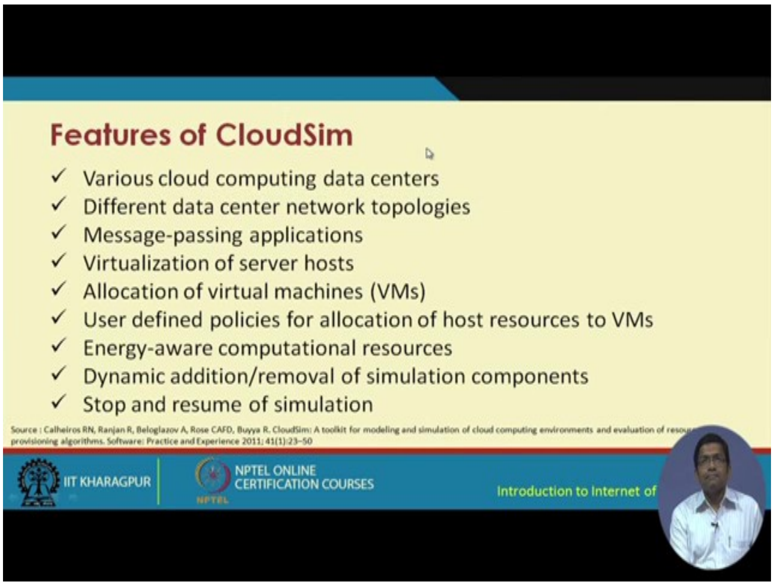
So, CloudSim is a simulation platform as I said before which has different modules which has different classes for different cloud computing environments including modules for data center you know for modeling data centers modules for data center virtual machines applications users network topology. So, there are different types of modules and their corresponding models that are made available it is CloudSim is based on a java based environment it is written on a java based environment that allows to examine the performance of application services. It is also possible to dynamically add and remove resources in CloudSim and CloudSim was developed at the University of Melbourne by the team led by Professor Rajkumar Buyya, he is very much popular in cloud computing and in his lab the clouds lab of the University of Melbourne this CloudSim platform was developed.

(Refer Slide Time: 06:03)



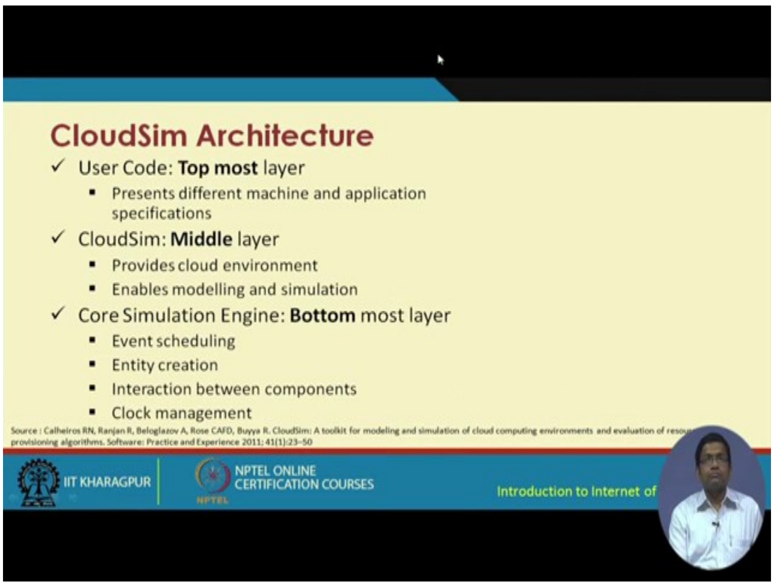
The advantages of CloudSim include taking care of time effectiveness. So, cloud based applications implementation has to be done in minimum time with minimum effort. So, time effectiveness is one second thing is dealing with fix flexibility and applicability supporting you know the use of diverse cloud environments enabling the modeling of application surfaces in any environment.

(Refer Slide Time: 06:36)



These are the some of the advantages of CloudSim. Features of CloudSim include I will just read from this list and because these are quite self explanatory I would simply lead them without actually needing to expend them in further detail. So, features include various cloud computing data centers different data center network topologies message passing applications virtualization of server hosts allocation of virtual machines user defined policies for allocation of host resources to virtual machines energy aware computational resources dynamic addition or removal of simulation components and stop and resumption of simulation.

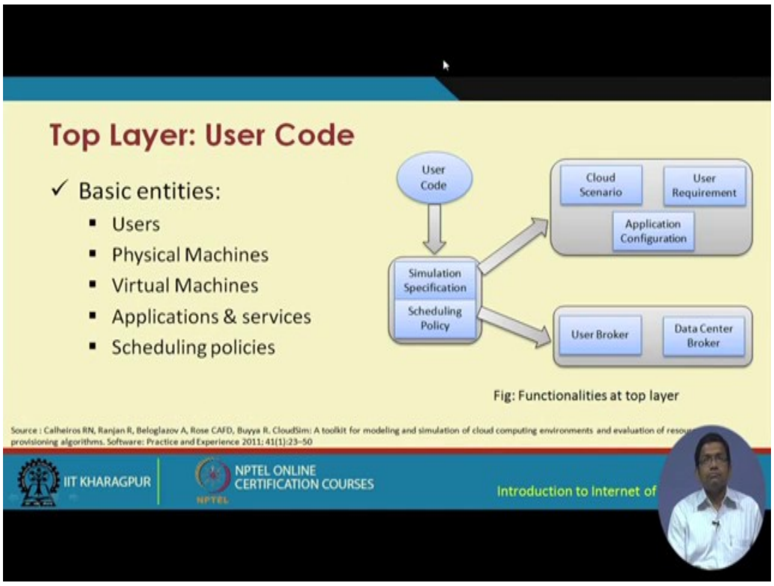
(Refer Slide Time: 07:26)



So, these are some of the features that are supported by CloudSim. In the CloudSim architecture we have different layers the topmost layer is the user code layer which basically presents the different machine and application specifications the middle layer is actually the CloudSim layer which provides the actual cloud environment. And also enables modeling and simulation of cloud and the bottom most layer is known as the core engine core simulation engine layer and these basically takes care of event scheduling event scheduling means because we are dealing with discrete event simulation different events like the creation of the virtual machine, the porting of the virtual machine on the host and so on.

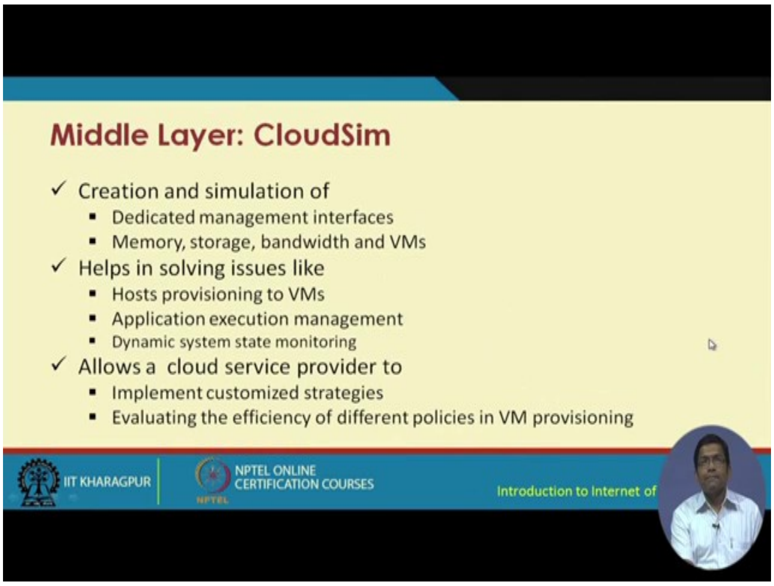
So, these are like discrete different events. So, scheduling of the events is taken care of at the bottommost layer the core engine layer creating these different entities these different virtual machines the data centers etcetera. Entity creation is also done at the core engine layer interaction between the different components the clock management because you know there is actually a clock class from which you know the whatever you know entities you borrow you inherit you know you have to take help of the clock; that means, the time you will be required to be inherited. So, that these different entities are time synchronized and overall we have a clock managed solution.

(Refer Slide Time: 09:05)



The top layer basically has different entities such as the users the physical machine the virtual machines the applications and surfaces and scheduling policies. So, basically I will show you with the help of this particular figure. So, what will happen is you have this user code and then you have the simulation specification and the scheduling policies. So, simulation simulation specification and you know the scheduling policy again breaks into 2 parts one is the application configuration which has sorry as a application configuration the cloud scenario and the user requirement. So, this is basically that simulation specification. So, this is taking care of by these three different components the cloud scenario user requirement and application configuration the scheduling policy is taken care of by this subcomponents which is basically the user broker.

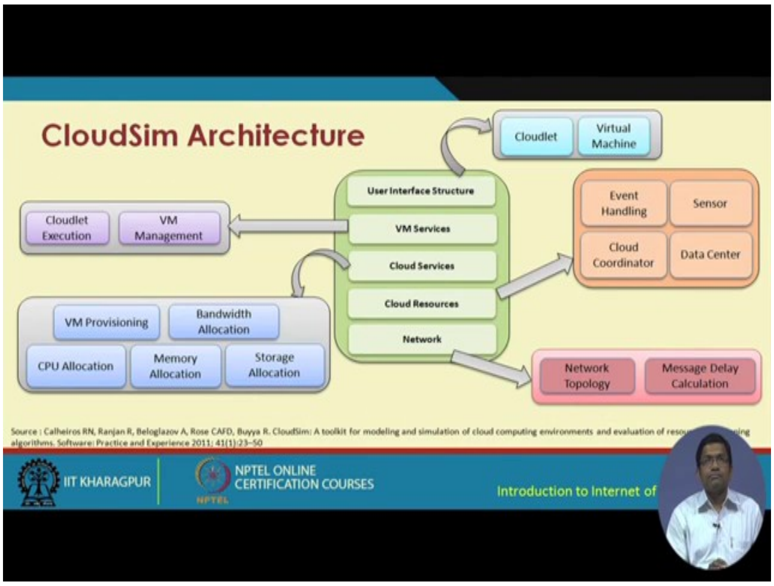
(Refer Slide Time: 10:05)



And the data center broker the middle layer is basically the CloudSim layer which takes care of the creation and simulation of dedicated management interfaces issues such as memory management storage bandwidth and virtual machine creation and simulation are taken care of at this layer.

This particular layer helps in solving issues like host provisioning to virtual machines application execution management and dynamic system state monitoring it allows a cloud service provider to implement customized strategies evaluating the efficiency of different policies in virtual machine provisioning here is the overall CloudSim architecture.

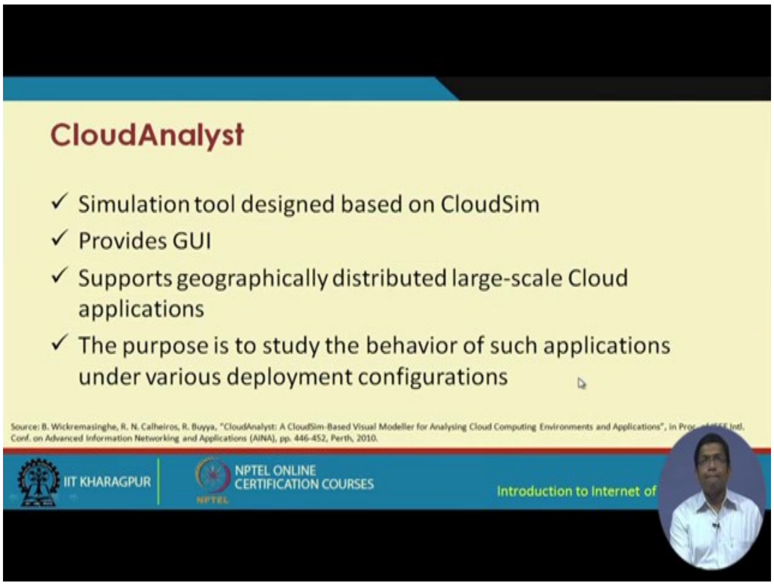
(Refer Slide Time: 10:45)



So, we have different layers in CloudSim we have the user interface structure the virtual machine services cloud services cloud resources and network. So, these are the different components of the cloud same.

So, user interface structure has 2 different sub components the cloudlet and the virtual machine. So, cloudlet is sort of like a small physical server which will put the you know which will create these virtual machines then we have what the virtual machine services constituting the cloudlet execution of the cloudlet that is created and the virtual machine management. Then we have the cloud services comprising of virtual machine provisioning bandwidth allocation CPU allocation memory allocation and storage allocation then we have the fourth one which is the cloud resources component of the layer which includes event handling sensor management data center and the cloud coordinator and then we have the network layer which takes care of the network topology and message delay calculation.

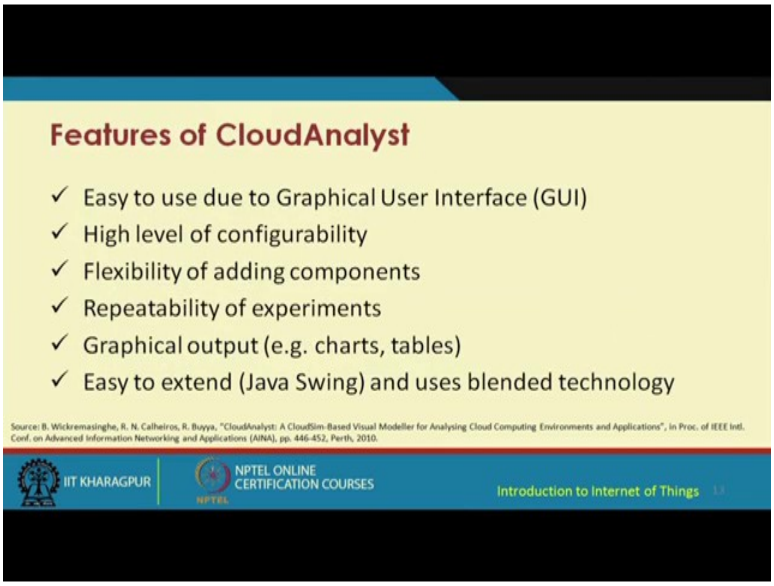
(Refer Slide Time: 12:02)



So, that was the CloudSim another production another system which works on top of CloudSim is the cloud analyst which is a product that was again developed by the group led by Professor Rajkumar Buyya.

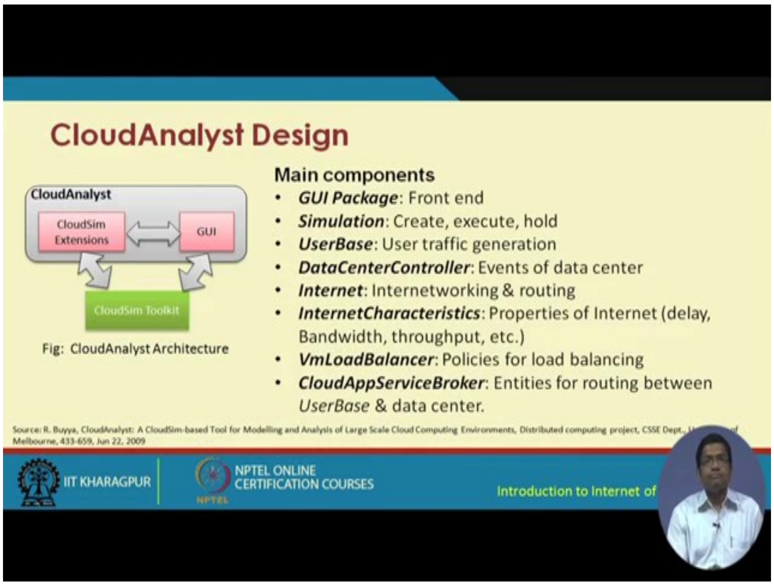
So, the crowd analyst is a simulation tool designed on top of cloud seemed to provide a graphical user interface that will support geographically distributed large scale cloud applications the overall purpose of cloud analyst is to study the behavior of such applications under different deployment configurations. So, basically this cloud analyst will have different metrics to trick take care of the performance of this cloud the different parts of the cloud and so on.

(Refer Slide Time: 12:54)



The features of cloud analyst include it is easy to use due to the availability of GUI it has high level of configurability it has a feature of flexibility of adding different components repeatability of experiments graphical output provisioning with the help of charts and tables.

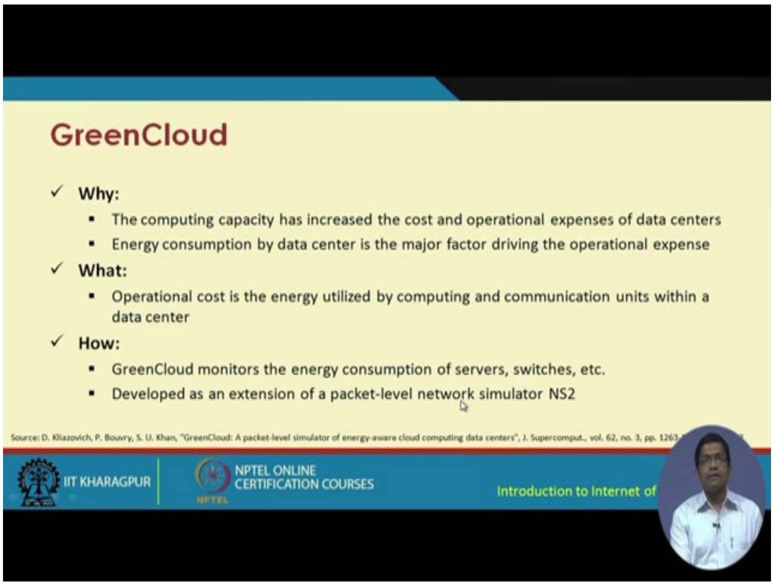
(Refer Slide Time: 13:25)



And easy extend extensibility with the help of java swing and different other technologies the cloud analyst architecture is given in front of you in the figure. So, we have 2 main components one is the CloudSim extensions by offering different metrics different you know different extensions that will help you to analyze what is going on how the cloud is behaving and so on and the graphical user interface. So, this interaction with the core CloudSim and the different components the 2 components of cloud analyst are shown in this particular figure.

So, the cloud analyst list basically comes with different components such as the GUI package for front end development the simulation, simulation component which basically creates executes and holds virtual machines then we have the user base for user traffic generation data center controller internet for internet working routing networking network provisioning. So, on internet characteristics component which basically takes care of properties of the internet with respect to delay bandwidth throughput etcetera the VM load balancer which takes care of issues of policies for load balancing and the cloud app service broker which takes care of entities for which has entities for routing between the user base and the data center.

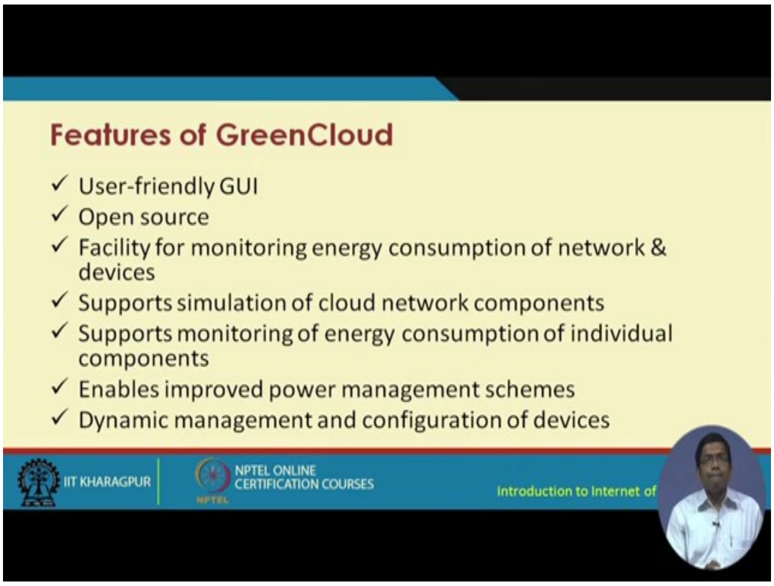
(Refer Slide Time: 14:47)



So, why do we need GreenCloud. So, sorry, so, that was the cloud analyst and now we have another Cloud simulation platform which is known as the GreenCloud. So, why do we need GreenCloud. So, in GreenCloud, by the way this GreenCloud was developed by a team of US and Europe. Pascal Bouvry group and Samee Ullah Khan you know from the University of North Dakota and Pascal Bouvry from University of Luxembourg in Europe. So, they together came up with discrete GreenCloud platform which is again a packet level simulator which is energy aware and that basically helps in reducing the overall you know energy expenses with the help of energy expenses in the adoption of cloud.

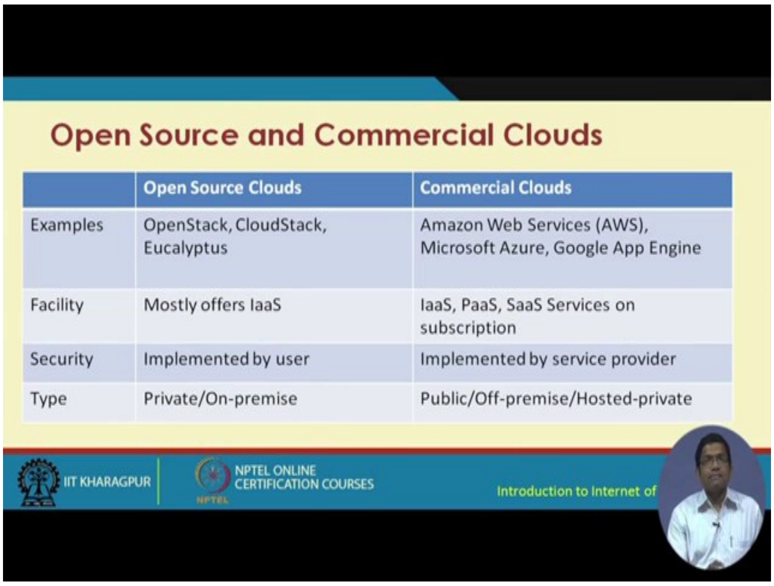
So, why do we need GreenCloud the computing capacity has increased the cost and operational expenses of data centers. So, energy consumption by data center is the major factor that drives the operational expenses. So, what is GreenCloud it offers operational cost. So, operational cost is the energy utilized by computing and combination communication units within a data center and how that is done GreenCloud basically monitors the energy consumption of the servers the switches etcetera and it is developed as an extension of NS2 packet level network level network simulator.

(Refer Slide Time: 16:30)



The features of GreenCloud are listed over here I would just read read it out for your convenience. So, number one feature is that it is it offers a user friendly graphical interface, number 2 is it is open source. Next is the facility for monitoring energy consumption of network and devices, forth is that it supports simulation of cloud network components, fifth is it supports monitoring of energy consumption of individual components. Next is that enables improved power management schemes which is very much important in the context of this particular simulator energy consumption monitoring and reduction is an important feature that is offered by GreenCloud and the last one last feature is dynamic management and configuration of devices.

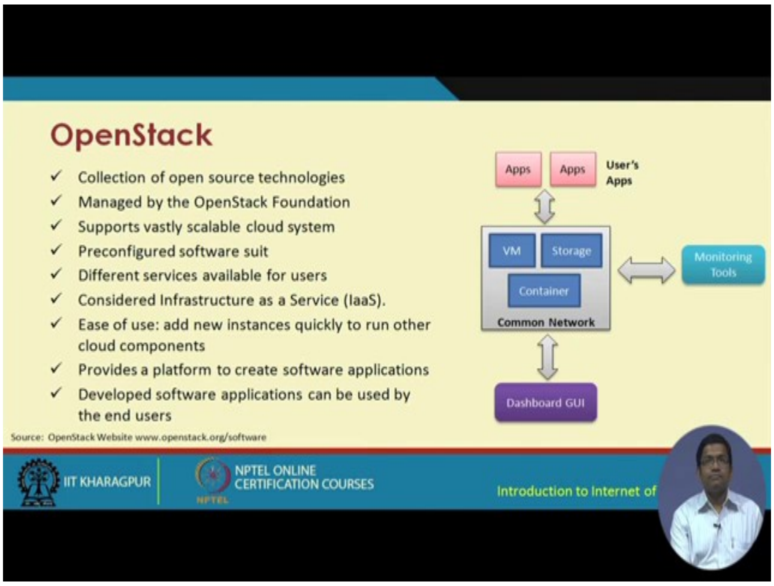
(Refer Slide Time: 17:23)



So, those were the simulators now let us talk about some real commercial and open source cloud platforms that are available for use. So, some examples of opens open source cloud include OpenStack; CloudStack eucalyptus and so on commercial cloud platforms include Amazon web services, Microsoft azure, Google app engine and so on. So, now, let us look at the open source cloud platforms these open source cloud platforms mostly offer infrastructure as a service whereas, the commercial ones offer in addition to infrastructure as a service platform is a service software is a service. So, on a subscription basis or; that means, on a payment basis in terms of security these security issues are implemented by the user; that means, by the customer at the user end and commercial clouds these are implemented the security aspects are implemented the security components are implemented by the service provider.

So, here the type of the cloud is private on premise; that means, in the facility of the user the cloud will be installed and so on premise and the commercial clouds are basically public off-premised. So, these are not available on the campus on the in the institutional premises and so on. So, these have to be available made a these are made available to the public and these have to be subscribed to over the internet.

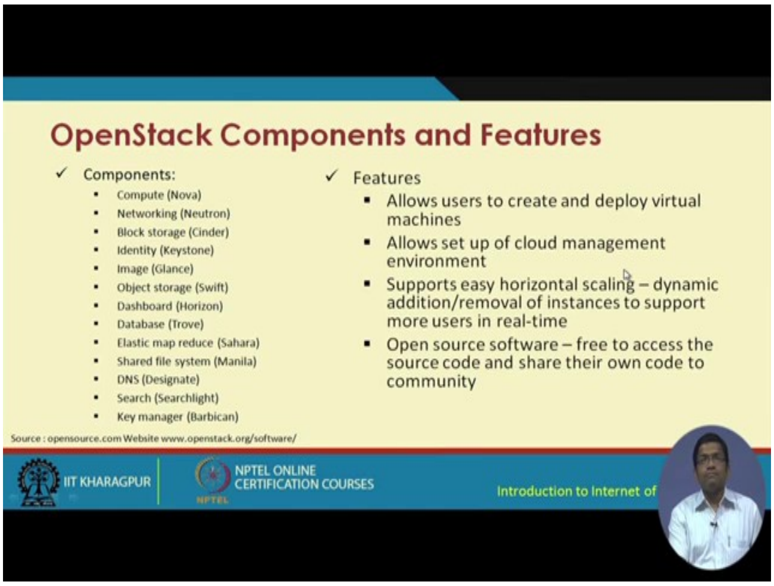
(Refer Slide Time: 19:03)



So, OpenStack is one very popular form of a cloud platform that can be used. So, OpenStack is a collection of open source technologies that is managed by the OpenStack foundation it supports vastly scalable cloud system it has preconfigured software units different services are available for the users it considers infrastructure as a service. So, OpenStack basically supports IaaS and not a SaaS or PaaS it is easy to use because you know one can easily add new instances and can quickly run different cloud components it provides a platform to create software applications and has been developed it has developed software applications which can be used by the end users.

So, this is basically the schematic of OpenStack. So, we have the common network component which includes a container storage and virtual machine. So, this is basically the common network component then you have these different apps at the user's apps layer and then it also connects with the dashboard geographical interface.

(Refer Slide Time: 20:20)



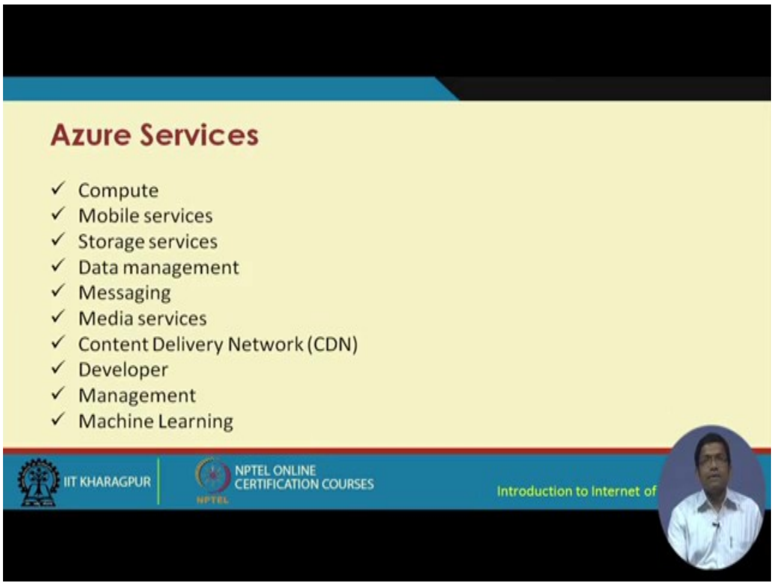
And the different monitoring tools are also available through the OpenStack platform OpenStack has different components and features. I am not going to go through, but as you can see over here they have different components for computation networking storage you know and so on and so forth database etcetera, etcetera and they have different names for each of them nova neutron cinder glance keystone swift horizon trove etcetera, etcetera.

These different components have their own different names the features include allowing users to create and deploy virtual machines allowing the setting up of cloud management environment supporting easy horizontal scaling. That means, dynamic addition and removal of instances to support more users in real time and open source software this is open source software which is freely accessible to anyone we along with the source code which can be shared to shared in order to share with the community for the deployment and use of this platform.

(Refer Slide Time: 21:23)

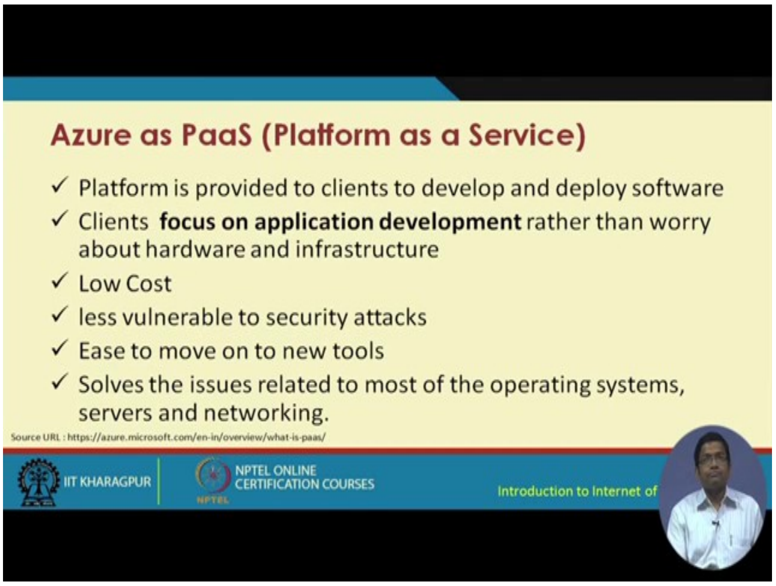
Microsoft azure is available on a payment basis it is not free it you know earlier it actually it used to be known as the windows azure it supports infrastructure as a service and as and also the platform as a service. So, infrastructure as a service was also offered by OpenStack, but not platform as a service. So, this paid software Microsoft azure basically comes with the platform as a service in addition to the infrastructure as a service it supports extensive set of surfaces to quickly create deploy and manage applications there are many many programming language support and frameworks that are available in this particular platform the azure platform and it is available across a worldwide Microsoft managed data centers.

(Refer Slide Time: 22:11)



So, these are the different advantages of Microsoft azure and here the list of different services that are supported by as your are given in front of you we have support for computing support for mobile services storage services data management messaging media services content delivery content delivery means that you know something like offering different types of media you know etcetera through platforms like YouTube and so on.

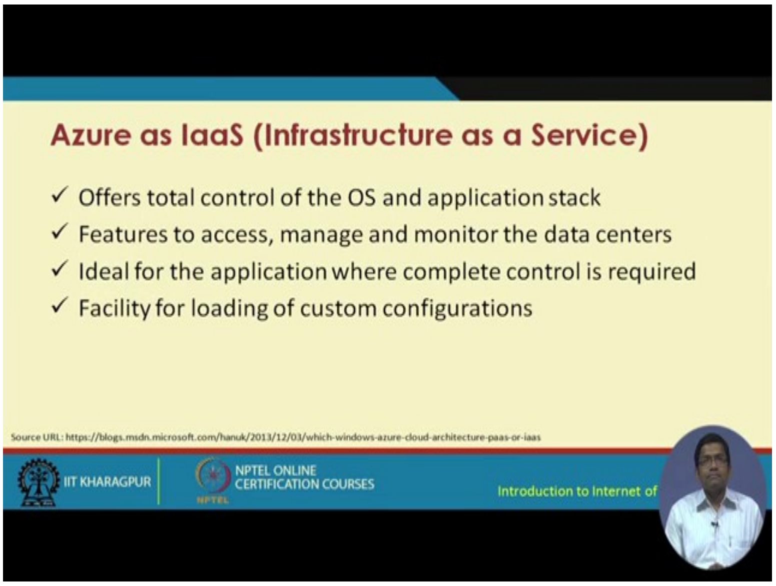
(Refer Slide Time: 22:47)



So, content delivery network developer you know developer services management services and machine learning support. Azure as a platform as a surface PaaS platform is provided to clients to develop and deploy software. So, this is very important. So, when we talk about platform as a service we are talking about some platform that is offered for the development of the software to the clients you know clients get the development platform for use on a after makings the payments.

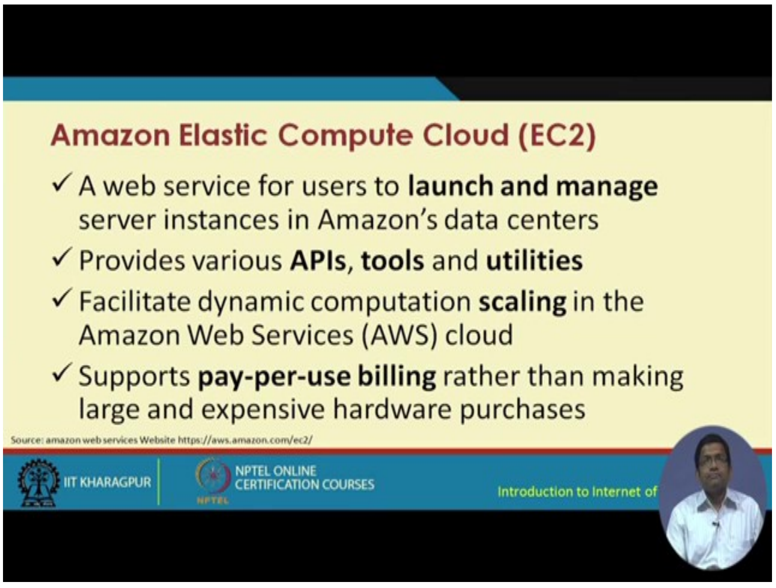
So, clients basically focus on application development rather than worrying about the hardware and the infrastructure Azure is low cost is less vulnerable to security attacks as claimed by them then it is easy to move on to new tools with the help of azure it also solves.

(Refer Slide Time: 23:36)



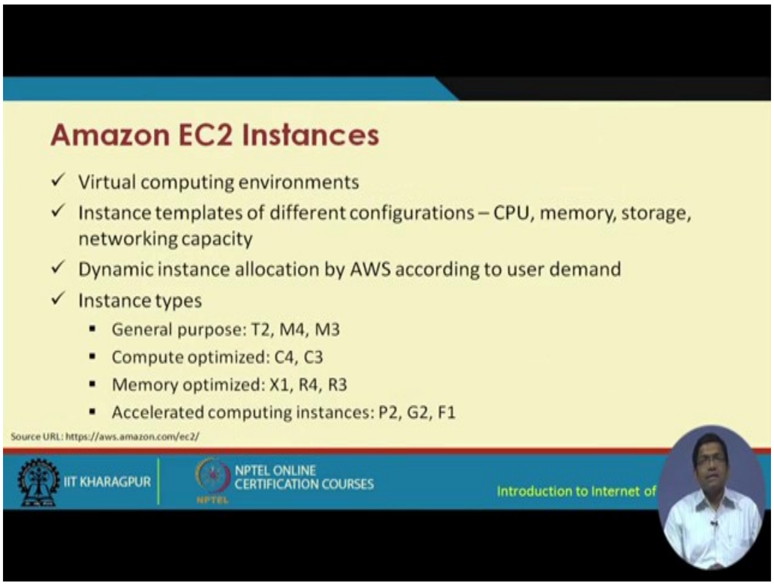
The issues related to most of the operating system servers and networks. Azure as infrastructure as a service the previous one was platform as a service. And the next one is infrastructure as a service in this particular module it offers total control of the operating system and the application stack it has features to access manage and monitor the data centers and it is ideal for the application where complete control is required.

(Refer Slide Time: 24:02)



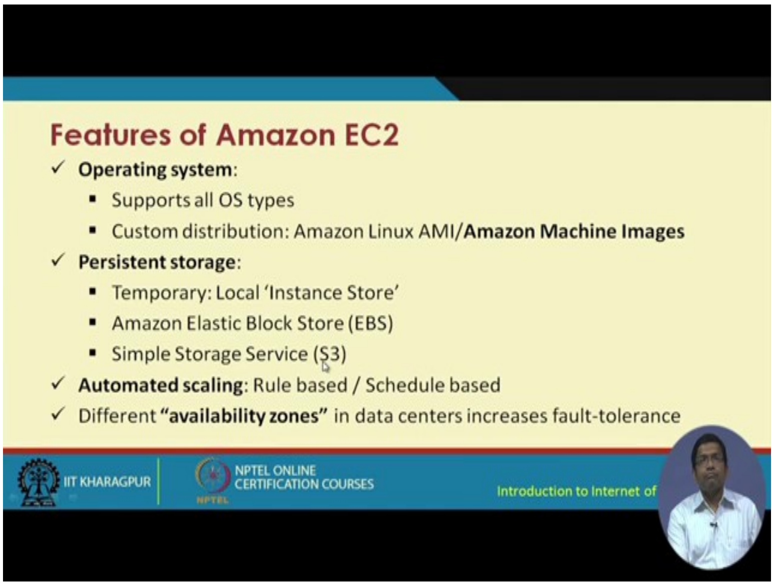
The next one which is also quite popular is the EC2 Amazon platform EC2 elastic compute cloud the name says it actually the advantages of Amazon EC2 is evident from the name. So, a web service for users to launch EC2 is a web service for users to launch and manage the server instances in Amazon's datacenter it provides various APIs tools and utilities it has the facility for dynamic computation scaling in the AWS cloud and it supports paper use billing rather than making large and expensive hardware purchases. So, Amazon has different is EC2 Amazon EC2 has different instances.

(Refer Slide Time: 24:42)



So, these instances are of different types for different serving different purposes and their specific names that are given by them in EC2 are also listed over here.

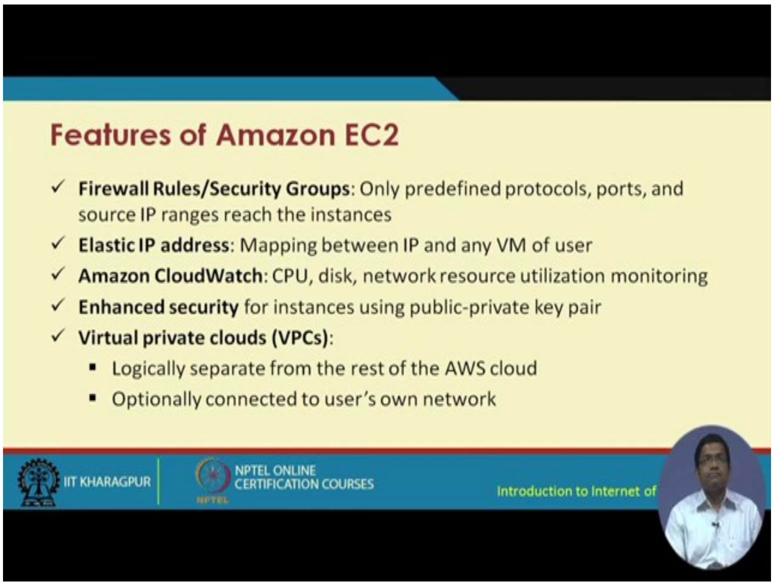
(Refer Slide Time: 25:02)



So, in terms of the operating system EC2 basically supports all operating systems in terms of storage it has temporary storage for local instance store which is a local instance store and also the Amazon elastic block store the EBs and the third is the simple storage service(S3). So, these are the persistent storage mechanisms that are available to a in EC2 then the automated scaling, which is basically for horizontal scaling where there are rules and schedules that are given and the scaling is going to be on the basis of that there are different available zones in the data centers that basically increases fault tolerance.

So, EC2 basically comes with the concept of available zones availability zones. So, in the availability zone basically it is designed, the zones are designed in such a way that if there is some component that goes down there will be some other component that is going to automatically take over.

(Refer Slide Time: 26:18)



So, the zone basically at the time of creation basically ensures that such availability is there. So, that basically improves the overall fault tolerance in data centers.

Features of Amazon EC2 also include firewall support for firewall rules and securities overall there is predefined protocol ports etcetera which has source IP ranges supporting different firewall rules and security mechanisms elastic IP address mapping which basically maps between the IP and the VM of users. So, what you have essentially is one pool which is basically the IP address pool the other one is the pool of virtual machines that can be created for the user. So, basically this elastic IP addressing will map between the IP addresses and the virtual machine and the corresponding virtual machine.

Amazon CloudWatch CPU disk network resource utilization monitoring these are some of these functions of CloudWatch then you have the enhanced security mechanisms as features in EC2 and the last one that I would like to mention specifically is the formation you know is the availability of feature for creation of virtual private clouds. So, which will basically logically separate the private clouds not private cloud, but it is sort of like a virtual private cloud. So, I can install in my lab a virtual private cloud which will be logically separating from the rest of the Amazon web services cloud and this can be optionally connected to the users own network.

So, with this we come to the conclusion of this lecture we have gone through 2 different aspects of cloud. One is the different simulation platforms they are there CloudSim cloud analyst so on and so forth thereafter we spoke about the actual you know cloud platforms that are available for real deployment. So, in which again there are 2 classes of such kind of tools one is the open source once. So, OpenStack by open foundation is OpenStack foundation is an example of a open source cloud platform. The paid ones include Amazon EC2, Amazon web services, Microsoft; Microsoft azure and so on.

So, with this we you know stopped over here with the cloud and also in another lecture you will be given some hands on demos some demos with which you can perform some hands on you know experimentation with cloud if you have the facilities with you. You can you know when we go through these different you know steps in the next lecture you can also perform the experiments yourselves with adequate facilities at your end.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

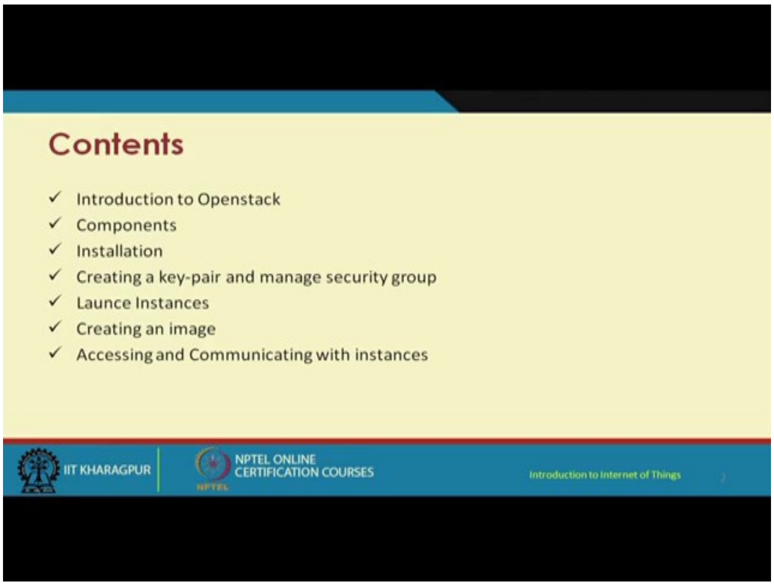
Lecture - 41
Cloud Computing: Practical

This is the fifth lecture in the series on cloud computing for internet of things. In this lecture, you will learn about some of the basics about a an open source platform for cloud which is openstack and in this lecture I will be assisted by one of the TAs, Mr. Anand Shri and he will show you how to create you know it is not possible to show you the installation of cloud or openstack specifically it is not a you know possible to show through this. Those installations are available; the instructions for installations are available you know through different links that are available publicly. Now once you have installed openstack then how to create virtual machine instances how to access those instances and so on, so, those manipulations how to do how to play around with openstack interface, so, those things we are going to show in this particular lecture.

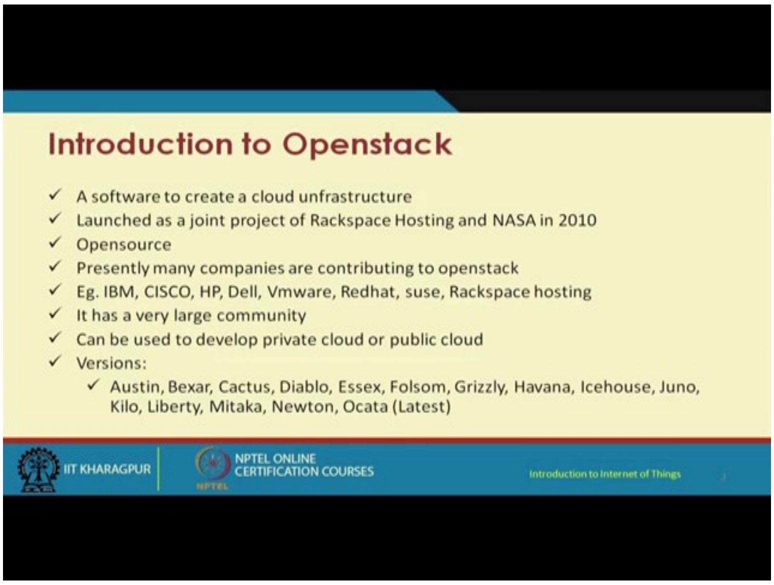
So, this basically is going to give you a practical exposure of cloud with a popular open source system openstack and so, this through this actually you can use openstack specifically with internet of things you know if you are building IoT platforms and for cloud requirements you can use openstack for it.

Hi everyone, my name Anand Shri and I am one of the TAs of this course. So, today I am going a do; I am going tell you about some basics about open stacks. So, let us get started. Here first let us start with what actually is open stack.

(Refer Slide Time: 02:02)

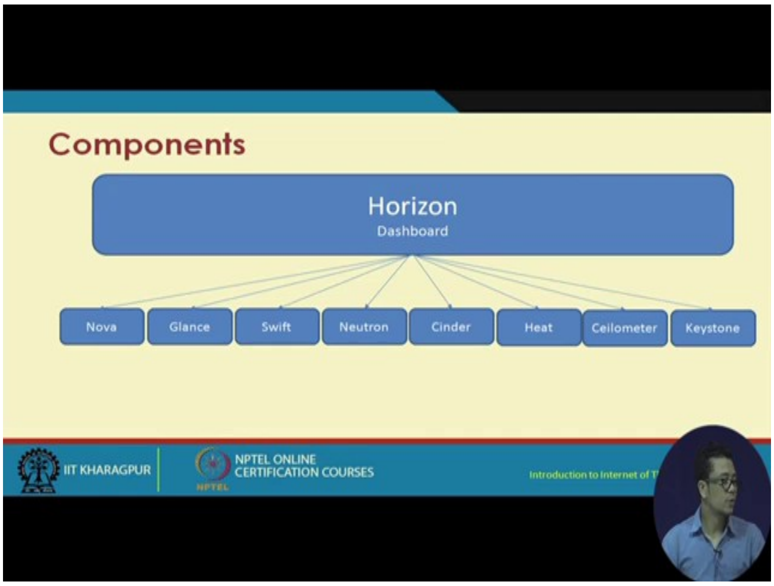


(Refer Slide Time: 02:04)



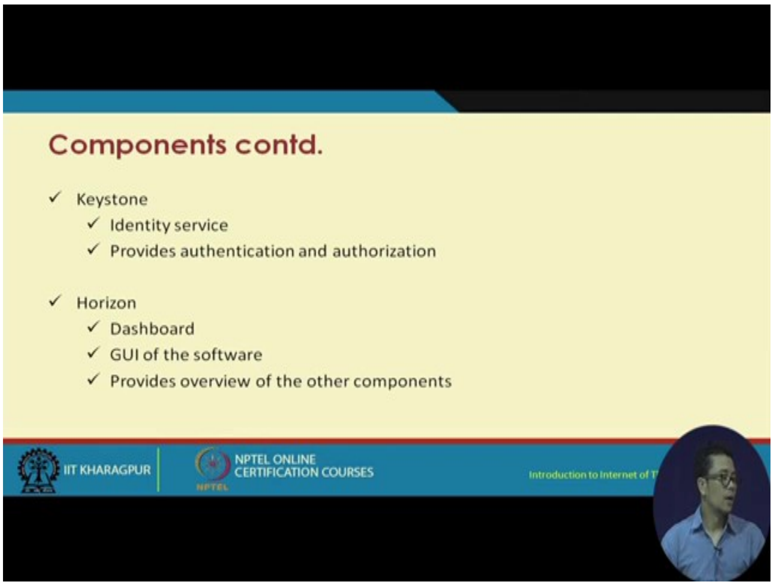
So, openstack is software through which you can generate your own cloud and it is a joint project of the NASA and the rack space hosting and it was established in; it was first released in 2010. So, right, but right now so many companies; so many big big companies are helping in developing the helping in developing this software. So, some of the companies are CISCO, IBM, HP, Redhat and so on so; obviously, actually you can even contribute in developing the software you can even develop your code that can upgrade the present openstack also. So, it is completely free and it is the only completely free open source cloud developing software that is available in the market. So, some of the versions of the openstacks are a listed here. So, it is a releasing order of the alphabetical orders. So, it was a first it was 2010, it was launched as the Austin, but right now the latest version is Ocata. So, let us go to the next slide.

(Refer Slide Time: 03:27)



So, these are components of the open stack. So, in openstack there are so many components and its components are acting their own function and its component has their own specific functions. So, first here is horizon. This horizon is the dashboard section. From this horizon you can actually access other components. So, actually horizon is the GUI interface of the software. So, it provides GUI sections.

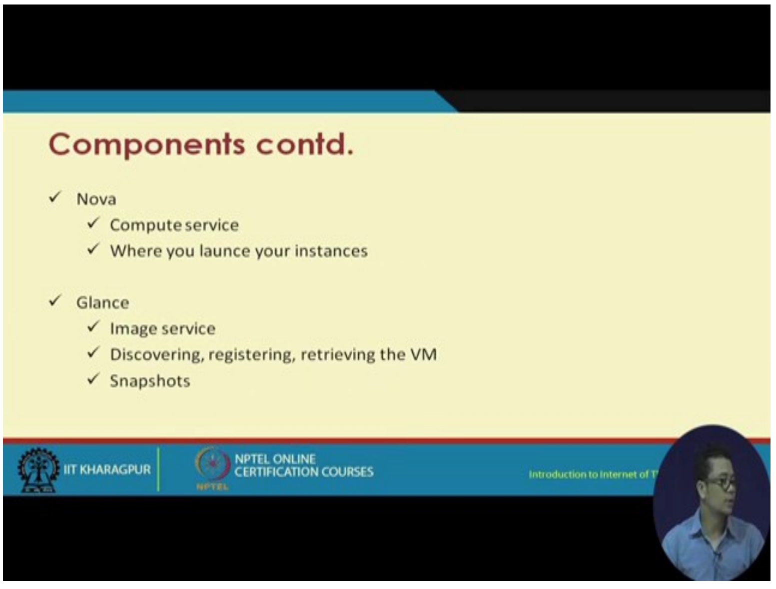
(Refer Slide Time: 04:01)



It also provides overview of the other components. So, when we do the practical section you will know what the horizon is.

So, next is the keystone; keystone is actually the authentication and authorizing system. So, when a user access the system or when a user access the cloud, this keystone will be able to detect if this user is authentic or if this user is authorized to use the resources that he is attempting to use.

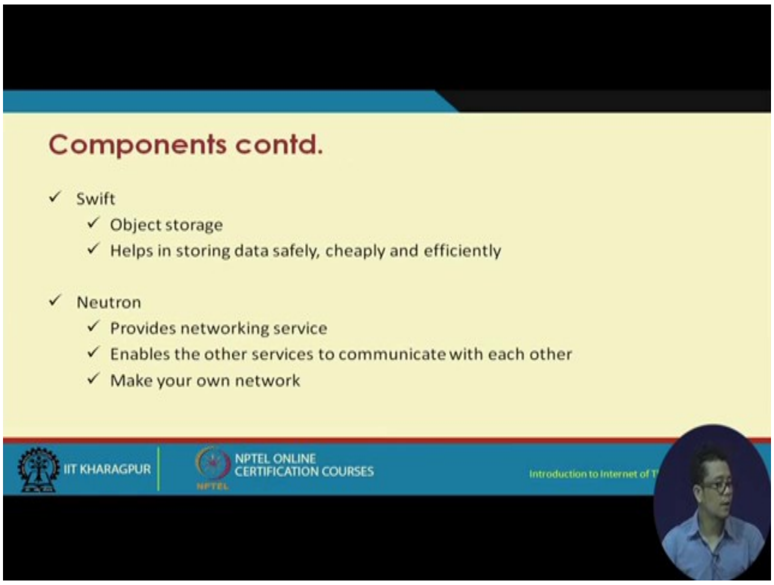
(Refer Slide Time: 04:36)



So, next component is a Nova, Nova is the compute service actually Nova is the component where we are going to launch the instances and all. So, and the glance is the email service.

So, for installing the instances we need images. So, for this we will use Glance. So, it is also useful in discovering registering retrieving those VM ware also and through this glance we can also give the snapshots.

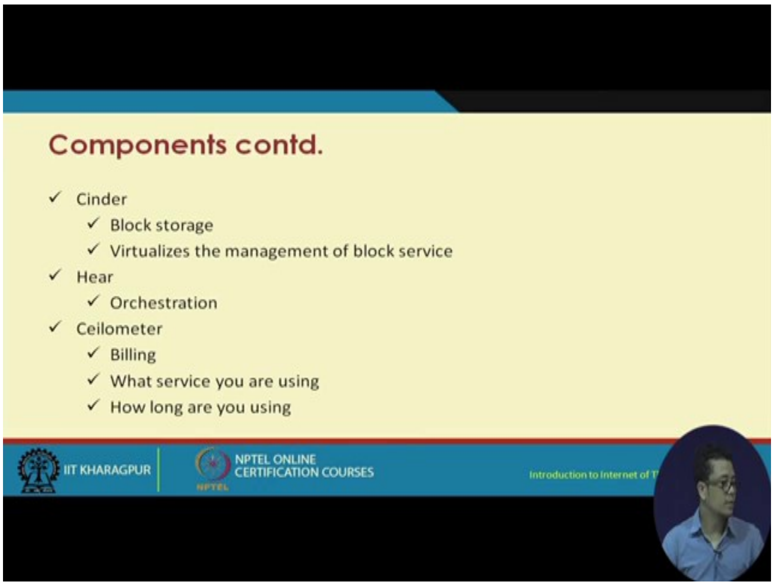
(Refer Slide Time: 05:16)



So, that we can use the snapshot later for the installation of the other VMs also and next is the Swift; Swift is full object storage. So, Swift helps in the storing data safely cheaply and efficiently so; obviously, it is also written on the slide also.

So, the next is the Neutron; Neutron is one of the most important part of the openstack because it is the because it is networking part of the system it provides the networking service of the softwares. So, through this we can access other components and through this we can access different-different instances and then neutron you can create your own networks you can modify your own networks and we can say it as a Neutron is providing like the network as a service.

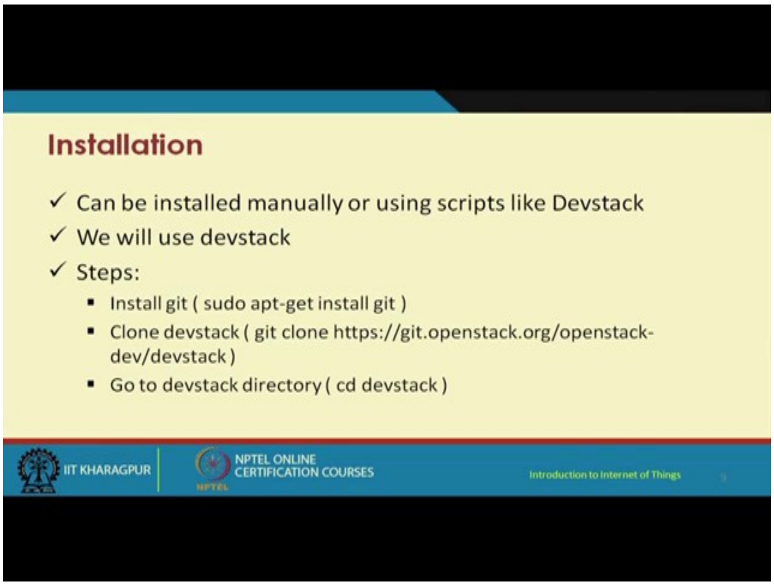
(Refer Slide Time: 06:11)



So, next component is the cinder; cinder is also a storage, but it is the block storage like it is something like pluggable type of storage and then next is the Hear and the hear provide orchestration.

So, and the next is the ceilometers; ceilometer is the billing section like through the ceilometer one can monitor what resource is using and for how long the resources is using. So, billing is actually helpful in helpful for the cloud service providers like a we can monitor which user is using which resources and for how long he is using the resources and according to the time and the type of resources we can build them we can say how much resources that he is using how much costs for that.

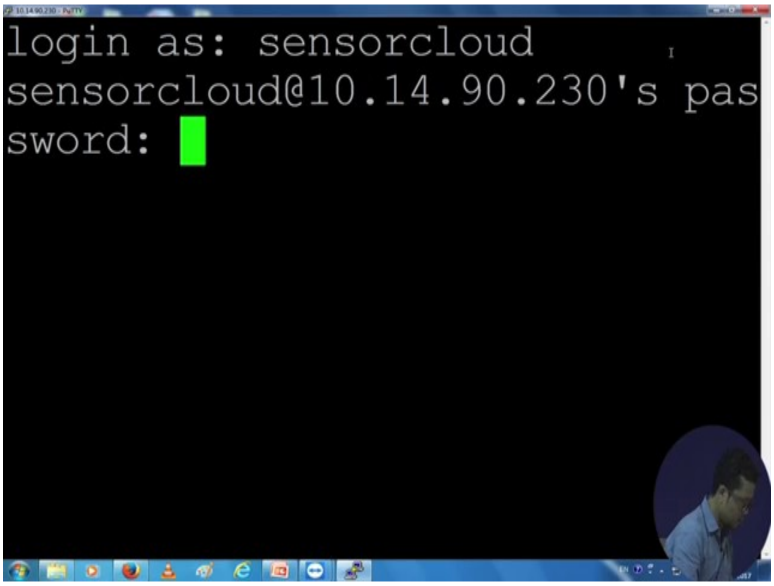
(Refer Slide Time: 07:10)



So, next is; so let us get started the installation part. So, actually in the installation there are many steps like we can also install manually like we can make our own VMs and then install it again and it is quite difficult. So, there are script devstack through which we can easily install the install the cloud like all this openstack in this devstack the installation steps are already written in the form of the devstack file. So, we can directly run the file and everything will be run by the script itself.

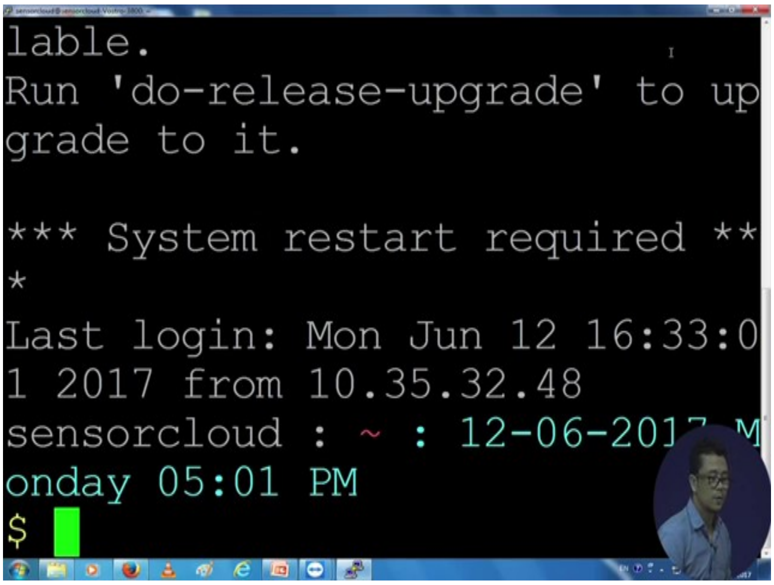
So, while installing the file we may face some problems like a proxy problem then it can the solving those kind of problem is already find already available in the internet also. So, let us here also I am showing how to solve it using the devstack. So, devtacks script is found in a git.openstack.org a website. So, you can easily clone from there and you can a clone then and you can access it easily. So, in order to clone it we have to first install the git softwares.

(Refer Slide Time: 08:39)



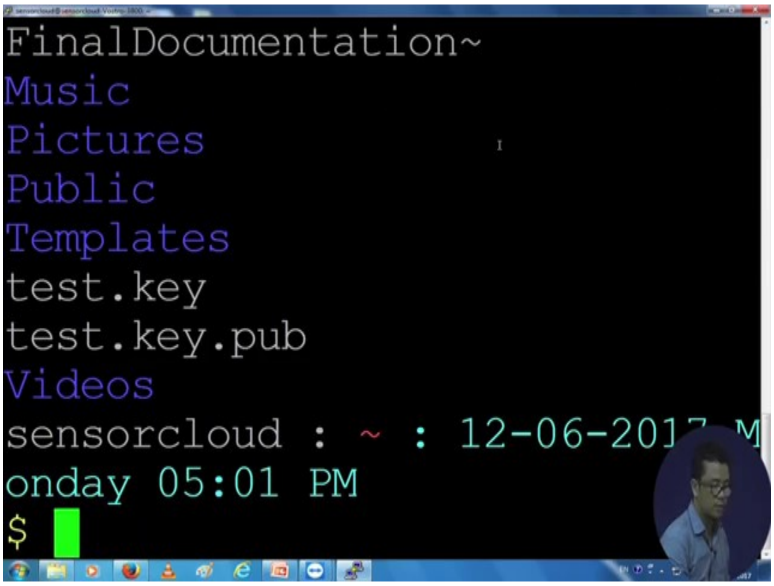
So, in order to it just perform the steps that I have given there like installation part just go to the command and after that just clone it and after that go to the directory like this. So, let us go to the machine where the cloud is installed and see; what is it showing.

(Refer Slide Time: 08:56)



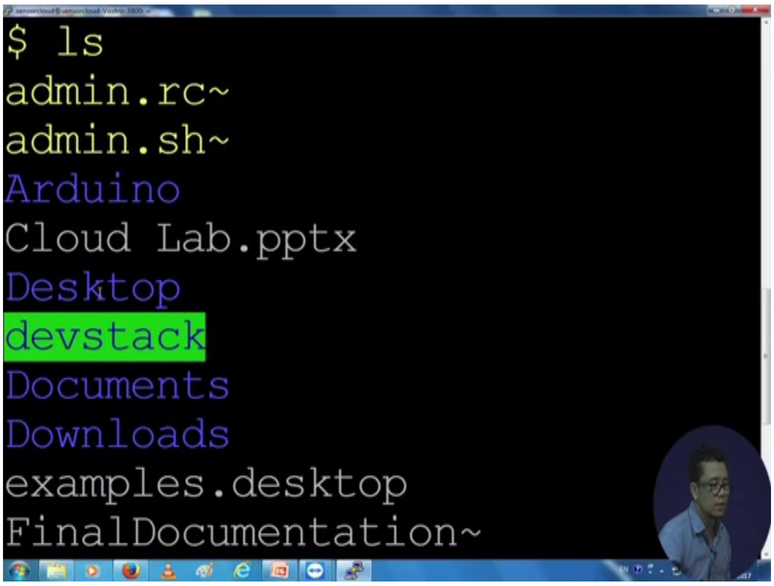
So, let us go there. So, it is running here. So, actually this devstack folder is clone in the home directory.

(Refer Slide Time: 09:06)



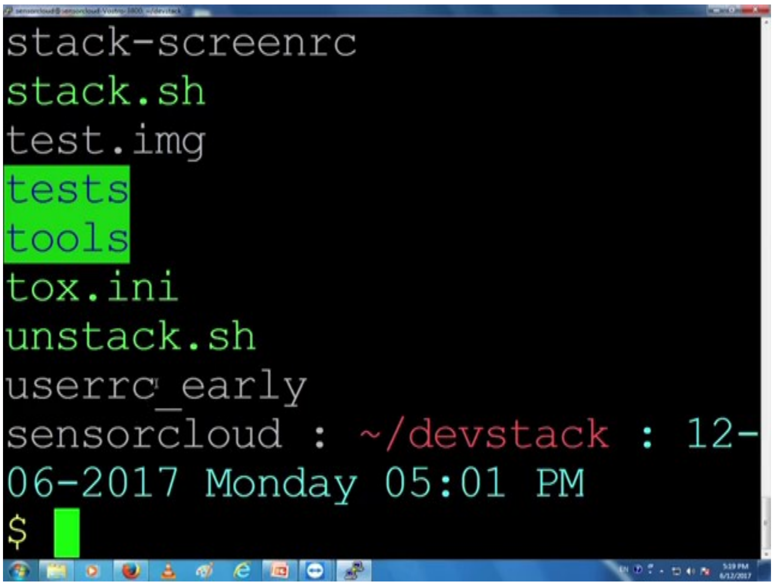
So, let us see what is in the home directory. So, we can see there is (Refer Time: 09:19).

(Refer Slide Time: 09:17)



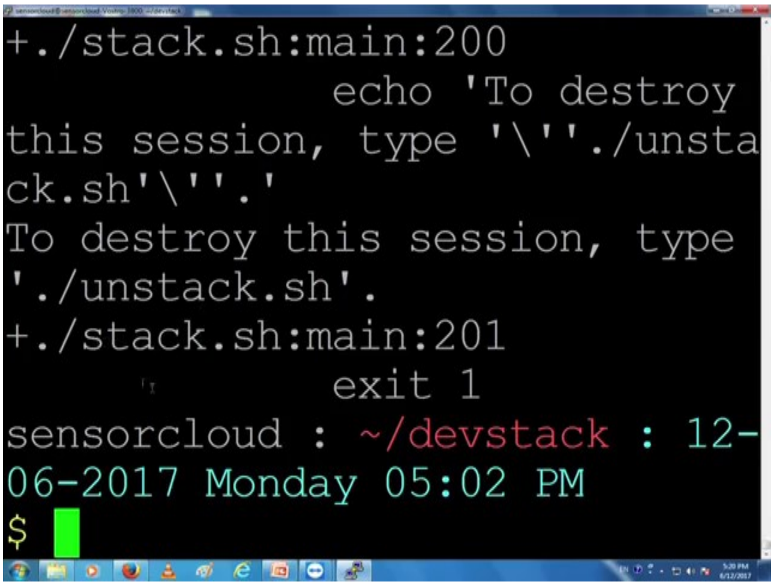
Desk here devstack here So, we will go to this folder. So, inside it So, inside it there will be so many files.

(Refer Slide Time: 09:35)



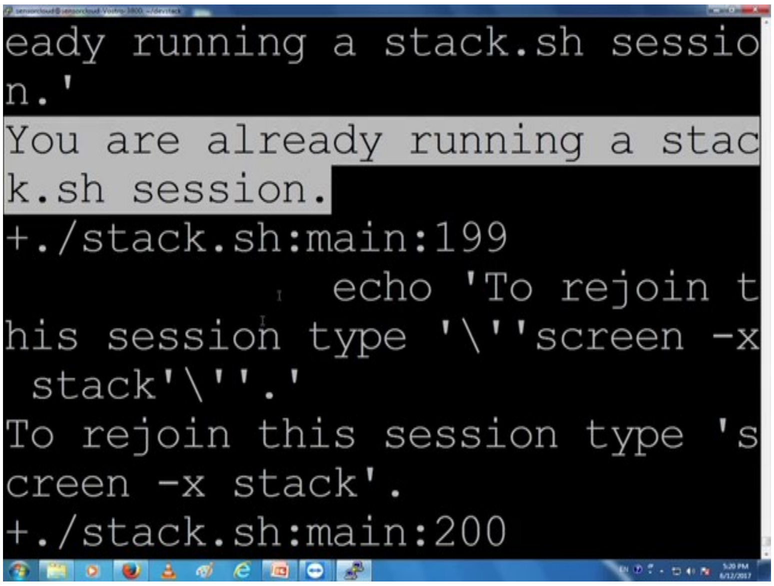
So, we just need to; we need to run this .stack.sh file. So, let us run it; right. So, it is saying that it is already installed already running there this stack.

(Refer Slide Time: 09:51)



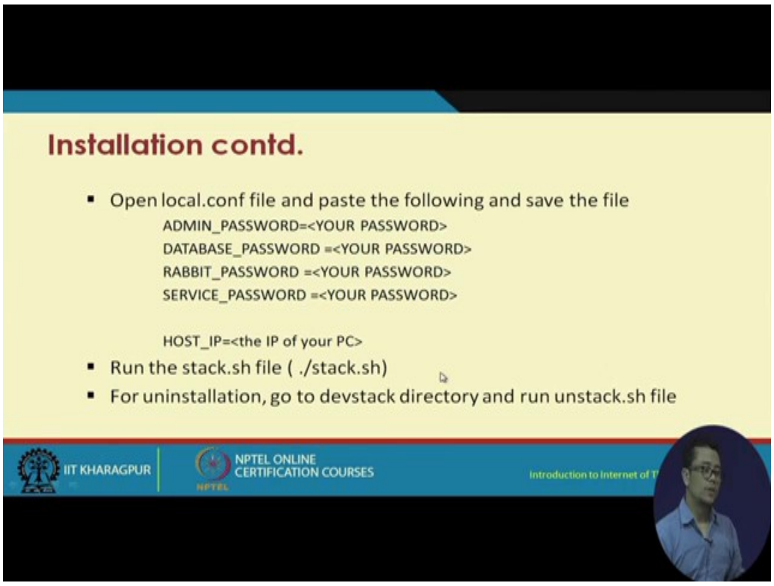
So, it means I have already the installed the cloud in my server; it means we I do not need to install it.

(Refer Slide Time: 10:05)



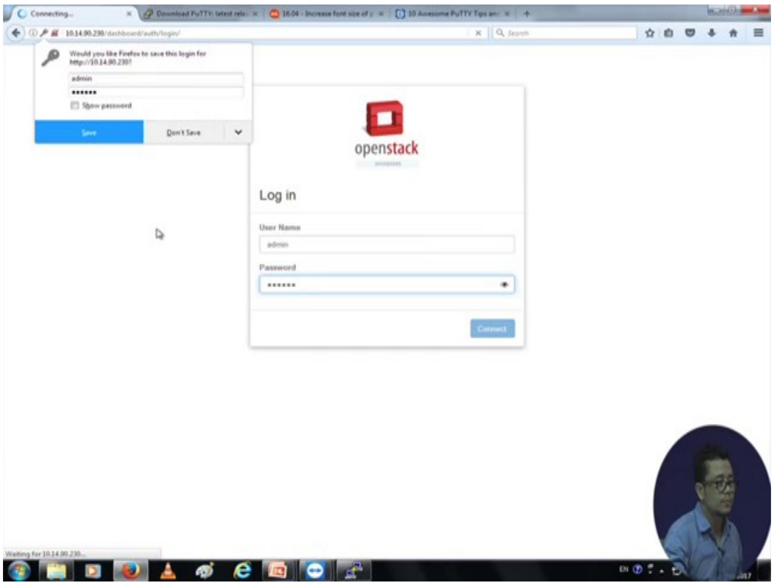
So, for the installation part; just go to the step and you will be able to install it.

(Refer Slide Time: 10:15)



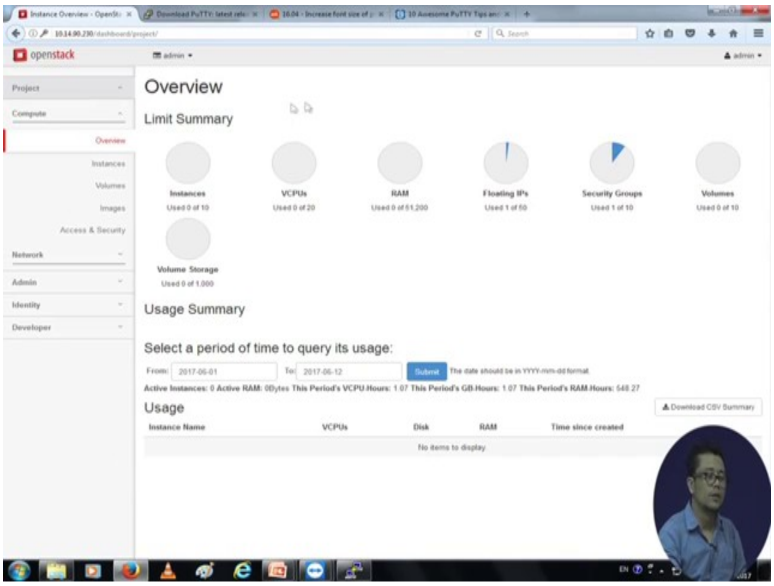
So, for the installation go to a there is some settings like a go to the local .config file and set this settings and run the .sh file stack.sh file for and for the un-installation just run the unstack.sh file.

(Refer Slide Time: 10:47)



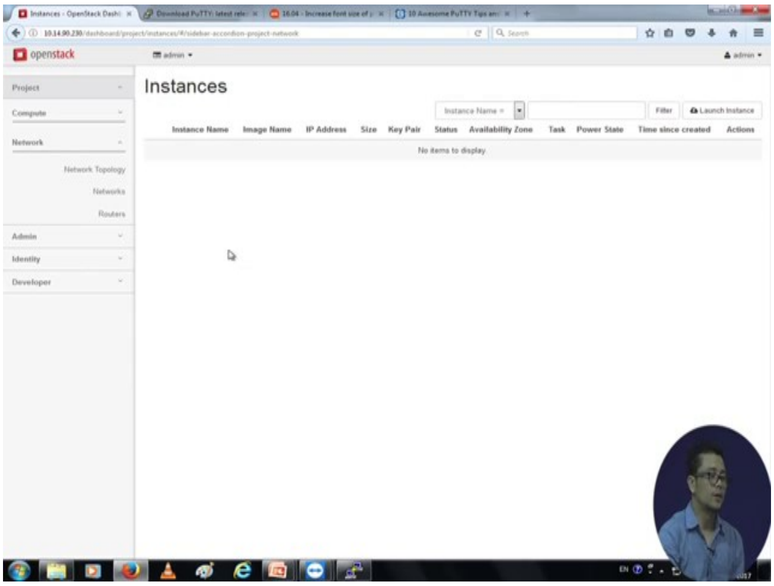
So, after that let us go to the actual cloud and see some working about how to lower the instance and how to delete it how to access the instance and all. So, let us go to the cloud go here I will be accessing as an admin this password is a password that you set during the installation part. So, you should remember the password and you should remember the username also only through the password and username you should be able to access this admin a section so successive.

(Refer Slide Time: 11:22)



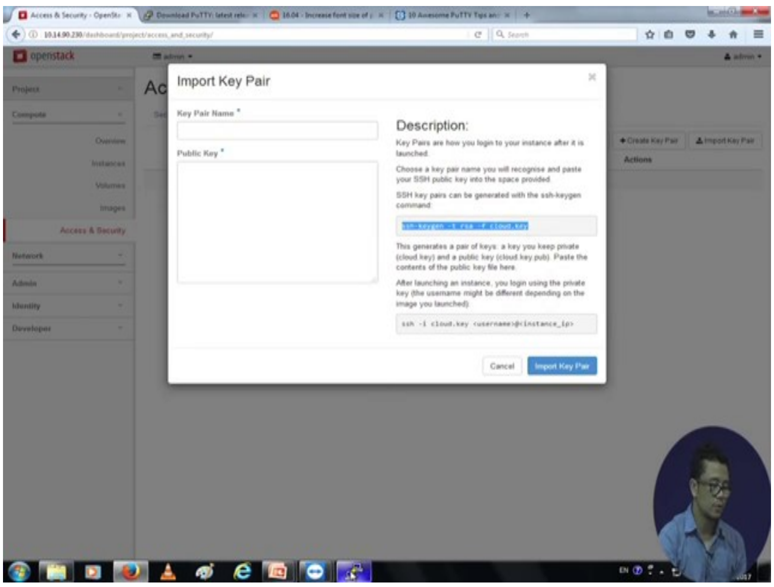
So, this is the horizon this is the horizon of the openstack means this is the GUI part of the section.

(Refer Slide Time: 11:39)

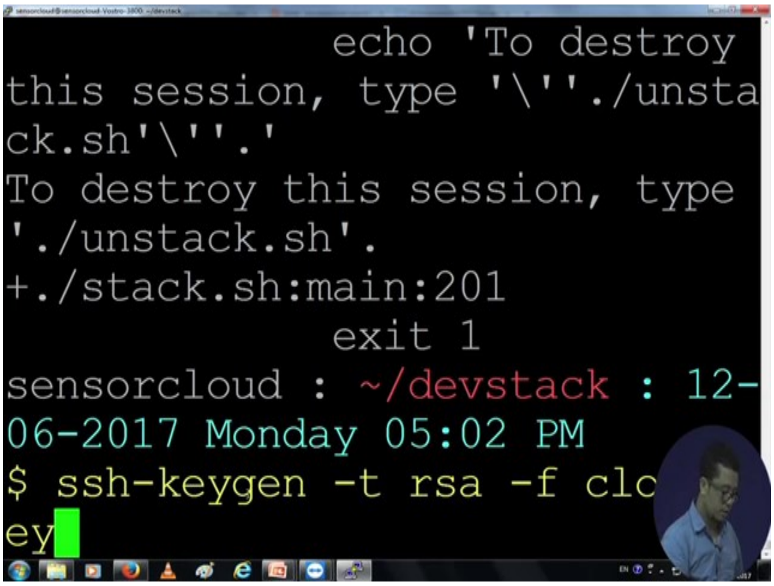


So, through this GUI part we can access to different components like instance instances; obviously, the glance part like a network networking is; obviously, the neutron part. So, let us get started with the creation of the key keys user keys it will be required for the launching of the instance. So, first let us create the key pair. So, it should be starts with the; you just go click the input key pair and here is the command for crating a key pair.

(Refer Slide Time: 12:13)

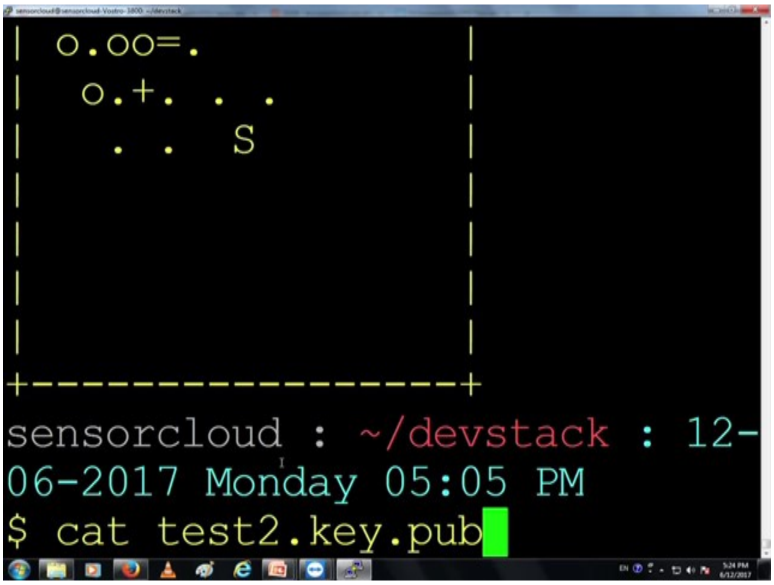


(Refer Slide Time: 12:20)



So, just copy it and go there and yeah let us copy it and make some yeah, like this is the name of the key, you should remember this key in order to access your instance yeah, yeah test 2.

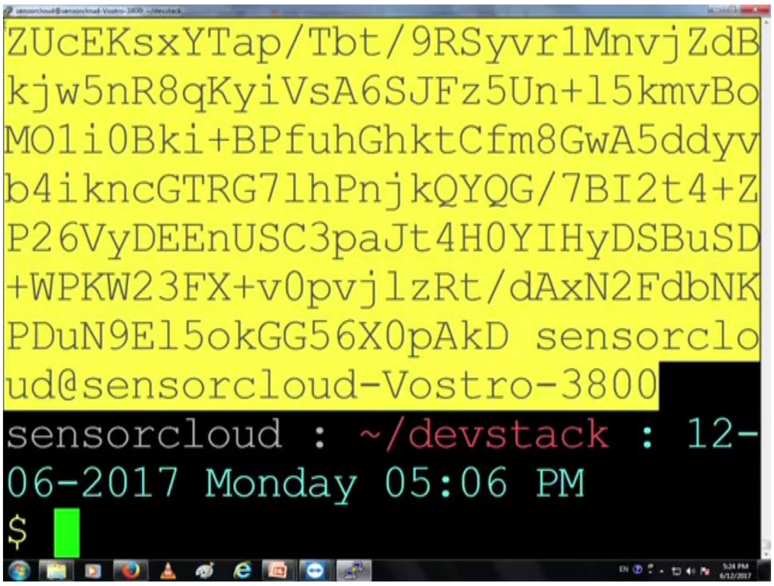
(Refer Slide Time: 12:44)



So, just double click it. So, key is already created. So, we want to access the key already the key should be created here after we create a key.

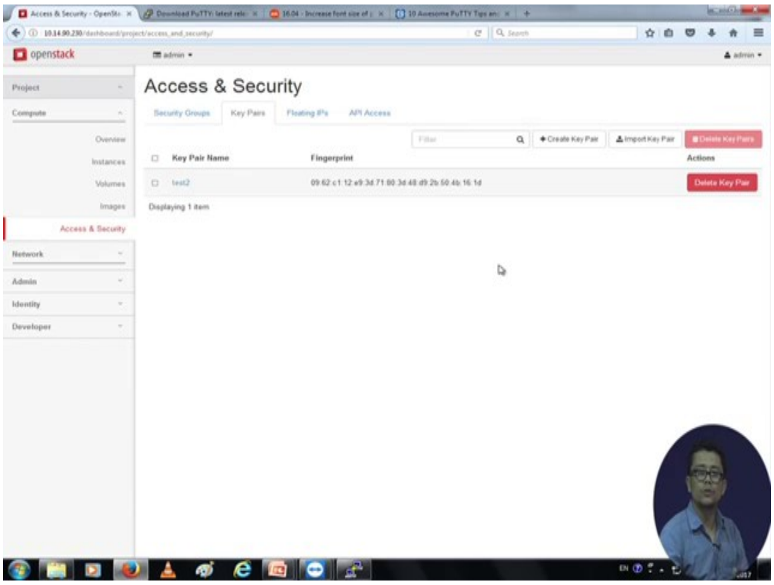
So, let us go create the key first let us access the key. So, this is the generated key actually this is the RSA generated key.

(Refer Slide Time: 13:13)



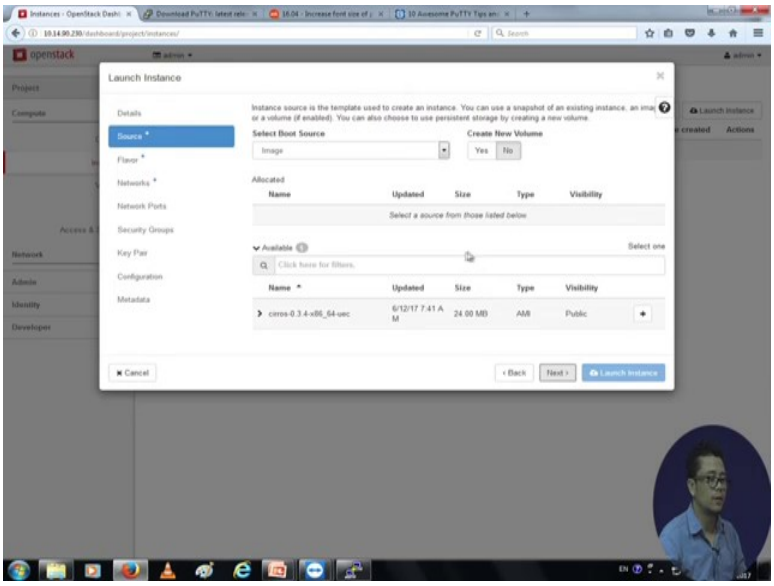
So, copy it copy the key and go there gives some name this will be the name of your key pair. So, let us give it test2 and place your the generated RSA key here. So, after that import the key.

(Refer Slide Time: 13:41)

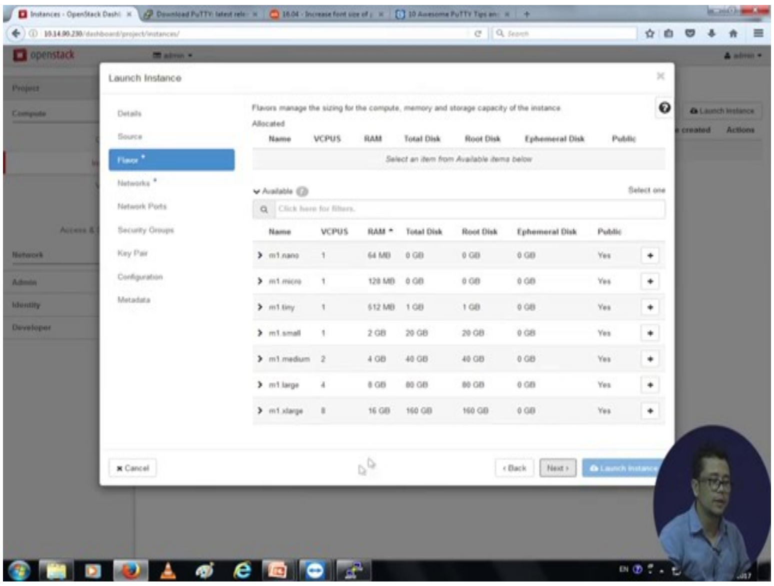


So, we can see that the key is already generated. So, through this key; this actually; this key is generated using your keystone; like this is the authentication part in authorizing part. So, this key is doing the authentication and authorization part of the cloud. So, let us go to instance and let us launch an instance. So, let us give the name of the instance like test2. So, this is the name of the instance you should give the name of the instance anything you like and after that go to next and select image this is the Cirros image this is the only image I have right now next time in others in the sometime.

(Refer Slide Time: 14:14)



(Refer Slide Time: 14:37)

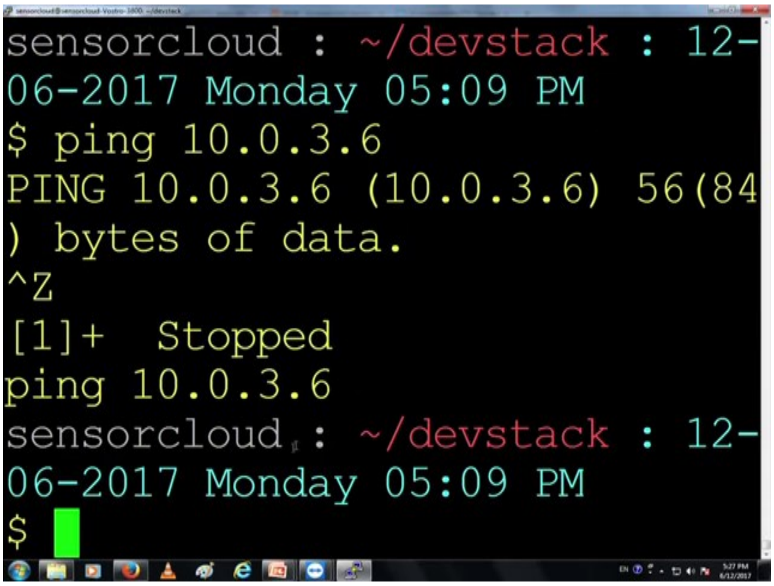


We will be discussing about the how to create the image and all. So, let us let us launch this instance first. So, you if it added then go to next and you just select one of name.

So, you should be some you should select it carefully. So, so you will not be able you. So, that you your instinctively happens you will run smoothly as well as it will not consume the name of your server also. So, for this Cirros; this I will select this tiny and after that next and what is network this is already I have created this network already. So, let us select this one and go to the network port and this security pair security group its already default and after that security pair. So, this is the security key that we have generated just now.

So, now, we can launch the instance. So, let us see it is scheduling it is installing it will take some time it is active now it is already launched. So, let us say if we can access this let us see if we can access this instance the instance is here. So, let us say if we can ping this instance the IP of the instance is this 10.3.36 3.6.

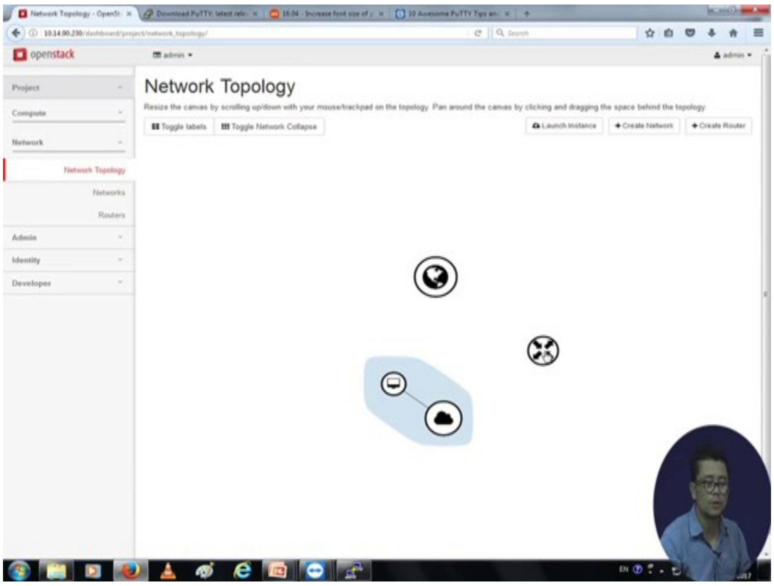
(Refer Slide Time: 16:39)



So, let us see if we can ping. So, I think it will not be able to ping I will explain you later. So, let us exit it and let us set some rules and all.

So, first we have not connect this instance to any external IP. So, if we do not connect it to external IP then we will not be able to access the other outside environment you will not be able to access it. So, let us create let us see.

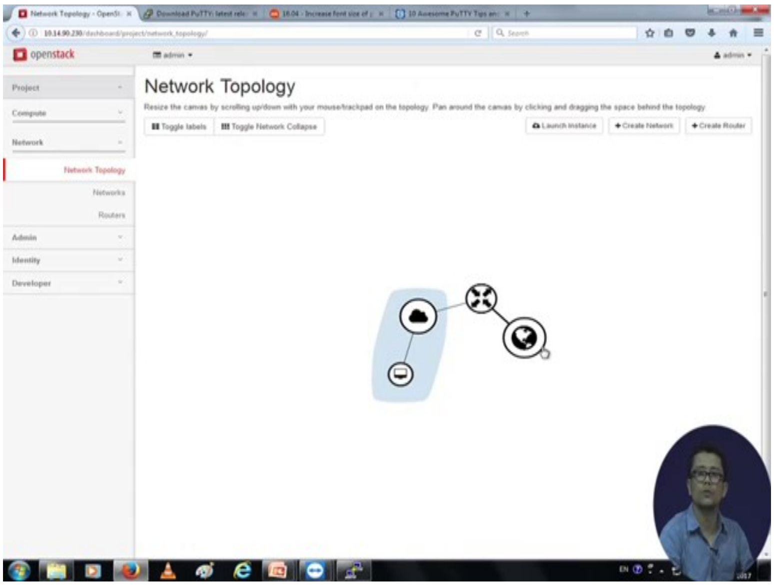
(Refer Slide Time: 17:11)



The network topology first, so, we can see that this is our instance. So, test2 is a instance and this is our this is our network. So, and this is the public. So, until we connect this instance to the public we the outside environment or the inner environment when we inter communicate with each other.

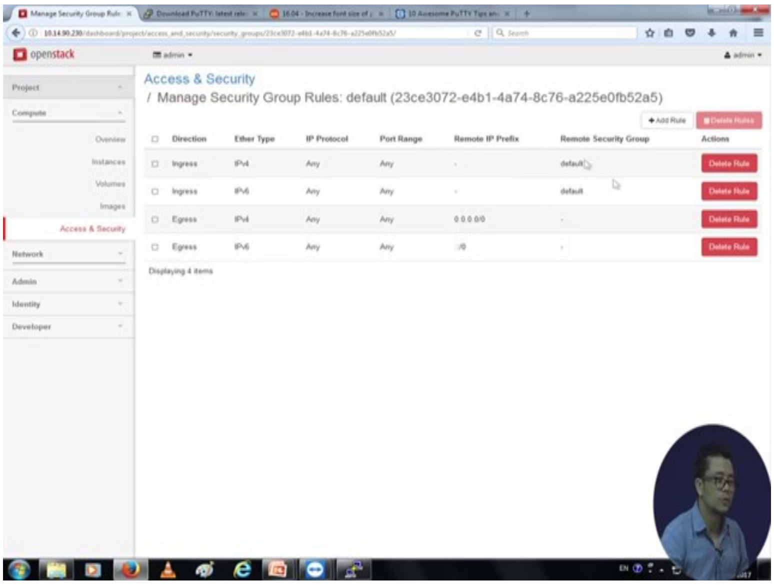
So, what we need to do is first we need to create a router. So, let us create a router create a router let us give some name like router one router one. So, it is created router and we can see that from network topology the router is already created it is created here. So, all we need to do is connect this public offset public port to the router and then connect this router to this network. So, let us do it. So, go to the router and to go to the interface and at interface select your network this is dc; this is a network. So, submitted and your network is connected to the router. So, right now what we need to do is connect the outside world to the router let us do it already done. So, let us see the network topology.

(Refer Slide Time: 18:59)



So, we can see that the router is connected to the inner world and the outer world. Now this outer world should be able to ping to the inner world or should be able to connect with the inner world. So, let us check if it is connecting or not again it is not again it is not connecting also. So, why it is it? So, let us check it because we have not set any security rule.

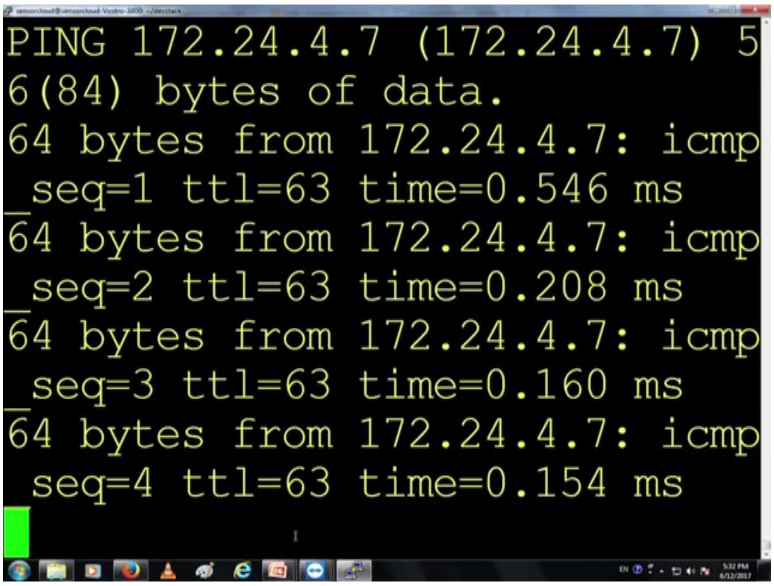
(Refer Slide Time: 19:41)



So, let us do it. So, for setting up the security rule go to the access and security and go to the security group and minus the rule. So, so we can see that there is an any role that is related to pinging for pinging the rules would be ICMP right. So, let us add the rule from here select the ICMP and edit. So, or our rule is added. So, we can we let us see it whether it is accessible from the outside world again it is not. So, why because we have not set any floating IP; that means, our instance is not connected to the to the outside world unless you know we have to set the floating IP. So, let us edit go to instance go there associate floating IP and let generate one; a new one, it is generated and associated.

So, we can see that there is another IP this is the floating IP of your instance. So, through this floating IP outside world should be able to access this instance. So, let us see it if is actually accessible or not let us copy the floating IP. So, let us ping it right.

(Refer Slide Time: 21:30)

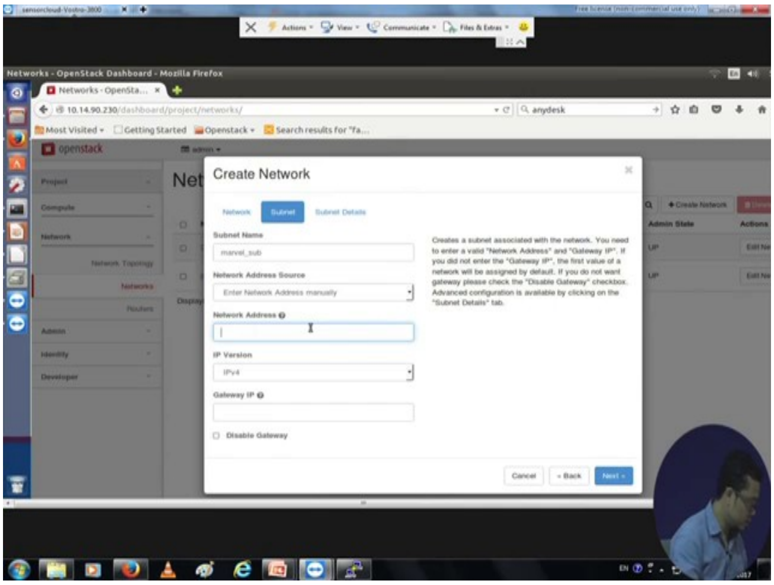


So, we can see that we can able to ping it, it means we are able to access these instance from the outside world it is a good thing. So, let us go here and this is accessible and we can check if it is let us set another rule let us add another rule like let us see if it is . So, we are not able to ssh the instance. So, for this we also need to get another rule. So, let us add it from here select the ssh rule and edit. So, we should be able to access it changed ok resolved it copy.

Now we can access the; so, yes, so, right. Now password what the key is. So, here we are able to access this from the outside world also we are able to access it from the outside world also. So, this is how we generated and how we create the instance. So, right now let us go to the neutron part let us go a bit deeper to the neutron part. So, let us delay these instance for a time being. So, that it will not consume much name of the hosting server right let us launch dc let us launch2 instance flavor tiny see if you remove this we do not need it now.

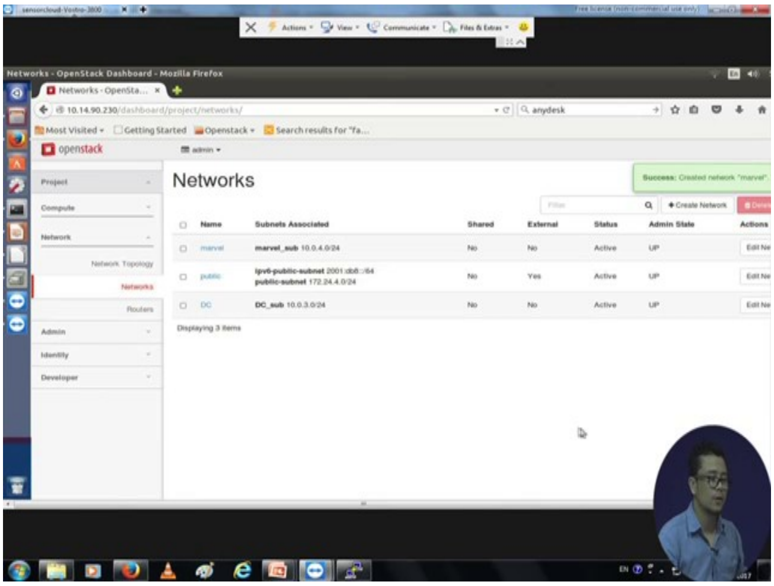
So, this launches instance and let us create another network. So, I will show you how to create a network here. So, for creating a network just click the create network and after that give a name like marvels yeah marvels and go to next.

(Refer Slide Time: 25:45)



Yeah you should click this create sub net part and go to next and give a sub net name like marvel_sub and after that you should give a network address ten dot zero dot like four dot zero slash ten for you should give the this subnet in the form of cider notation. So, let us go next and you should click this DHCP and after that create it should be created hence in a while it is gone a take a while.

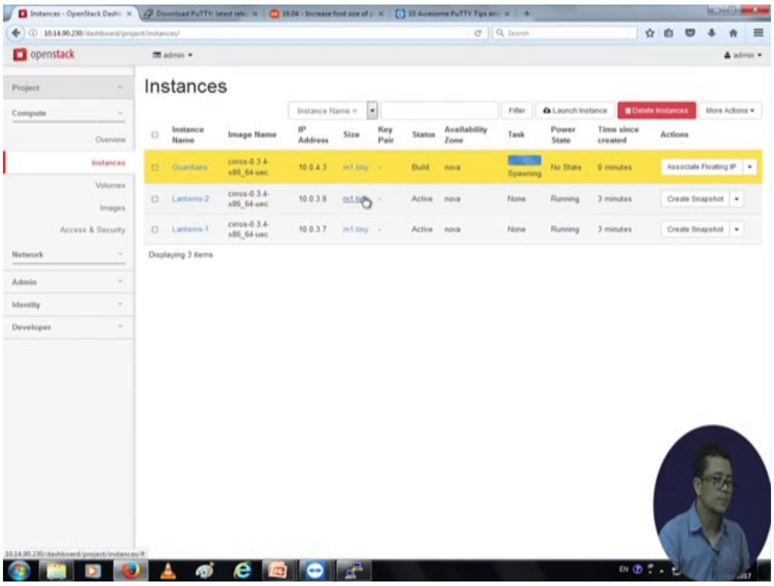
(Refer Slide Time: 26:15)



So, we have a marvel and we have the dc. So, let us connect this network. So, let us connect the instances that are created inside this marvel part and the dc part. So, let us creates another instances it is taking a bit longer than expected let us access this from here. So, so instance let us refresh it, it should not take this long its taking here also same here its coming. So, we have generated 2 instances one is the lantern one and then another is a lantern2.

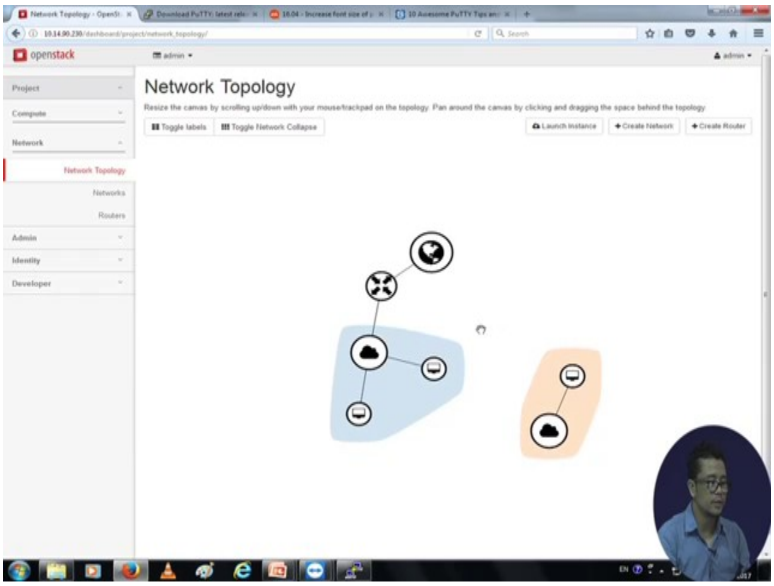
So, let us launch another 2 instances let us call it guardians. So, let us select the same and let us go to the next and select the; your flavors selected next and select the marvel next, next, next. So, we do not need this key right now. So, just launch it is gone a take a while.

(Refer Slide Time: 28:23)



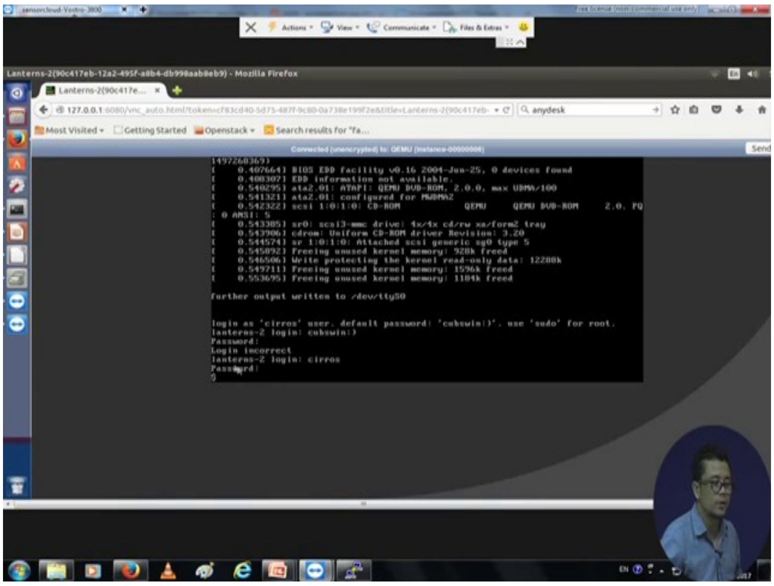
So, Yeah this is guardians and this instances under your marvel network and this lanterns is under the dc network. So, it is creating. So, let us wait for a while ok it is created. So, let us go to the network topology and check it if a check the network topology here.

(Refer Slide Time: 29:18)



So, it is loading let us wait for a while Yeah, we can see that this is your lanterns and this is your marvels these are not connected so; that means, we will not be able to access this pc this guardians from this lanterns because they are not connected.

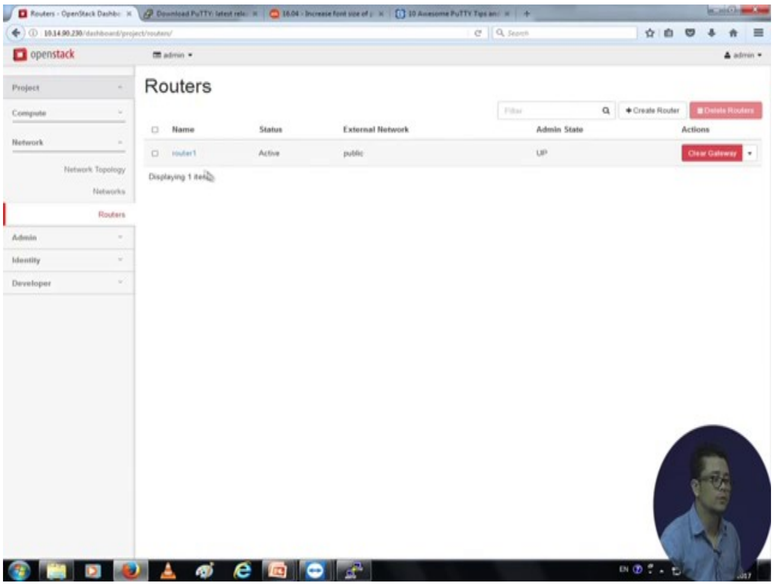
(Refer Slide Time: 30:31)



So, let us check if it is you know accessible or not let us go from here and let us go to the lantern like go to the console go to the console here for the cirros this is the password just. So, it is sorry login as cirros and password is a cup swin. So, we are under this cirros. So, it is the lantern two. So, let us check if it is you know we can access the guardians from the lantern.

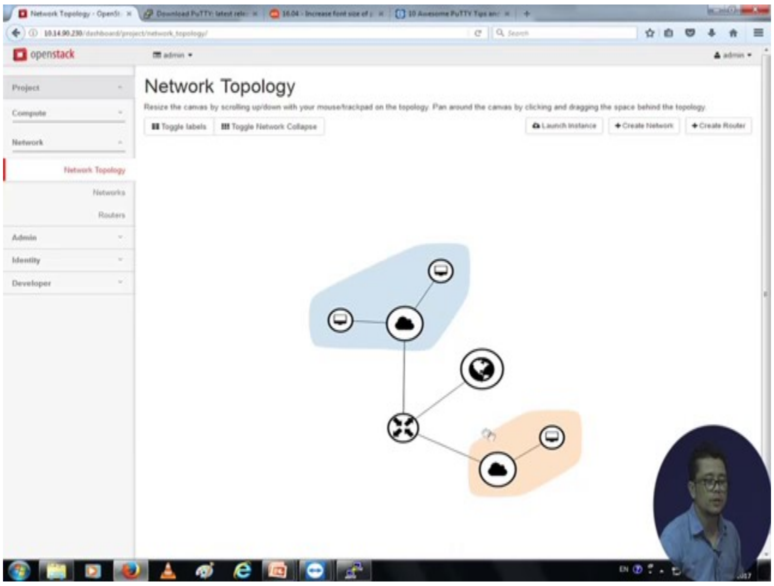
Let us check the guardians what is the IP of the guardians let us check it. So, IP of the guardian is this. So, let us copy it and let us check if it is accessible or not let us go here and ping 10.0.4.3. So, it is not accessible. So, we should set you know we should connect the 2 networks. So, let us do it let us do it. So, go to the network go to the router. So, router is already created.

(Refer Slide Time: 31:54)



So, go to the router and add interface at the marvels here. So, here we can see that from a network topology.

(Refer Slide Time: 32:12)



This 2 worlds are already connected. So, right now the 2 should be able to connect to each other. So, let us check if it is able to connect it or not so right.

(Refer Slide Time: 32:45)

Now, we can see that the 2 networks are able to connect. So, this how you set your neutron is how you set up your network and this is all. So, let us end here this session. So, so these are the references.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 42
Sensor - Cloud – I

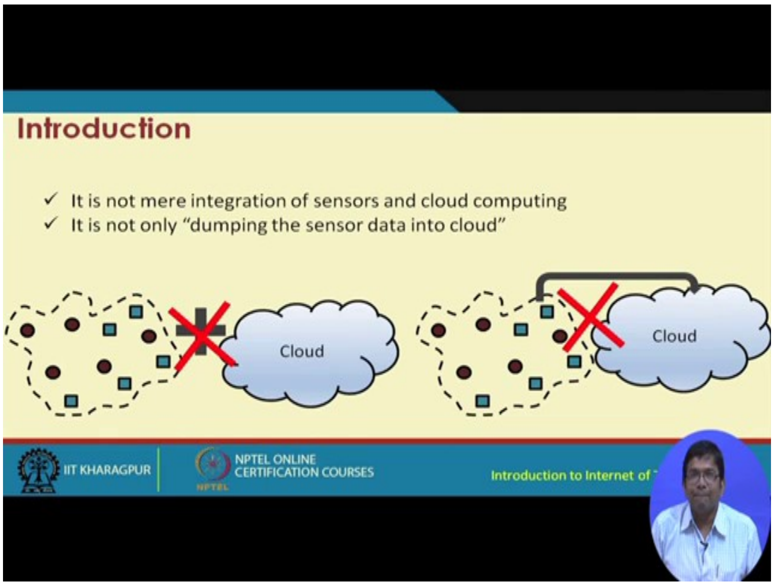
In this lecture, we are going to get introduced to a very fine technology, the sensor cloud technology which has become popular in the last few years. It is popular particularly for IoT environments, for the development of IoT environments.

(Refer Slide Time: 00:41)

So, sensor cloud sensor cloud as the name suggests is about integration of 2 technologies sensor i.e. sensor networks and cloud technology. So, the whole idea is through the integration of sensor technology or sensor network technology with cloud. We offer sensors or sensing as a service, in the same way as in the traditional cloud computing platform which we have gone through in other lecture.

So, in cloud computing, people are talking about offering computing facilities as a service infrastructure, computing infrastructure as a service; software as a service platform as a service and so on. So, this is what we have gone through during the cloud computing lecture. So, here in sensor cloud, we are talking about can we have a model where sensors or sense data or sensing can be offered to end users as a service, a very fine technology, a very nice idea. That can basically revolutionize the way we look at IoT today.

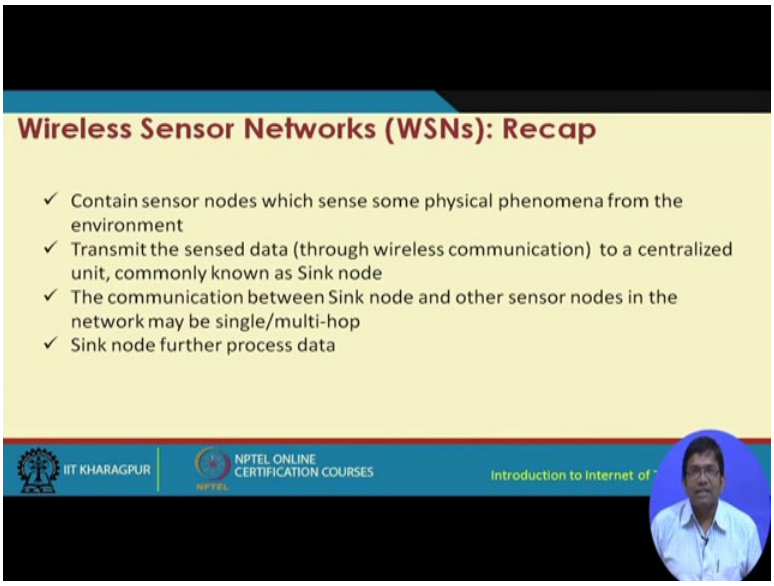
(Refer Slide Time: 02:10)



So, let us look at it further. So, in sensor networks we are primarily concerned about sensing of a particular region, where the sensors are deployed. In cloud computing, we are primarily talking about storage of the data processing of the data and so on. However when we talk about sensors and cloud together, we are talking about how we can basically integrate the benefits that are obtained from each of these 2 technologies, but those benefits are not nearly about getting the sense data to the cloud, dumping the sense data to the cloud or it is not about the simple virtualization of the sensors the way; we have seen that computing platforms are virtualized in cloud. So, here also it is not a very simple integration of sensors and cloud computing technologies. So, it is not a mere integration of sensors and cloud computing technology and also, at the same time, it is neither the integration and at the same time, it is nor the dumping of the sense data to the cloud. Neither of these 2.

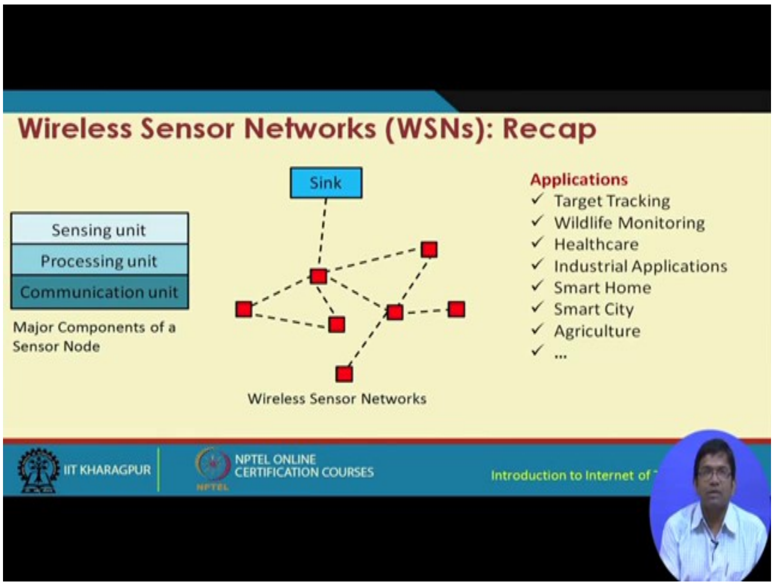
So, we can think of it as both of these plus some additional attributes, neither of these alone, both of these together plus several other benefits that we can get out of this integration.

(Refer Slide Time: 04:02)



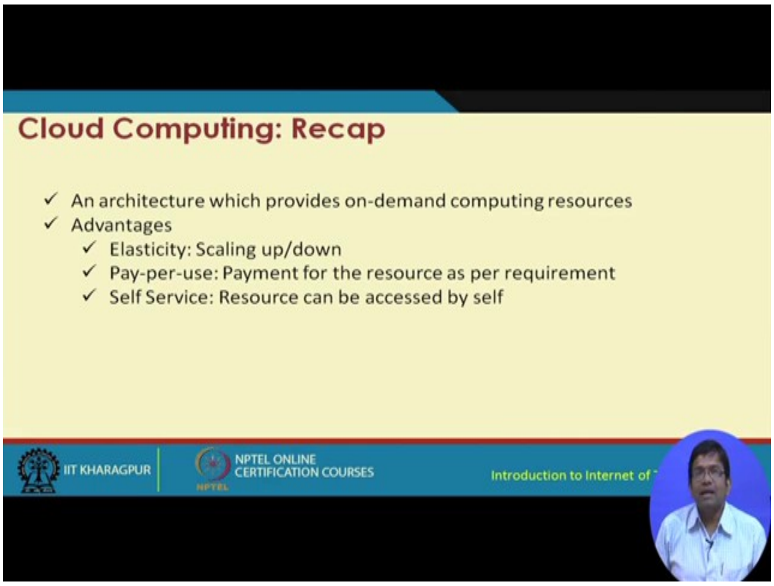
So, just a quick recap of sensor networks; we have already gone through it in detail. So, in a sensor network what we have? We have the sensor noses sensing the physical phenomena that are occurring in the environment of their operation. These nodes send the data, the sense data to the sink which is a centralized unit and the communication between the sink and the other sensor nodes in the network is typically multi hop which can also be single hop of the sensor node. That means, the source node and the sink are sufficiently close to each other and the sink node basically either processes the data itself further or it sends it to a server for further processing. So, this is what additional sensor networks does.

(Refer Slide Time: 04:51)



So, in a traditional sensor network, we are typically talking about such a scenario. We have the sensor nodes connected to the sink sensor nodes sensing the data, sending the data to the sink, the sense data to the sink. So, we have in every sensor node a sensing unit, a processing unit and a communication unit. Sensing unit will have to sense what is going on around it. Processing unit will do some processing; you know some basic processing and the communication unit will send it forward to the next top neighbor for final delivery to the sink. The different applications of sensor networks, we have already gone through; again target tracking, wildlife monitoring, health care, industrial applications, smart homes, smart city, agriculture, vehicular networks, that means, connected vehicles and so many different types of applications of sensor networks cloud.

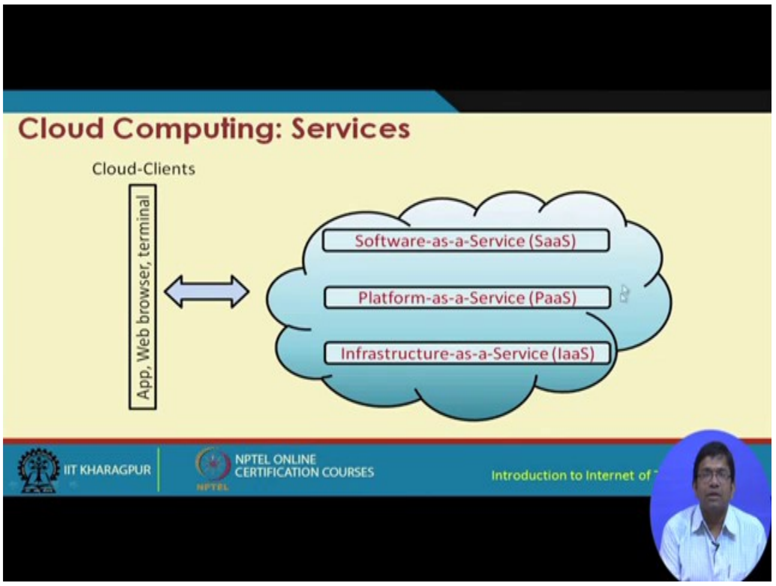
(Refer Slide Time: 05:51)



Let us have a brief recap. Cloud basically provides architecture, some computational platform which can be used on demand to get access to computational resources whenever required, that means on demand on a pay per use basis. So, the advantages of cloud technology over the traditional server based technologies like server farms etcetera, one is elasticity and that means, we can very easily scale up or down as per the requirements. If there is increase in the requirement of computational resources, then you know without actually going about buying those additional resources, one can simply subscribe and pay for those resources and start using them through the click of a mouse button.

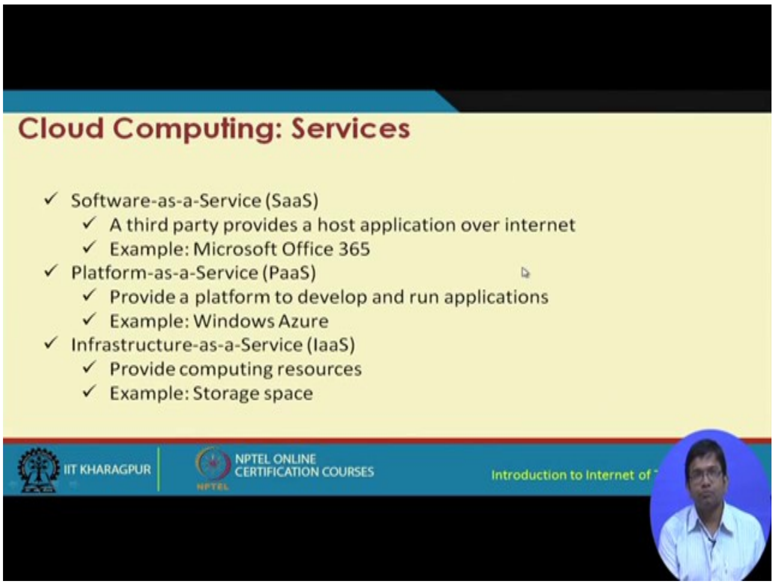
Self service, the resources can be accessed by this, by self. That means you know the resources can be accessed by themselves and themselves means the sensor nodes or the computing computational nodes.

(Refer Slide Time: 06:54)



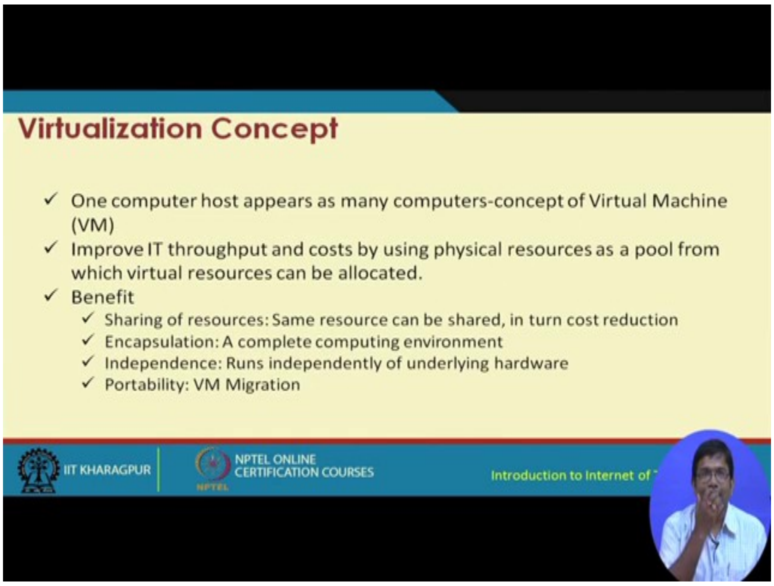
So, we are talking about 3 types of typically or traditionally 3 types of cloud computing services. Infrastructure as a service IaaS, platform as a service PaaS and software as a service is SaaS. Different cloud clients like different apps, web browsers, terminals etcetera are going to get access to the data and the services from the cloud.

(Refer Slide Time: 07:35)



So, what are the services? SaaS, PaaS and IaaS and I will just give you some example once again. We have already gone through it and I will skip it. I will not skip, but I will go through pretty fast. So, software as a service, a good example is Microsoft Office 365, platform as a service example Windows Azure and Infrastructure as a service you know several examples of inclusion of storage spaces, computational resources and so on.

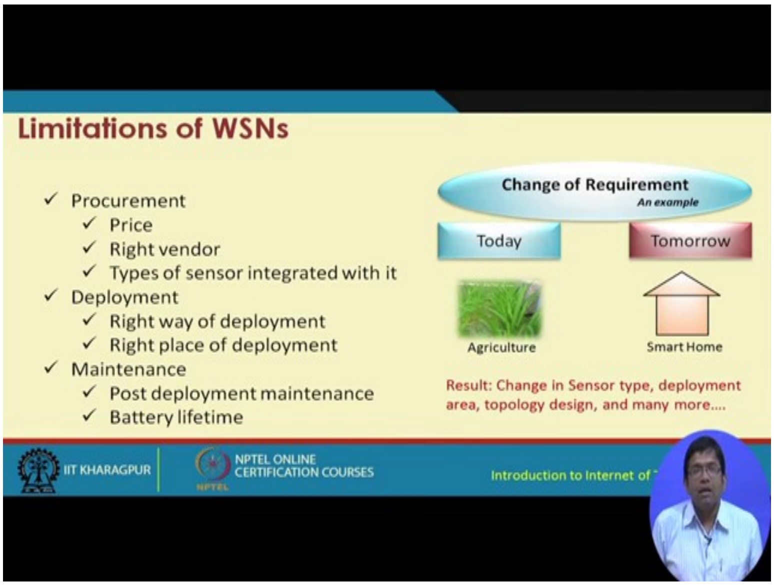
(Refer Slide Time: 08:08)



Now, let us come to the concept of virtualization which is key to cloud and sensor cloud. So, virtualization through the virtualization concept physically one computer might be holding on to the resources and to many computers. Those resources can be shared, they can used, those other computers can use those resources and can get access to the resources as and when required. So, overall the throughput and costs are going to be increased and the benefit is that virtualization basically permits or enables this sharing of the resources which means that the same resource can be shared in turn through the reduction of the cost.

Encapsulation which is that virtualization technology basically provides a one-stop solution, a complete solution giving a complete computing environment. Independence basically means that it runs independent. That means, virtual terminal runs independent of the underline hardware and this virtual terminals are portable. That means, that a user might be using the computational resources through a virtual terminal and that resource where it is not used, those resources map to the actual physical resources and those physical resources can be made available to another user.

(Refer Slide Time: 09:50)

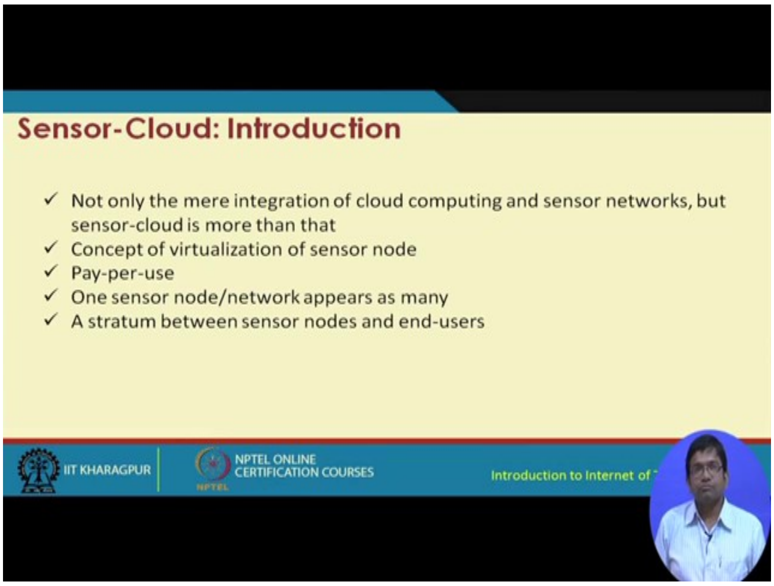


Now, the limitations of WSN networks; so, what we are talking about is the overall price of procurement is quite high. So, if we have some sensing needs, so the only way to go about you know full filling those needs is to buy from the market sensors, sensor, nodes and sensor networks and then, go about deploying.

Then, the question is that we also have to be careful about procurement. We want to procure price, right vendor, types of sensors that are integrated to the platform. So, this is one limitation. Second limitation is about deployment. So, what is required is to have the right way of deployment and the right place of deployment. Right way means how it is going to be deployed and where it is going to be deployed and in terms of maintenance, most the deployment maintenance and battery life time are other limitations of sensor networks.

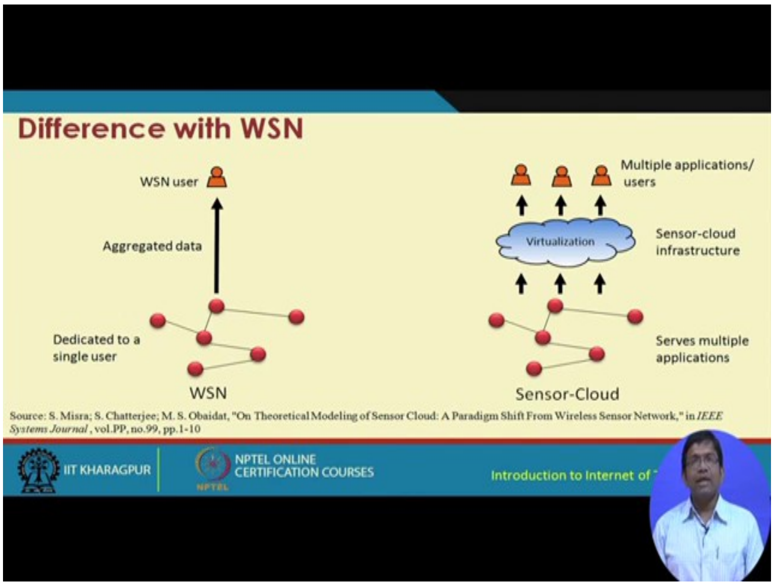
So, from an applications perspective, again what we see is when the application changes, the requirement also change. However, we will see that the sensor cloud technology can come to a rescue at least partially.

(Refer Slide Time: 11:27)



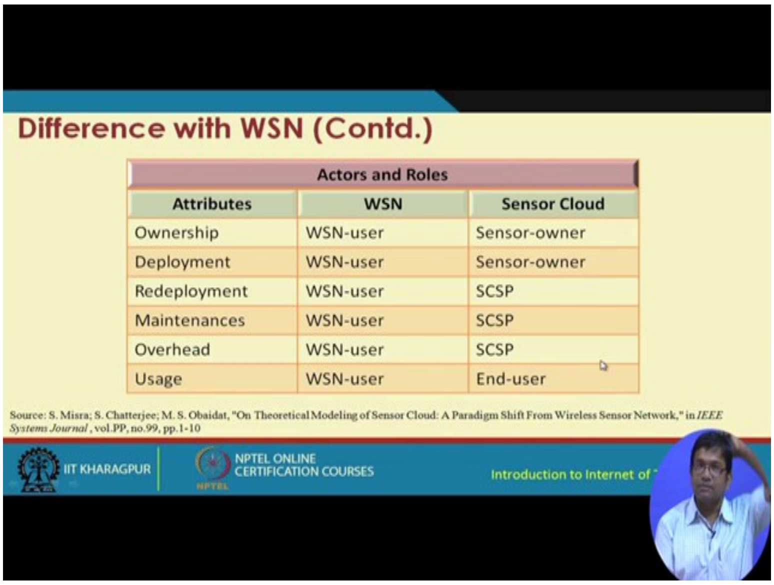
Through the introduction of sensor cloud, not only the mere integration, sensor cloud is not only the mere integration of cloud computing and sensor networks, but it is also about pay per use facility offering pay per use facility using the concepts of virtualization of the sensor node and introducing a layer between sensor node and the end user.

(Refer Slide Time: 11:58)



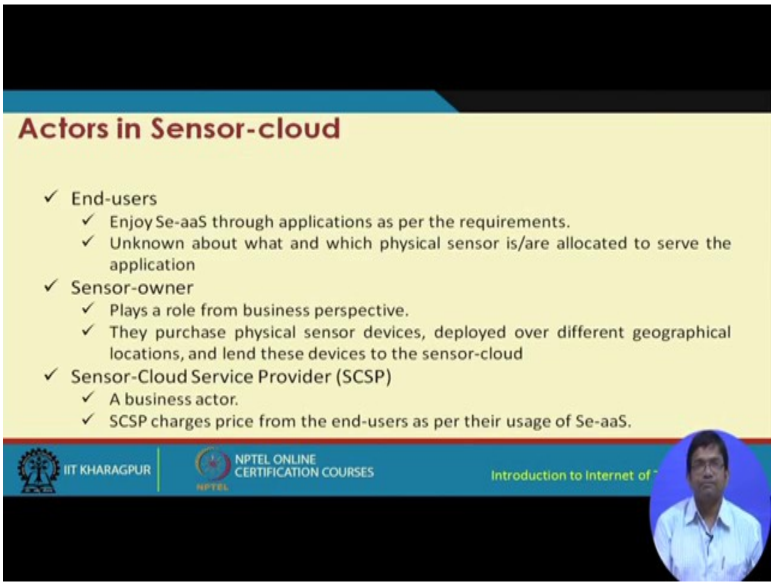
So, here is a side by side comparison of traditional sensor networks with sensor cloud. So, typically in the traditional sensor networks, we are talking about single user in sensor cloud. The benefits would be experienced more when we are talking about multiple users. Then, in sensor networks, the data are aggregated and send to the sensor network user and in sensor cloud, the infrastructure basically takes care of it. The sensor cloud infrastructure basically is tasked to aggregate and send it forward and at the device level, these devices are dedicated to a single user in sensor networks and this can be improved by serving multiple applications by the different sensors. So, these are the different advantages of sensor cloud over sensor networks.

(Refer Slide Time: 13:05)



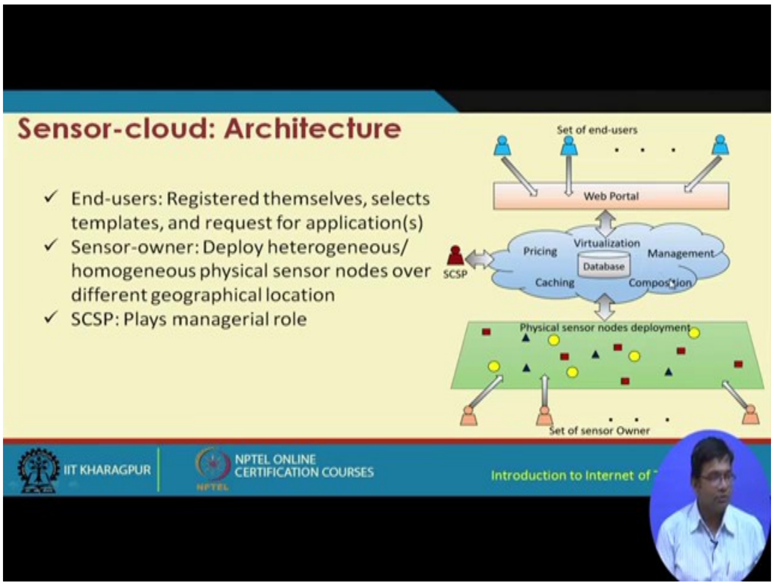
Now, in sensor cloud we are talking about not a single user or a single actor or a single role, but we are talking about different types of roles, different types of actors, we are talking about sensor owners who basically own the sensor, we are talking about SCSP sensor cloud service provider who may not be the owner, but is separate from the owner and is simply you know the service provider, sensor cloud service provider, the sensing service provider and when we have this maintenance with respect to maintenance, again the service provider does it overhead and usage. So, we see that we have diverse types of sensor cloud, we have diverse types of sensor cloud actors and in the traditional sensor network, we use to have only a single type of actor which is the WSN user.

(Refer Slide Time: 14:10)



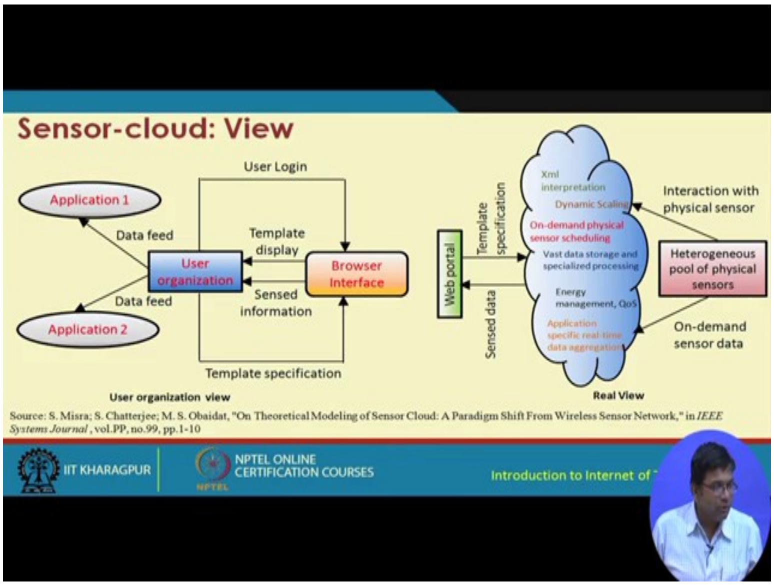
So, we have end users, we have sensor owner and the sensor cloud service provider, 3 different types of actors.

(Refer Slide Time: 14:25)



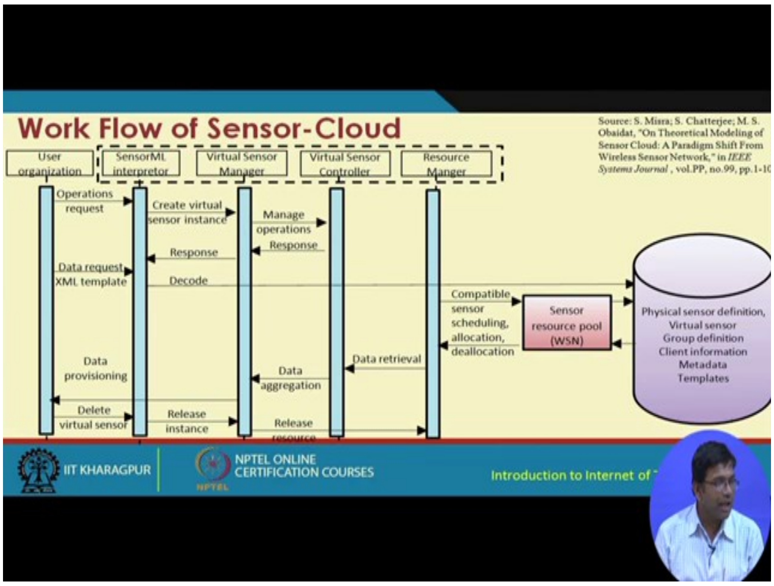
We additionally have end users and SCSP which is basically the sensor cloud service provider which primarily takes the managerial role. So, we see in this particular figure, we have a state of sensor owners, then we have through virtualization, pricing, caching composition management. We take care of servicing, the request from the SCSP and also, sending the responses back and finally, the vertical communication over here with the weight portal.

(Refer Slide Time: 15:10)



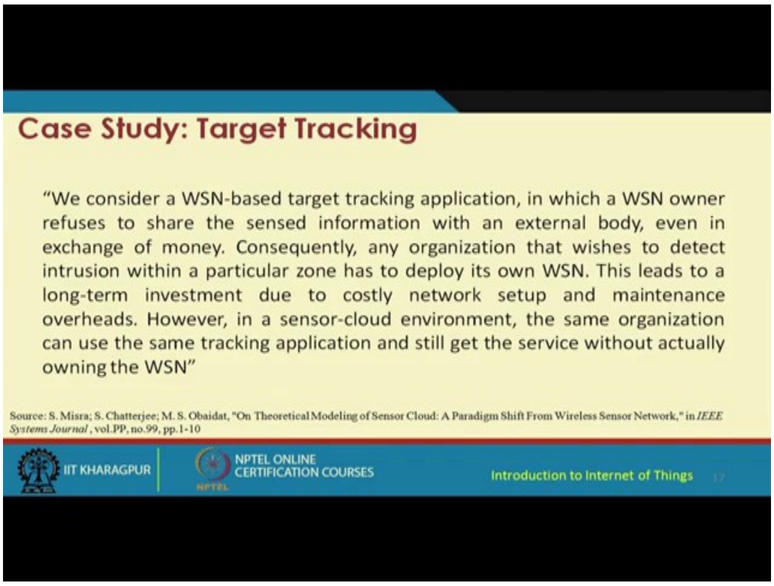
So, the left hand side figure basically shows that how the sensor cloud data is accessed through a browser interface. So, we have a browser interface and the templates as well as the sensed data are sent to the user organization, and this data from the user organization are basically fed as data feeds to diverse applications. On the other hand, on the right hand side figure, we see the real view of sensor cloud. So, here we see that there are only a few functionalities scaling, dynamic scaling, then on demand physical sensor scheduling, energy management, quality of service and application specific real time data aggregation.

(Refer Slide Time: 16:06)



So, here is the flow diagram, the sequence diagram of sensor cloud. So, as we can see over here, the different actors or roles include user organization, Sensor ML Interpreter, Virtual Sensor Manager, Virtual Sensor Controller and Resource Manager. So, initially from the user organization, a operation request is sent to the sensor ML interpreter. This creates the virtual instance of the sensor, then this is basically sent to manage the controller to basically function on the controller. A response is received from the controller and the response is again transmitted forward further and then, this XML template is decoded like this. This continues. The data are stored in the sensor resource pool and different functionalities, such as service sensor, physical sensor, definition virtual sensor, group definition, client information, metadata and templates are used over here in this architecture.

(Refer Slide Time: 17:35)



Let us now briefly consider a case study. So, we considered a sensor network based target tracking application in which a sensor network owner refuses to share the sensed information with an external body even in exchange of money. Consequently, any organization that wishes to detect the intrusion within a particular zone has to deploy its own senor network. This leads to the long term investment due to costly network setup and maintenance overheads. However, in a sensor cloud environment, the same organization can use the same written application and still get the service without actually owning the sensors. So, this is the whole advantage. You know we the users have sensing needs, but they do not have to really own the sensors in order to get access to the sensed information about the physical environment of operation.

So, with this we come to an end of the first part of the lecture on sensor cloud. The next lecture is going to be on the more advanced topics of sensor cloud. So, there we are going to learn about the different solutions as well about how to handle different solutions in sensor cloud.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 43
Sensor Cloud – II

So, this is the second part of the lecture on Sensor cloud.

(Refer Slide Time: 00:26)

In the first part, we have understood what is sensor cloud, the advantages of sensor cloud over regular sensor networks and how sensor cloud can help in real life applications. So, we are now going to look at some of the issues in the building of sensor cloud. So, you know just as a recap of what we discussed before in the first part, when we talk about sensor cloud, it is about integration of 2 technologies. One is sensor networks and cloud trying to take advantage of the inherent capabilities of dissemination of sensor networks. So, sensor networks are very much good in data acquisition and thereafter, dissemination of this information and cloud basically is good in terms of information storage, data storage.

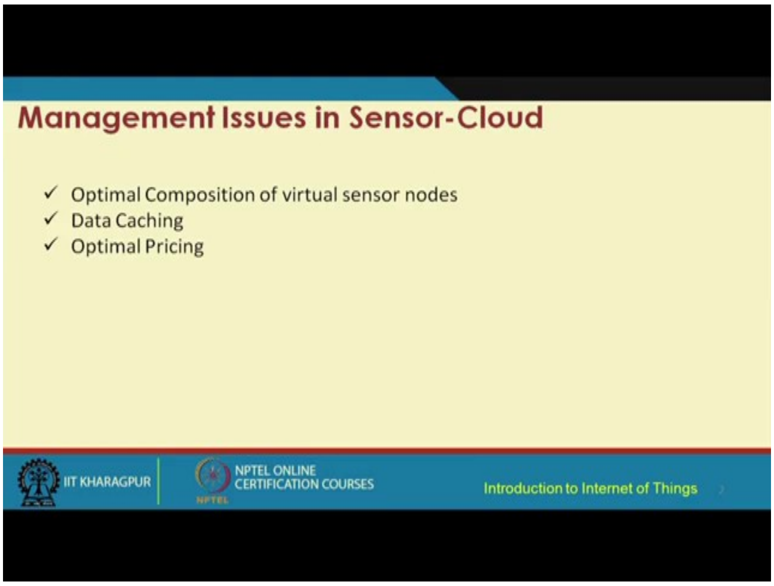
So, trying to harness the advantages of both is what we try to do in sensor cloud. So, how is it done? It is done with the help of the virtualization capabilities. So, in sensor cloud, we are offering sensors as a service through the technology of virtualization by which these different sensors are virtualized and these visualized instances of the sensors are made available to the different users different users of sensor cloud. In sensor cloud architecture, typically, there are different types of users. One is the end users themselves, the second is the sensor owners and the third is the sensor cloud service provider.

So, like this could be few other you know different types of actors or the stake holders as well, but typically we are talking about these stakeholders. So, what happens is the sensor owner is the one who basically makes these you know who basically procures and makes these sensors available? They own the sensors, they have purchased the sensors and they have made the sensors available for you know for use. Sensor Cloud service provider is mostly concerned about the supervision, the management of the sensor services. So, they basically in conjunction with the sensor owners, they deploy the sensor nodes in the region of interest, in the area of interest like in the city or several cities. They will be deploying these different sensors at different points and then, the sensor data are going to be made available to the different users.

So, though the main advantage of sensor cloud is through a virtualized platform, through the technology of visualization, the different owners are able to access these different sensor devices for performing their own sensing tasks. So, what we have is basically sensors as a service or even we can think of as the concept of sensing as a service. So, sensors as a service means that the sensors to whoever require you know who ever requires the sensors, they would be able to get access to the services in the same way as infrastructure is made available through a virtualized platform in cloud to the end users. The similar kind of analogous thing is done over here. Instead of infrastructure, we have the sensors and the sensors are made available to the users.

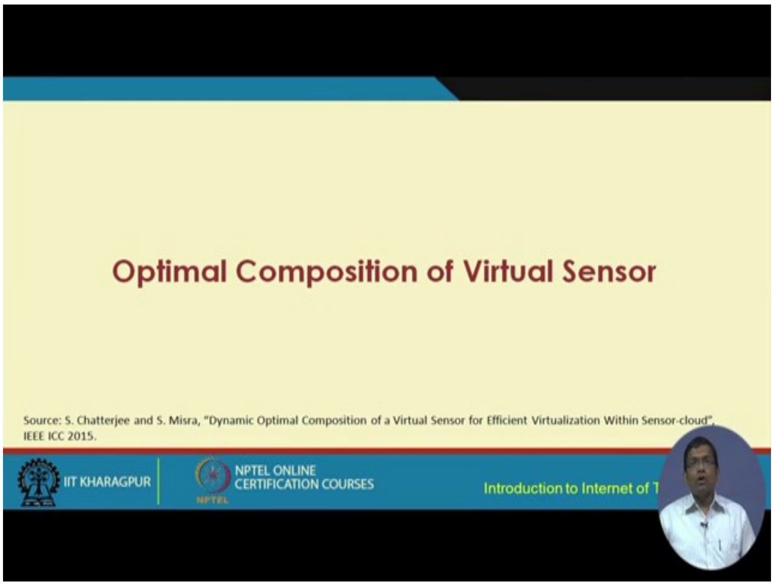
So, this is the whole idea of sensor cloud and in this particular back drop, we have to understand that if we have to develop this kind of infrastructure of sensor cloud, how can we do it. So, let us look at some of these different issues.

(Refer Slide Time: 04:15)



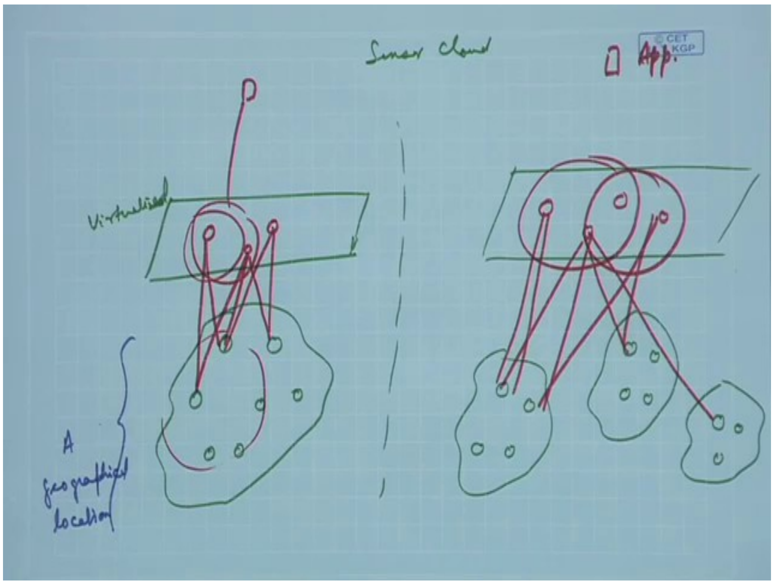
So, first one is the management issue first one is the management issue in sensor cloud. So, we have different types of concerns. What is the optimal composition of the virtual sensor nodes and what is the optimal composition of the virtual sensor nodes. So, what it means I will talk about it shortly. The second one is the data caching you know. So, what happens is for certain applications, it is not required to always prime the sensors physically. At the physical level, you know the data do not change too much. So, you know data can be cached and can be made accessible to the end users, to the different users. If the data is not very stale, you know it can be made available to the end users as per the need and then, is the optimal pricing. So, pricing is very much important because it is a service offering sensor. Cloud service provider is offering these different services. So, service offerings are there, so how the price is going to be like, this is the optimal pricing.

(Refer Slide Time: 05:18)



So, first we will talk about the optimal composition of virtual sensors. So, this particular you know; if you are interested to look further into the details of this, this is a paper along with one of my students. We have you know this was published in ICC, International Conference on Communications in 2015. So, optimal composition of sensor virtual sensors.

(Refer Slide Time: 05:43)



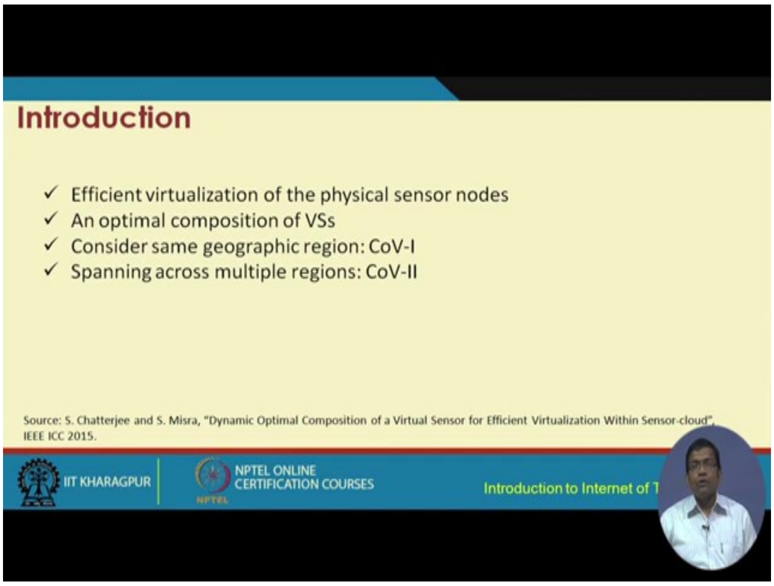
So, let us consider 2 different scenarios like this of sensor cloud. In one scenario, let us say we have we have these different sensors that are deployed and these sensors finally have to be virtualized virtualized, right. So, how many virtual instances are we going to create and what are these instances. It is not going to be like you know one physical sensor to one virtual sensor, it is not like one to one mapping between these physical sensors and virtual sensors. So, we could have these are like few virtual sensors that are created and corresponding to this one. We have this physical sensor, we have this virtual instance, we could even be having something like this or even we could have something like this.

So, this kind of mapping is possible is possible anyway. So, keeping apart that particular issue, you know which sensors, which physical sensors or corresponding to which physical sensors which virtual sensors are going to be or how these virtual sensors are going to be grouped along among themselves for a particular application on top. So, let us say how we are going to group them to serve a particular application on top. So, that is one issue and here we are considering that these sensors are physically located in a particular geographical location.

So, all these sensors are in one geographical location. Now, it might so happen that in real scenarios, it might so happen that we have different geographical locations and in these different geographical locations, we have first of all different sensors and the same thing has to be done over here in virtualization and the composition of these virtual sensors. So, what is going to happen here, again we are going to have few of these. So, this mapping has to be done and you know this particular sense in a virtual instance might be mapped with 2 different physical sensors in 2 different geographical area or it could even be something like these or these and these and something like that.

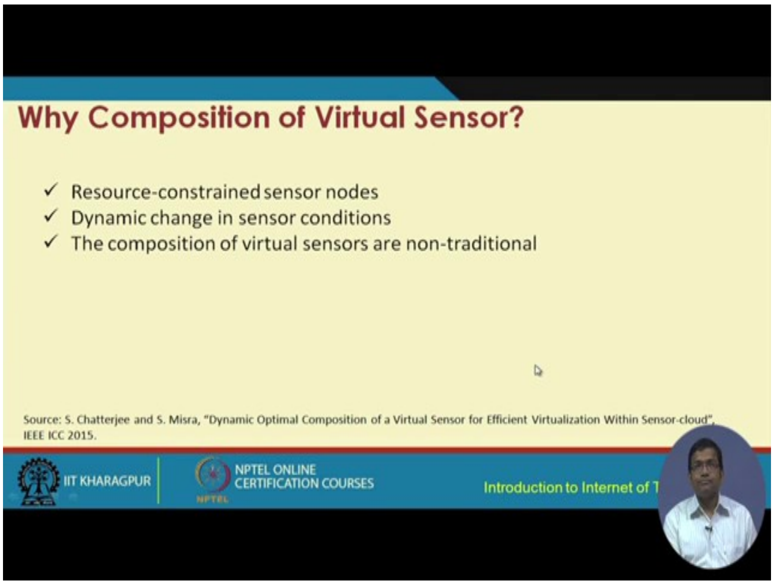
So, 2 things have to be taken here of a particular virtual instance corresponds to which physical sensors in a particular geographical location or across different geographical locations, number one and number 2 is how do you group these different virtual sensors together in order to serve a particular application in order to serve a particular application. So, this is the whole problem, a very fundamental problem to do with the deployment of sensor cloud. So, optimal composition of virtual sensors, the detail paper I set is available over here.

(Refer Slide Time: 09:40)



So, efficient virtualization of the physical sensor nodes is one problem. Then, how do you optimally compose these virtual sensors, how do you put them together, how do you group them together. So, for this again if all these sensors are located in the same geographic region, you have one kind of scheme and if it is spanning across multiple regions, you have a different scheme.

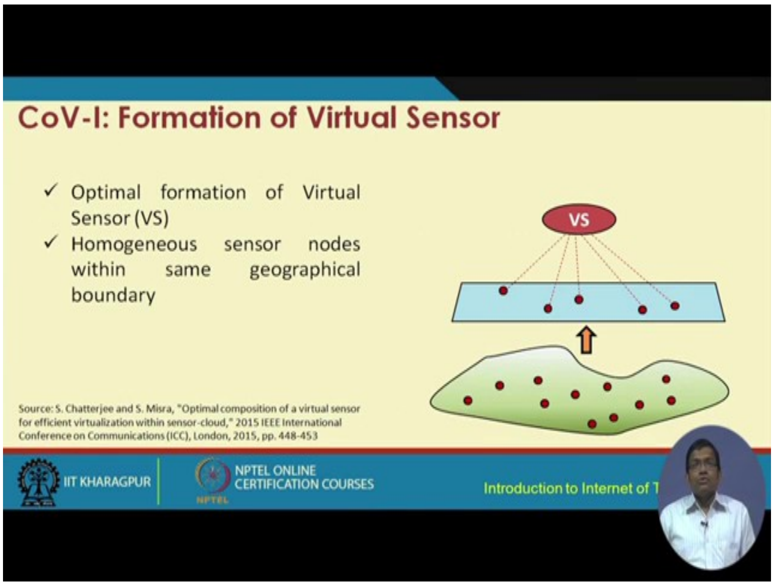
(Refer Slide Time: 10:07)



So, why composition of the virtual sensors? It is because the sensors are inherently resource constraint, energy constraint, communication constraint, computation constraint and so on. Dynamic change in sensor conditions also exist to the sensors. We are changing dynamically, not only their duty cycle, the energy resources etcetera. Their status they change dynamically and not only that, but also the physical conditions around them also change. The sensor conditions consequently will also change. Additionally it might so happen that some sensors, they are you know due to some hardware or software failure, they fail operate and that is why they do not you know at one instance of time they are operating, but at the very next instance they may not be operating.

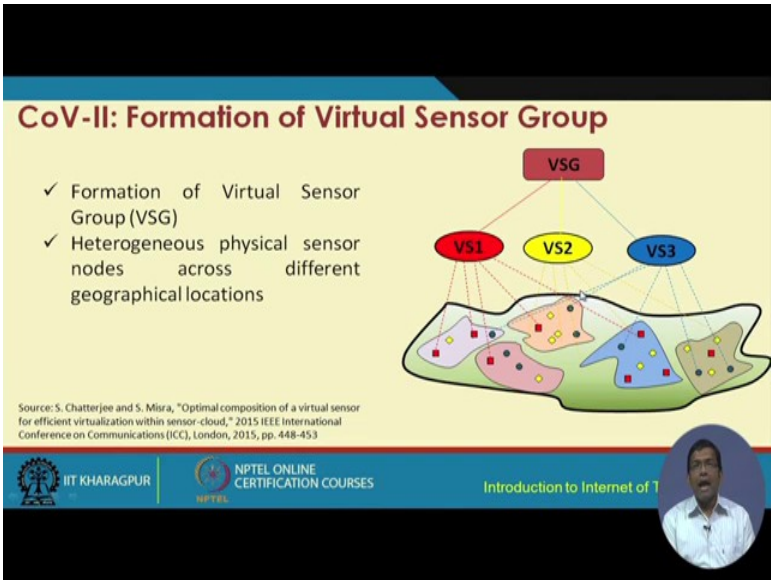
So, we have all these different types of changes that are possible in these kind of networks. The composition of the virtual sensors are non-traditional you know. So, you know if we talk about traditionally, what is going to happen let us say we have this infrastructure as a service software as a service you know each of these. So, let us see infrastructure as a service or like software as a service. So, what they are dealing with is just one kind of virtualization, virtualization of only one type whether if the virtualization of software virtualization of infrastructure and so on, but over here we have a different scenario. Here we are talking about virtualization of different things. Different types different types has to be virtualized, so it is a bit different over here.

(Refer Slide Time: 11:54)



So, the formation of virtual sensors as I tell you before, if all these different sensors are located or collocated, not only collocated, but also may be in the same geographic location, they could be virtualized and these virtual composition, virtual sensor could be formed out of a subset of the physical sensors in this particular manner and in this particular scenario, it is considered that for optimal composition. We at the physical level, we are homogenous sensor nodes. The sensor nodes, they all have their own you know different specifications. Not different specifications, but the same specification. They all have their own same specification and you know you group them together in order to form the virtual sensor node.

(Refer Slide Time: 12:43)



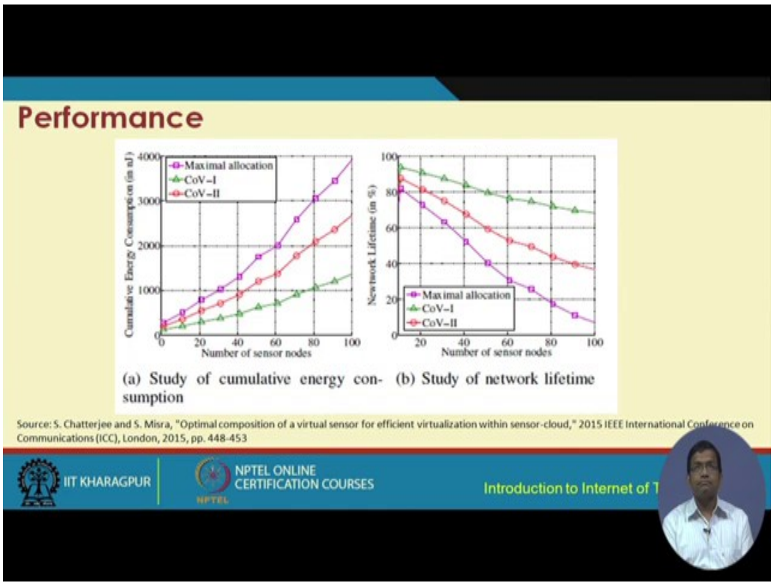
In this particular scenario, we have the virtual sensor groups, different locations, geographical locations having different sensors and as you can see over here through these different labels, they have not labels, but you know we have these different colored sensors denoting different types of sensors in specification in types. Types means; you know temperature sensor, humidity sensor, these are different types.

So, you know temperature sensor, you know pressure sensor, camera sensor, these are different types of sensors. So, you know in this particular formulation, they have considered, we have considered that not only that the sensors are geographically distributed, they are geographical separated from each other, but you know they can be composed, they are heterogeneous and they can be composed in this particular fashion. So, you can have a virtual sensor which is comprised of or it is mapped to the physical sensors in one geographical location and some other physical sensors in another geographical location, some other physical sensor in a third geographical location, some other physical sensor in a fourth geographical location.

So, these all will be taken together. They may not necessary be one and the same. They may not be the same that is they may not all be of the temperature sensor, but they could be you know temperature sensor along with pressure sensor. You know temperature sensor in one location; pressure sensor in one location. So, they all can be put together and club together, abstract it together as a virtual sensor. So, we have likewise different other virtual sensors formed together and these virtual sensors add another higher level can be put together and grouped together to form virtual sensor groups. So, for example, VS1 and VS2 can be grouped together to form a virtual sensor group or VS2 and VS3 could be you know grouped together to form virtual sensor group. In this particular example, we see that a particular virtual sensor group is formed out of these three VS; VS1 VS2 and VS3.

So, remember one thing that unlike the previous formulation, here we had considered homogenous sensors at the physical level and here we have considered heterogeneous sensors on top of the fact that they could be geographically dispersed. They may not all be in the same geographic location. Different sensors from different geographic locations can be mapped together to form virtual sensors at the higher level of abstraction and these different virtual sensors again can be clubbed together to form virtual sensor groups.

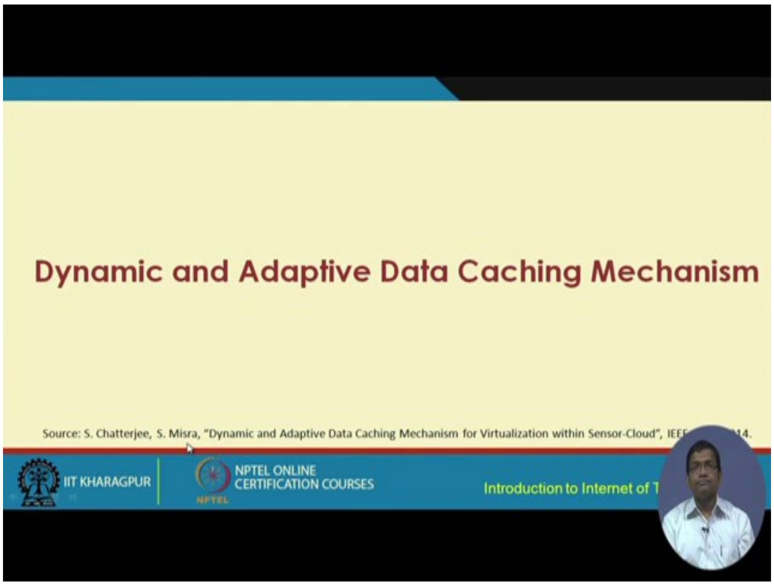
(Refer Slide Time: 15:40)



So, in terms of the performance, you know when we talked about CoV I and CoV II corresponding to the composition of the virtual sensors in the homogenous and the heterogeneous geographically distributed manners as we spoke about in the previous 2 slides. So, we have you know if we look at the comparison of performance with respect to the energy consumption, because this is cumulative energy consumption for PC over here is CoV I. This is the plot for CoV I and this is the plot for CoV II. So, as we can see over here that the energy consumption basically steadily increases in each of these and quite understandably that CoV II basically in curse greater energy consumption compared to CoV I and in terms of the life time, this is a comparison of the lifetime for each of these 2 scenarios. As we can see over here that the red colored one is for CoV II and the green colored labels are for CoV I.

So, life time on the other hand increases not other hand, but lifetime basically increases if we have the homogenous sensor scenario, where the sensors are from one geographic location and they all have the same specification. So, we have these 2 different scenarios of cumulative energy consumption and network life time and the comparisons between CoV I and CoV II and as I said before if you are interested to look further into these, you may refer to this particular paper. The optimal composition of a virtual sensor node, for efficient virtualization within sensor cloud, this is a paper that you know was published by us in ICC conference that was in 2015 in London.

(Refer Slide Time: 17:38)

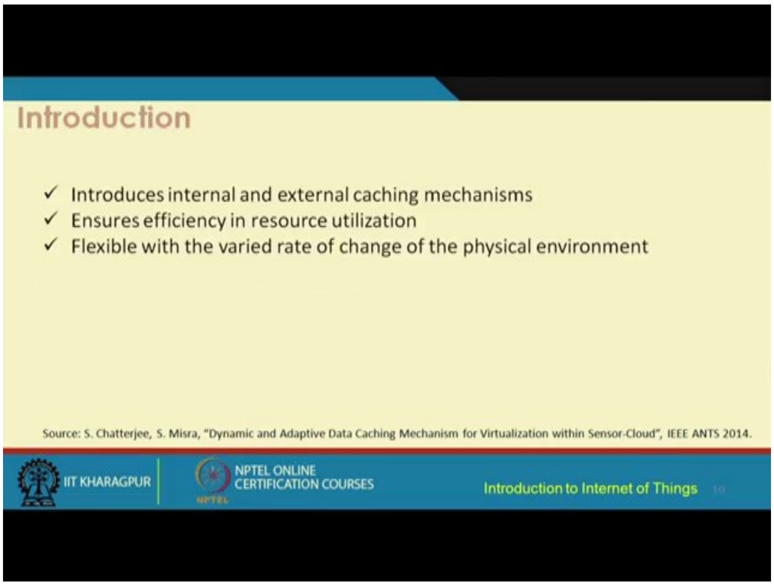


Then, we come to the second problem which is the dynamic and adaptive data caching mechanism. So, before I go to the details of it, I would like to give you a few examples. Let us say we are talking about environment monitoring with the help of different types of sensors including temperature sensor.

Now, in a particular area, the temperature does not change too frequently. So, it is unnecessary to always collect data from the different sensors at very frequent intervance. It is unnecessary and similarly, it is also unnecessary to make the corresponding virtual sensors available to the end users to different end users. So, it is sufficient if the temperature values are connected and are cached and are stored and we made available to the different users whenever they need access to that information. It is not required to create a virtual instance and then, have that virtual through that virtual instance collect or prime that particular sensor to collect the data to make that sensor in a sense and collect the data at you know consecutive instances of time at subsequent intervals of time by different users.

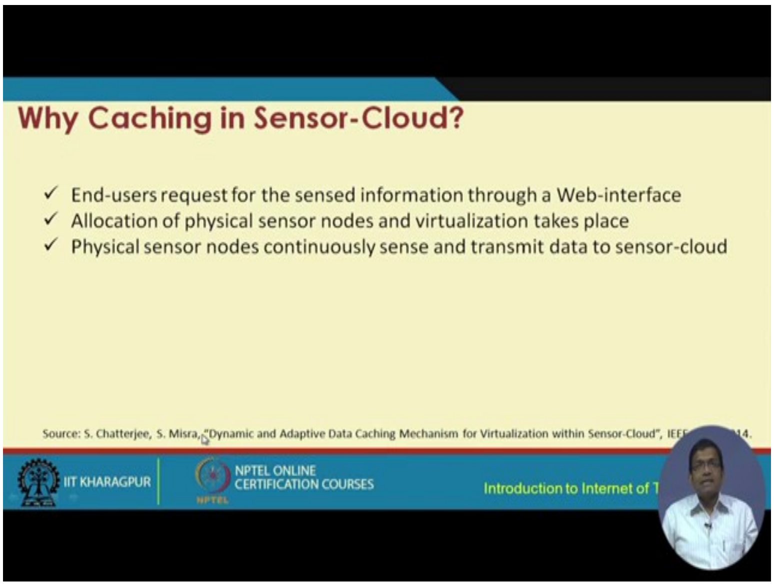
So, it is required to cache. So, there are likewise different scenarios, different applications where this is required to cache.

(Refer Slide Time: 19:16)



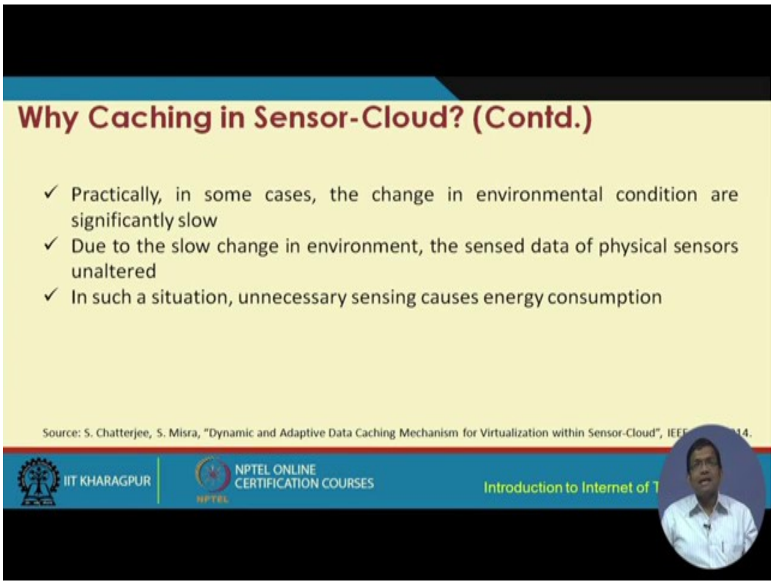
So, we will look at the different ways to cache. So, basically this caching introduces 2 different types of cache. One is the internal cache; the other one is the external cache. So, this example that I was giving you was about that external cache. We will look at the internal cache shortly. So, this caching mechanism basically ensures efficiency in resource utilization. So, caching basically is flexible with the varied rate of change of the physical environment.

(Refer Slide Time: 19:43)



So, why caching is required in sensor cloud because end users request for the sensed information through a web interface and the allocation of the physical sensor nodes and virtualization takes place and the physical sensor nodes continuously sends and transmit the data to the sensor cloud, and that is the reason why you know it is not always required to you know prime and probe the sensors to sense and continuously send the sensed data through the web interface to different end users.

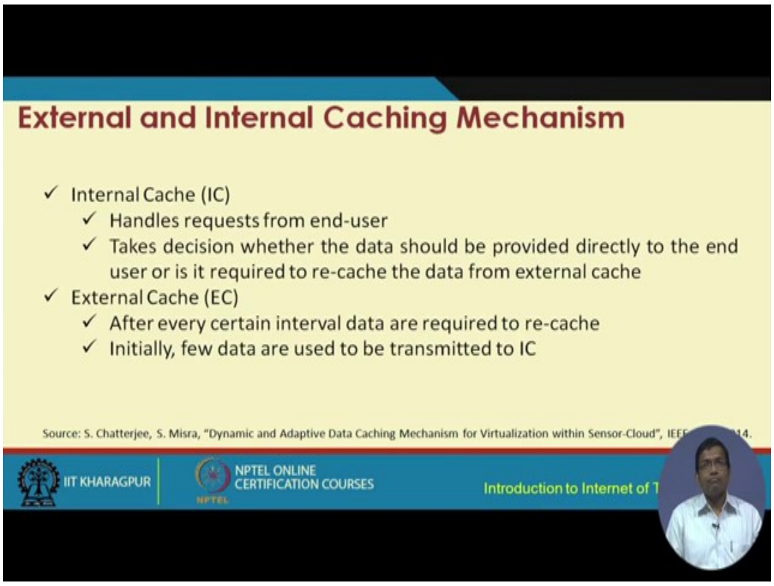
(Refer Slide Time: 20:17)



So, practical in some cases, the change in environmental conditions are significantly slow like in the case of temperature change or humidity change and so on. So, they are not very fast. So, it is not required to always sense through the physical sensors. So, even if you sense, it will give you merely the same value. The physical sensors are not going to give vastly different values. So, they remain physically unaltered. Due to the slow change in the environment, the readings are going to be unaltered.

So, in such a situation, it is unnecessary to sense because sensing would again unnecessarily consume energy which is undesirable.

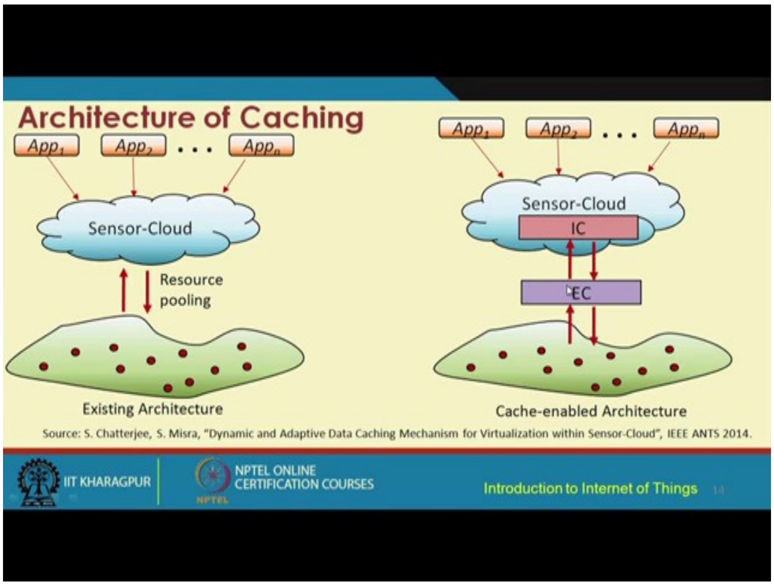
(Refer Slide Time: 21:01)



We introduce the concept of internal cache and external cache. I am going to talk about these 2, but before I proceed further, I would like to give you the reference for this particular paper while published by us. If you need more details about this internal and external cache and how this caching mechanism operates, you can go through this particular paper, the reference of which is given over here at the very bottom of this slide and this was published in the ICC conference in 2014. So, let us now go back and try to understand; what is the difference between the internal cache and the external cache.

So, the internal cache basically handles the request from the end users, takes decision whether the data should be provided directly to the end user or is it required to re-cache the data from the external cache. What is this external cache? So, it is a separate piece of server or hardware which at every certain interval of time, it collects the data and stores inside it. So, initially few data are used to transmit to the internal cache.

(Refer Slide Time: 22:14)

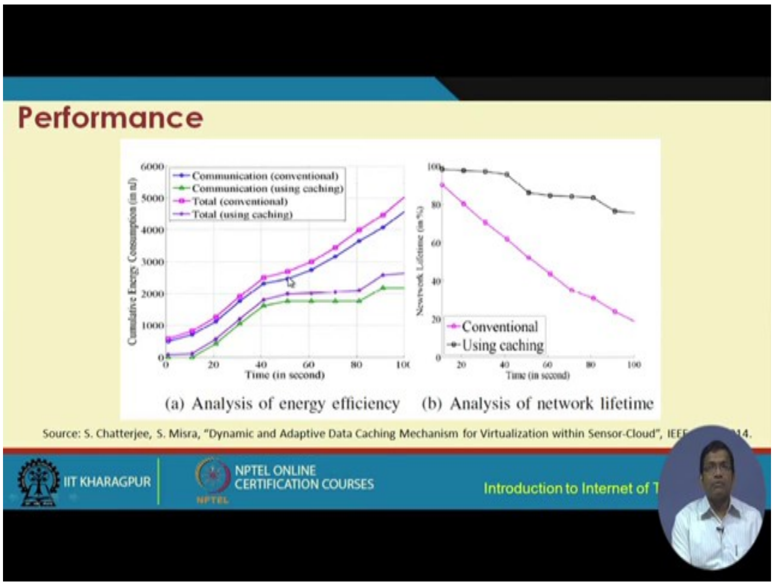


So, this is the architecture of caching. So, this is the existing architecture and this is the case cache enabled architecture. On the left, we have this existing architecture where we had these different physical sensors and this is that sensor cloud and these apps are getting accessed to the sensors through the sensor cloud, through resource pooling mechanisms.

Now, in the cache enabled architecture, we have this internal cache and the external cache. External cache could be conceptualize something like a separate server which is outside the cloud, where the data that are made available to the end users through these apps are also cached at the same time in this server in this external cache. So, you know it might happen that periodically at different instances of time, it is not required to prove that physical level sensor again. So, you know the data if it is not very much stale, it could be fetched from this particular external cache and if it could be done even better, it might happen that these different virtual instances that are in the sensor cloud here, the data might be also available. May be one user is already using it and that data could be made available because if you have to fetch it outside the cloud, that is going to increase the time for fetching. So, you want to keep something over here as well.

So, this is internal cache and this is how it differs from the external cache. So, external cache is an external server kind of thing, however internal cache is resident inside the cloud, inside the sensor cloud and this is how it differs from the external cache.

(Refer Slide Time: 23:59)

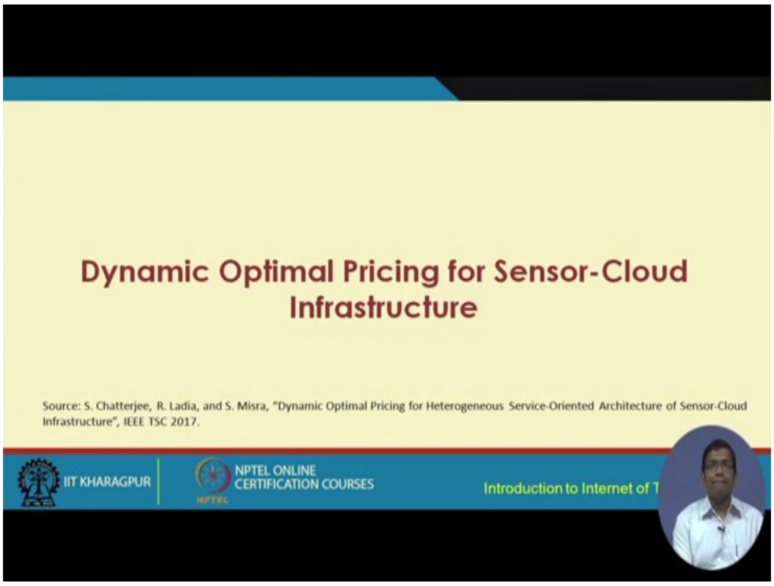


Here is the comparison of performance between the caching mechanism you know using internal and external caching mechanisms and in the conventional mechanism like as I showed, the conventional means this is existing conventional mechanism and caching based mechanism means this particular mechanism is what we see is the performance comparison between the 2.

So, in terms of let us say the total you know cost total energy consumption, so total energy consumption in the case of the conventional mechanism means, without using the caching mechanism is shown over here, in this particular pink colored plot. Whereas, the total energy consumption using caching is shown in this particular purple color plot. So, as you can see over here that the total energy consumption decreases quite significantly if we are using the caching mechanism as shown in this particular figure. How it compares with this pink colored plot in terms of the network life time here is the conventional scenario and here is the scenario of using caching. So, as you can see over here, conventionally the network lifetime is much more reduced and if we are using caching, the lifetime basically improves a lot.

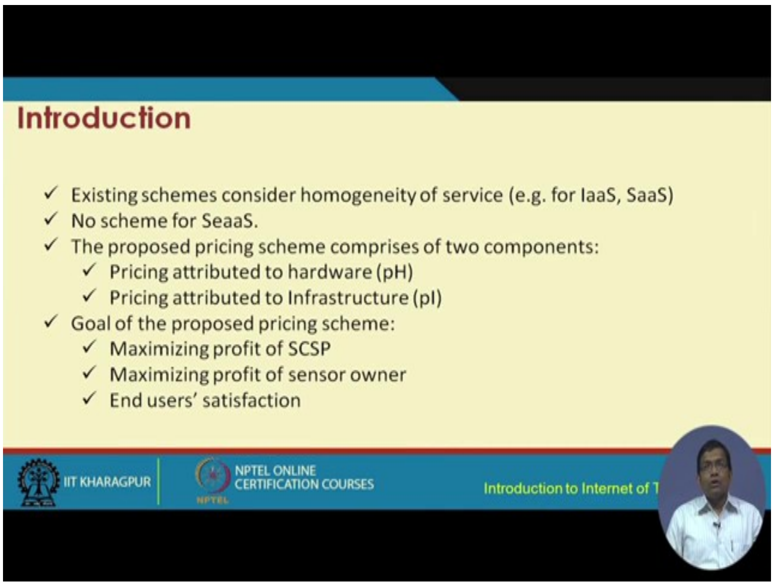
So, it is quite significant in terms of the difference between using caching and without caching mechanism. So, caching basically improves overall network life time.

(Refer Slide Time: 25:38)



Finally, I would like to talk about another issue of sensor cloud. Again this is taken from a paper that we have published in IEE transactions on services computing in 2017 and here we have ticked into the issue of pricing in sensor cloud and how we can come up with an optimal pricing mechanism in a sensor cloud scenario, where that pricing mechanism itself is not only optimal, but dynamic in nature. So, the pricing itself is dynamic.

(Refer Slide Time: 26:12)

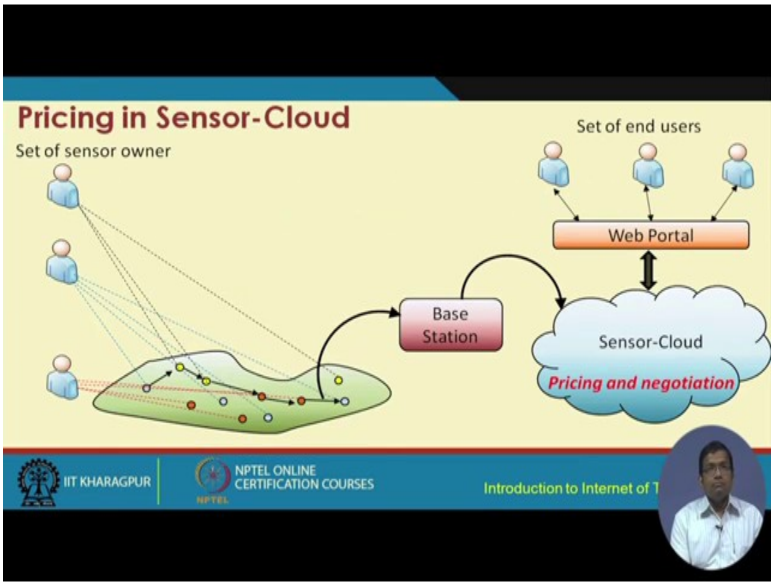


So, how does it happen? So, we will talk about that.

So, if we look at the existing cloud where IaaS, SaaS, PaaS models are used, there you are talking about homogeneity of services. So, existing pricing schemes in the cloud, the regular cloud are talking about homogenous services whether it is a SaaS service, the PaaS service or IaaS service and there is no scheme for pricing for sensors as a service. That means, this particular sensor cloud scenario sensors as a service c as scenario. So, we have proposed a pricing mechanism that comprises of 2 components. One is the pricing that is attributed to the hardware which means the sensor and the pricing that is attributed to the infrastructure. That means, the other infrastructure that are that are in place the operating system, the other hardware infrastructure the switches the servers and so on.

So, pricing attributed to the hardware which is for hardware like sensors and the pricing attributed to infrastructure, so p H and p I. So, the goal of the proposed pricing scheme is to maximize the profit of the sensor cloud service provider, maximize the profit of the sensor owner and to maximize the satisfaction of the end users.

(Refer Slide Time: 27:36)

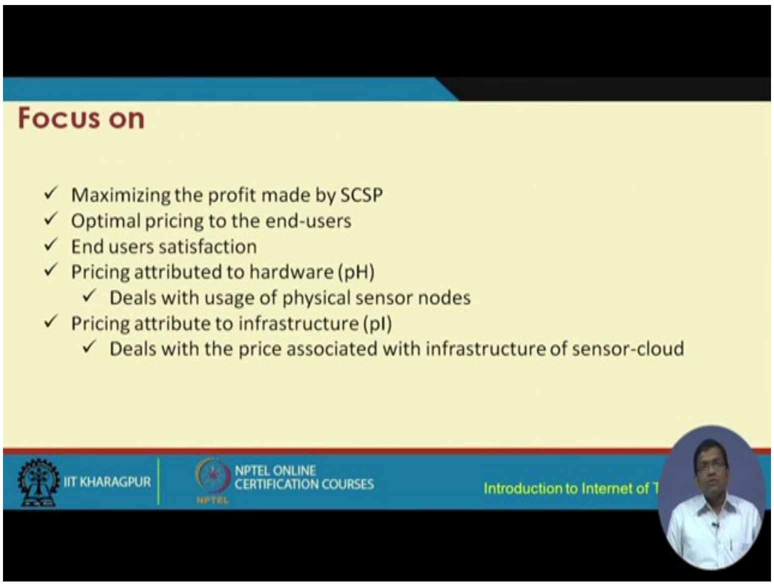


So, if we look at this scenario, we have this different end users. Now, you see that what might happen if the sensing has started from particular point. So, to sink when it travels in sensor networks; the sensor data from the source to the sink, it travels via different intermediate hops and these hops could be belonging to different sensor owners in this particular manner.

So, when you talk about a pricing mechanism, we have to take into consideration the pricing due to the hardware cost belonging to different sensor owners in addition to the sensor cost of the specific owner from where the sensor sensing has taken place of the sensor from the sensor. So, this sensor data is made available through the base station to the sensor cloud and is made accessible to the end users. So, end users will not only have to pay for the hardware cost of these sensor, that means the source sensor, but also the hardware cost of these sensors plus also hardware cost. Not hardware cost, but the infrastructure cost or other types of infrastructure that are in place like the base station, the servers, the switches and so on.

So, all these also have to contribute towards the price. So, how do we come up with a pricing mechanism, negotiation is the scenario where the prices can also be negotiated. So, this may not happen in all different cases, but in some cases it might happen that the end users would be able to bargain and be able to negotiate the price with the sensor owners or with the sensor cloud service provider. So, there would be some kind of a bargaining mechanism in place. It will be a market place kind of scenario, an oligopolistic market place scenario, where this kind of bargaining can take place.

(Refer Slide Time: 29:47)

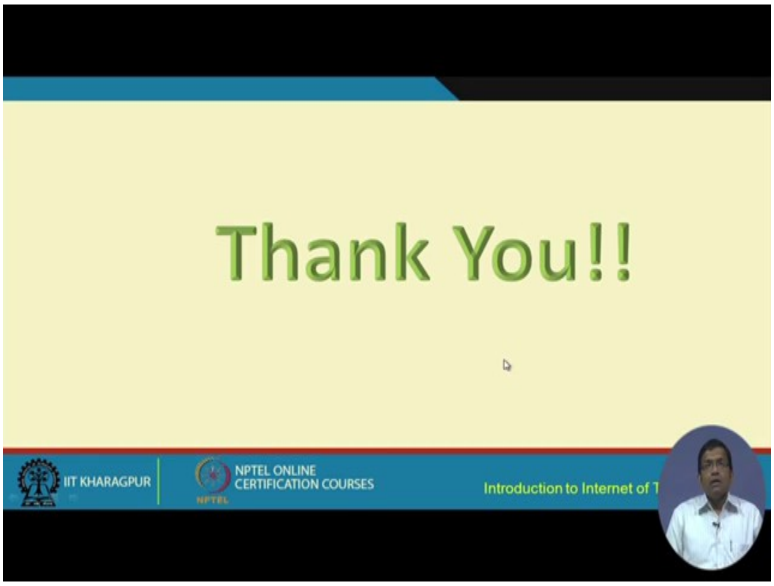


So, the focus is on maximizing the profit that is made by the sensor cloud service provider, optimal pricing to the end users, increasing the satisfaction of the end users by considering different factors. All the above three by considering different factors, such as the pricing that is attributed to the hardware while dealing with the usage of the physical sensor nodes, pricing attributed to the infrastructure by dealing with the prices associated with the infrastructure of the sensor cloud.

(Refer Slide Time: 30:16)

So, these are some of the different issues and the least of different references. If you are interested to know further about sensor cloud, the different works on sensor cloud, here are few references for you. As you see over here in our group in the Swan lab, we have done a bit of a digging into the depth of sensor cloud, sensor as a service, virtualization of sensors, composition of sensors, caching of different sensors and so on. So, these are different things that we have done in one of the papers. I will tell you that this particular paper also talks about a comparison between a side by side comparison, a quantitative comparison between sensor cloud and the traditional sensor networks.

(Refer Slide Time: 31:04)



So, with this we come to an end of sensor cloud. Sensor cloud is a very important technology at present for enabling sensor networks; sorry for enabling internet of things and internet of things basically you know if you think little bit deep can be made efficient. The implementation of internet of things can be made efficient if we are talking about sensor cloud and sensor cloud has some similarities with in concept with the fog computing and cloud computing.

That also has been covered in the different literature and this is for you to try to understand that; what is the difference between sensor cloud, fog computing and regular cloud computing. This is all to do with efficiency; you know access to different services. You know these are with respect to these things. Basically they differ a lot and we know it is not like if sensor cloud is there. We do not need cloud. It is not like that and also, it is not like that if sensor cloud is there, we do not need fog. So, we need all these three things at different times. You know they are useful for different scenarios. So, we need all of them together. So, all of these technologies are required to build Internet of Things.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

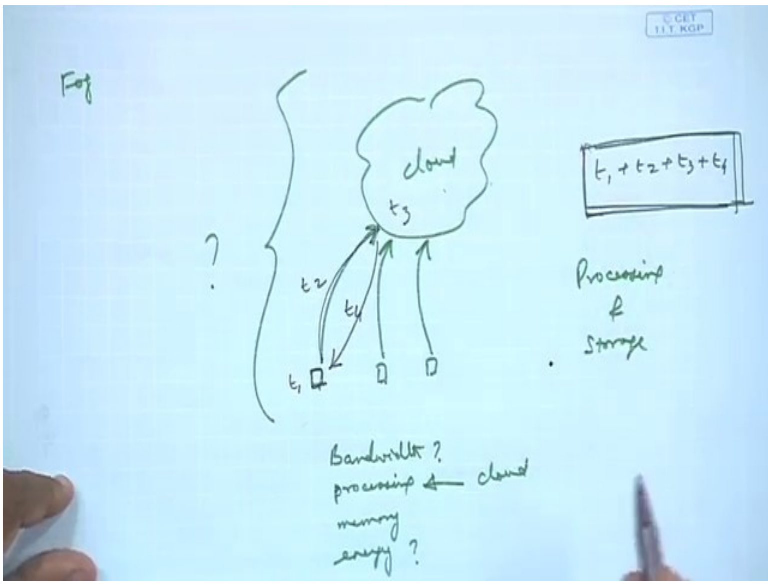
Lecture – 44
Fog Computing – I

In a previous lecture, we discussed about cloud computing and its importance in Internet of Things.

(Refer Slide Time: 00:23)

So, cloud is very important because you see that internet of things IoT devices; sensors, RFID devices and so many different types of devices, this sends so much of data and finally, those data have to be handled and that is the reason that a cloud came into picture; that all these data will be sent to the cloud for further processing and so on and so forth. Now, the main problem with cloud in internet of things environment is that latency. So, what is meant by latency; I will explain to you before we go formally about discussing the concept of fog.

(Refer Slide Time: 01:14)

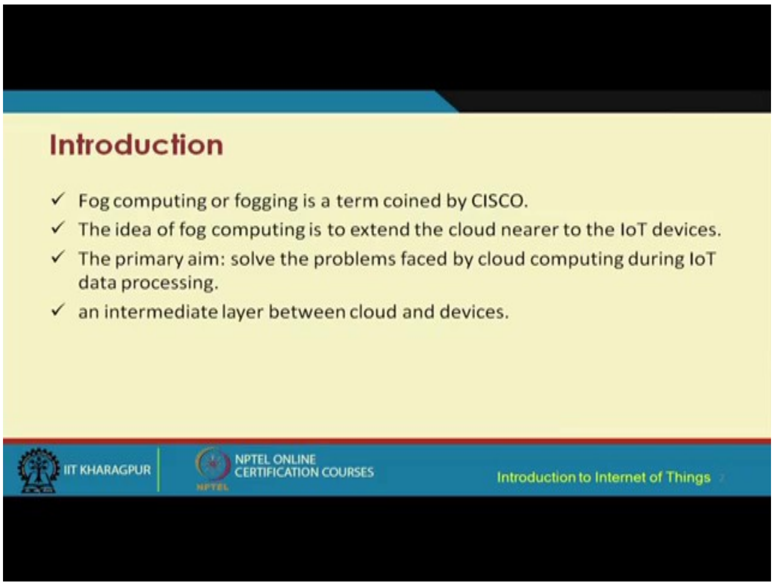


Let us say that we have a cloud and we have different IoT devices deployed. Now, what we have discussed when we were talking about cloud computing in the context of internet of things is that each of these devices, they send all these data to cloud; for further processing and storage further processing and storage. Now, that is a problem because you see this IoT environments, number one are constraint in different ways with respect to bandwidth, with respect to processing, with respect to memory, with respect to energy and so on so forth.

Now, this processing can be handled with the help of cloud, but what about the bandwidth, what about the energy consumption because what is going to happen in this sort of scenario of use of cloud in the IOT context is lot of data is going to float all around; over the network, lot of data through the internet are going to be sent to the cloud and that will unnecessarily consume the bandwidth and that will also consume unnecessarily the limited energy that is resident in all this devices and so on. So, we do not want to do that because communication consumes most of the energy.

So, we do not want unnecessary communications to take place and even if we do, we have to limit. Even if we have to communicate and that is required because in a network basically IOT is basically a network, so network communication is required, but how do we handle it efficiently this is what we are going to discuss in this particular lecture. So, can we do something which is better than cloud? So, this is where fog comes into picture.

(Refer Slide Time: 03:46)

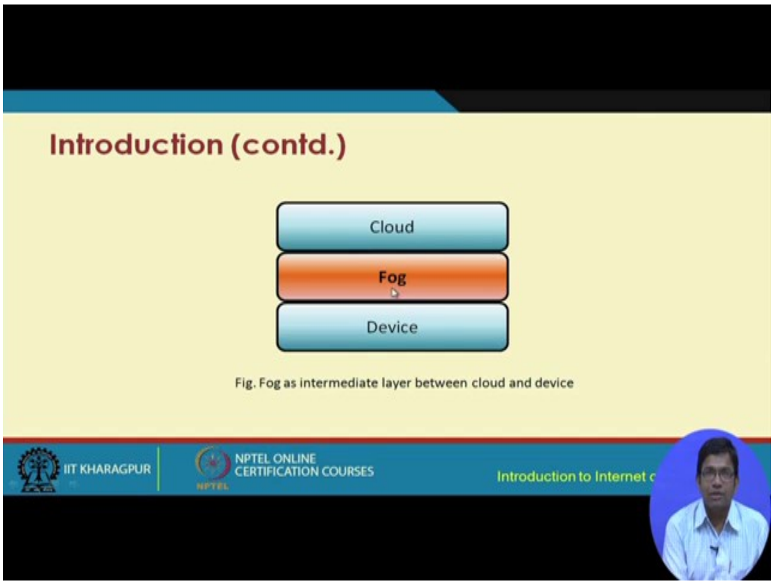


Fog was introduced by CISCO. So, it was sort of like an idea about how to being the cloud facilities close to the IoT devices because as we saw that we have all these data sent to the cloud you know that will not only take the bandwidth, limited bandwidth that is there in this kind of environment, but also that is going to take lot of time take lot of time. So, in this particular case, the time that is required will be the time from when that event is sensed, that piece of data is sent to the cloud. So, this one let us say this is t_1, this is t_2, then the time for processing t_3 and finally, that response will be sent back, so t_4 So, the response will be sent back for may be activation or something like that.

So, this basically becomes t_1 plus t_2 plus t_3 plus t_4. So, this is the total time that it takes until when the receiving device gets a signal about what to do and by such a time in most of the real life applications of IoT by this kind of time, you know most of you know the events, most of the unwanted events would take place. For example, if it is a surveillance application, maybe the intruder by this time because there is so much of latency that is involved, by this time the intruder might have already intruded into the territory or if it is a medical emergency scenario, by this kind of time it takes to send it to the cloud processing at getting a response back etcetera. So, even the real timelines is going to be lost and because of this particular issue what is going to happen is, if it is medical emergency situation, the patient might die, right.

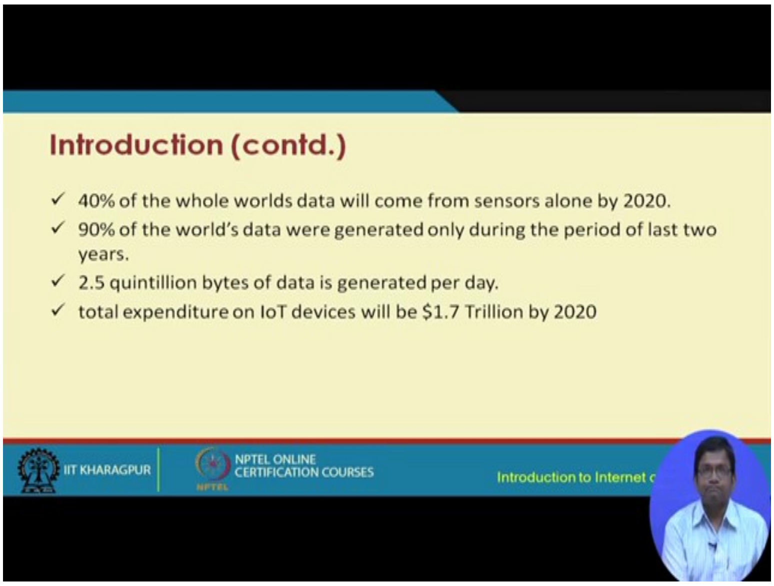
So, what is required is can we reduce the latency and this is what we are trying to do in fog computing. So, as I said that fog was basically proposed by CISCO and the whole idea is can we bring the cloud facilities, the attractiveness of cloud closer to the IoT device layer and the whole idea is to solve the problems that are faced by cloud computing for use of IoT for data processing. So, this is the whole objective of fog computing and the whole idea is also to reduce the delay that is incurred in sending the data from the sensor device to the cloud, from the cloud getting a response back and activating the particular device. So, can we reduce this particular time? So, this is the whole idea.

(Refer Slide Time: 06:51)



The whole premise under which the fog computing works, so conceptually what we have, we use to have IoT and cloud. You know this is the device layer where all these IoT devices, the physical devices operate and this is the cloud where all the data are sent for processing and storage. So, what fog is saying is, it is going to be sort of like a middleware or a middle layer rather where some of the computation, some of the processing, some of the storage at least transient storage is going to happen. Before the data that is sensed by these devices are sent to the cloud. Before it is sent to the cloud, can we do some intermediate processing, intermediate storage for you know quicker decision making? This is the whole idea behind the use of a fog computing.

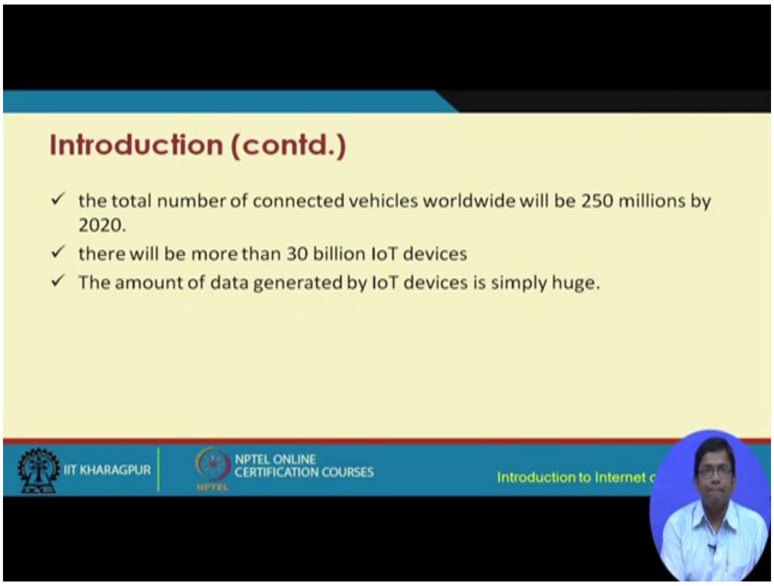
(Refer Slide Time: 07:41)



So, let us go back to some statistics which you know we also went through at the beginning of the course. So, we know that now it is because of all these different sensors etcetera, there is lot of data that is floating all around. So, it is estimated that by round 2020, 40 percent of the world's data will come from sensors and 90 percent of the world's data will be generated only during the period of last 2 years. So, 90 percent of world's data was generated only during the period of last 2 years.

So, you know it is also estimated that every day about 2.5 quintillion bytes of data is produced and the total expenditure on IoT devices will be about 1.7 trillion dollars by 2020. So, given all these different statistics, we now have to think about architecture of internet of things; where in we can use all these different devices in a scalable manner, such that the processing happens with large number of devices in a quicker manner and in an efficient manner.

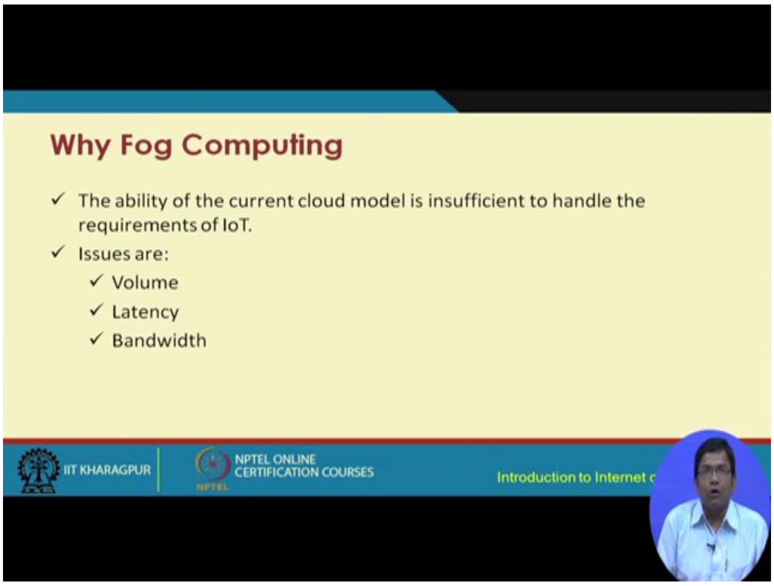
(Refer Slide Time: 09:03)



The total number of connected devices, sorry the total number of connected vehicles worldwide will be about 250 million by 2020 as per estimates and there will be more than 30 billion IOT devices again as per estimate.

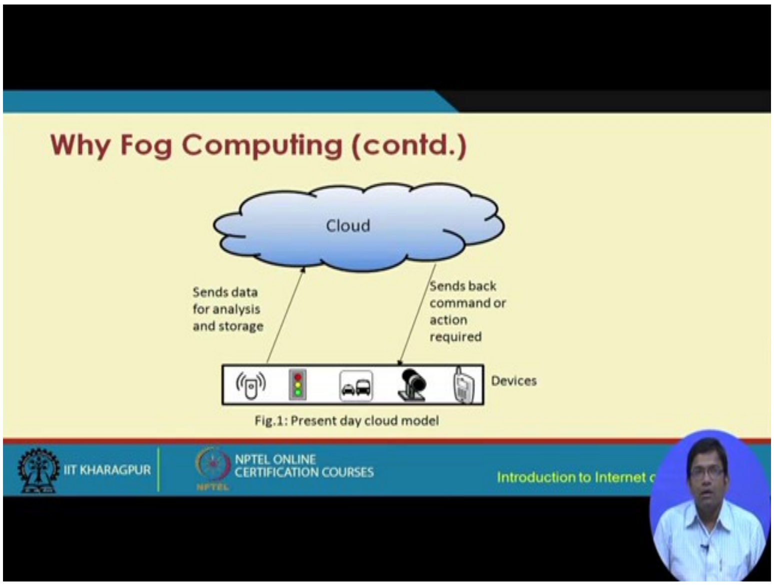
So, the amount of data that is going to be generated by these IOT devices is obviously quite huge. So, how do we handle this kind of huge data? I mean one way is basically to use all these big data analytics and so on, but even before that can we deduce the processing time of these data, can we do something from the network point of view and that is where we have to take help of fog.

(Refer Slide Time: 09:46)



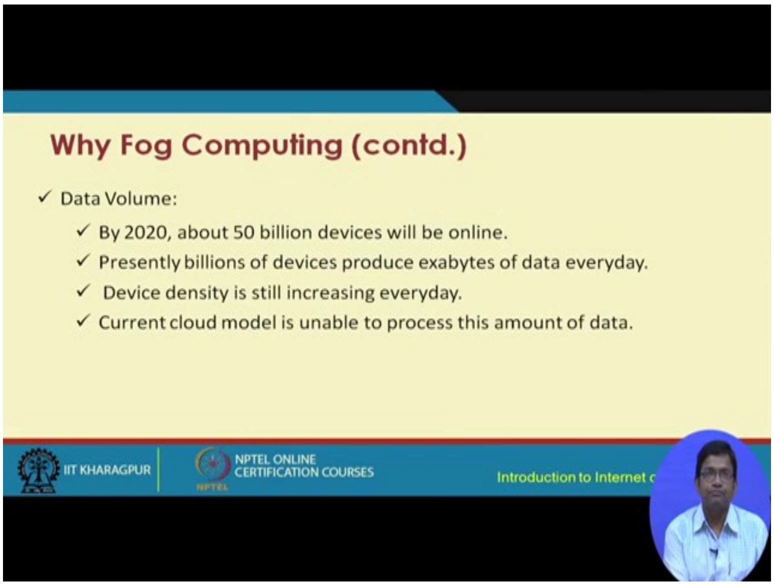
So, why do we need fog computing? It is because cloud has certain deficiencies. You know it is insufficient to handle the requirements of IoT. So, there are issues with volume of data that is produced by the IoT devices, the latency. That means, the time that it takes for a sensed data to go to the cloud and then come back, that duration is the latency and the bandwidth. Bandwidth means that you know how much data is going to I mean how much channel is going to be occupied because of this communication of all these data from the IoT devices.

(Refer Slide Time: 10:35)



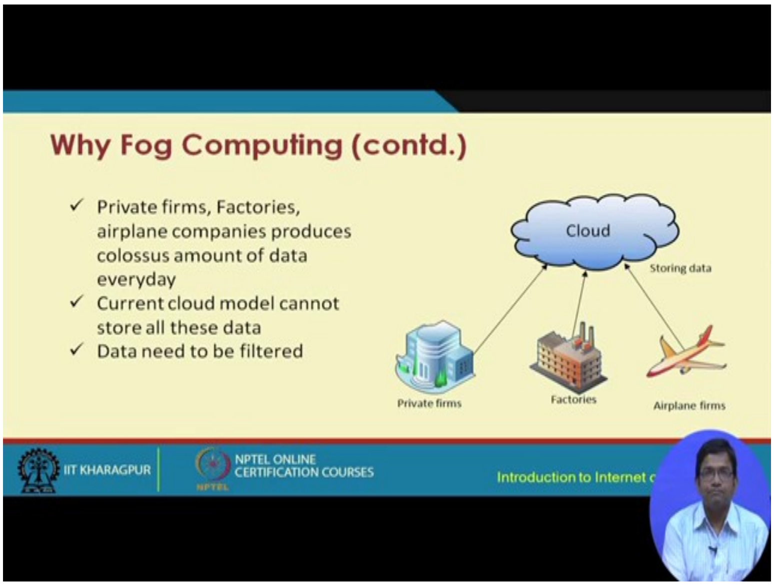
So, the fog computing architecture looks like this. So, we have all these IoT devices and we have the cloud. So, as I said traditionally we have to use these IoT devices to sense the physical phenomena occurring around them; send the data to the cloud and get an action or comment back. So, as we can see over here that this is the traditional cloud model. So, why we need fog computing because we want to reduce this particular time and typically, this cloud servers might be physically located even continents away means you know it is typical to have them in different cities and so on, but even continent away also. So, this physical limitation also introduces large latency in communication.

(Refer Slide Time: 11:39)



So, in terms of the data volume, it is estimated that by 2020, about 50 billion devices will be online and presently billions of devices produce exa bytes of data everyday and this is big data, right. So much of data is going to a produced every day, not only every day, but every second, every minute. Unusual volumes of data are going to be produced because of the introduction of internet of things. Exabyte means 10 to the power 18. So, you know we have gigabyte, terabyte, betabyte, gitabyte, exabyte, right. So, typically we use traditionally with gigabytes up data maximum, but now it is with you know internet of things and so on, it is very common to have terabytes, gitabytes, exabytes of data that is produced everyday and to handle this kind of data volume. So, the device density is also increasing everyday. So, the current cloud model is unable to process these amount of data.

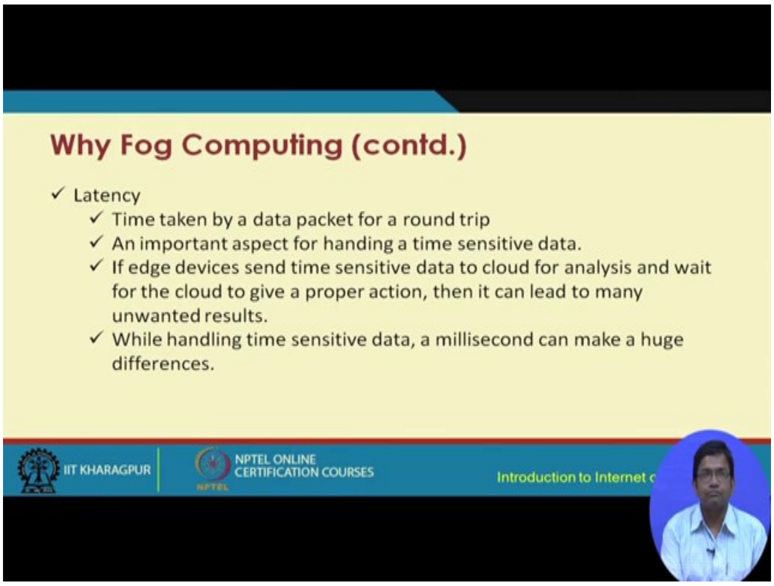
(Refer Slide Time: 12:55)



So, the private firms, factories, aero plane companies, they all produce huge volumes data every day. So, if you look at this particular figure, this will be clear. So, we are not talking about data produced by a single firm, we are talking about data that is produced by several firms you know and the different devices that are used in those firms i.e. the IOT devices, the embedded systems devices that are basically used in those firms. You know huge volumes of data are produced every day by a single firm and definitely large number of firms also produce large volumes of data factories. The same kind of thing factories also produces large volumes of data, aero plane companies. Airplanes themselves have lot of different types of sensors. They also produce large number of data. So, all these data would have to be sent to the cloud for further storage and processing.

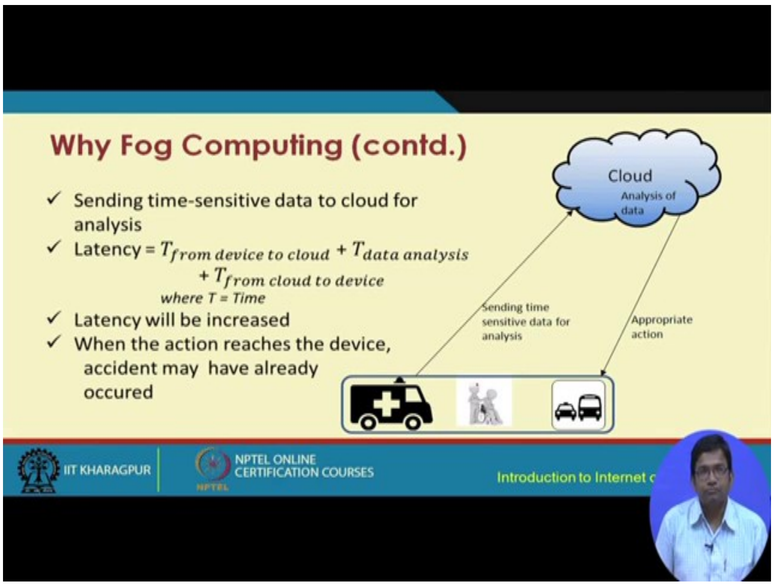
So, the current cloud model that we have already gone through in the previous lectures on cloud computing cannot basically store all these data. So, this data that is produced the raw form of data has to be filtered before the data is sent to the cloud., So, this has to be pre-processed, filtered before it is destined for storage and processing in the cloud.

(Refer Slide Time: 14:28)



In terms of latency, lot of time being taken by a data packet for a round trip and this is what I was explaining to you with the diagram that I showed at the outset. So, an important aspect for handling time sensitive data is basically to handle this issue of latency because if it is time sensitive, it is real time data. So, time is important and that is the reason why latency has to be handled with special interest. If the age devices sent time sensitive data to the cloud for analysis and wait for the cloud to give a prospered action, then it can lead to many wanted results. So, file handling time sensitive data a million second can make a huge difference.

(Refer Slide Time: 15:18)

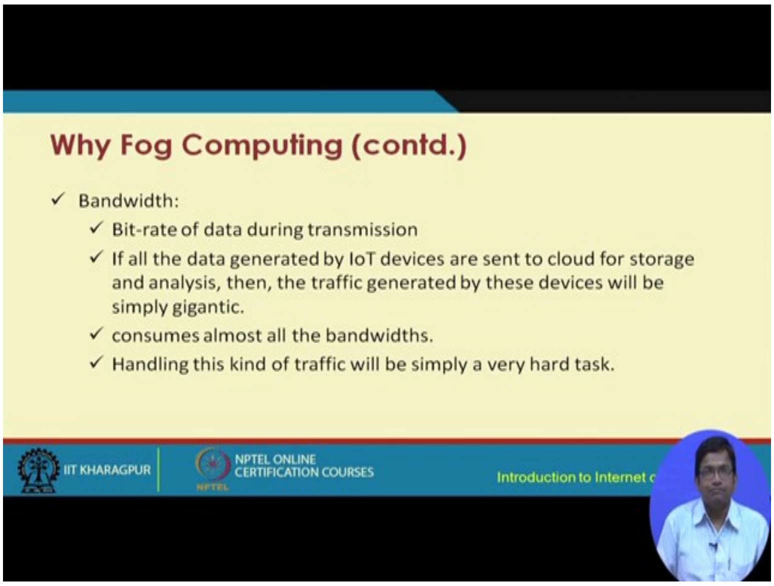


So, look at this particular figure over here. So, ambulances, then different buildings and different other you know different other devices and so on and cars and so on. So, they basically generate data which are time sensitive in nature. So, they basically generate; which are time sensitive in nature. So, that is the reason why they have to be processed pretty fast to be able to use the data in a meaning full manner.

So, they have to be paid processing pretty fast. So, ambulance for example will generate some data. So, the time that it takes the data to go from here to the cloud and come back, this can be represented with this you know this can be shown in the form of this kind of equation. So, latency equal to the time, it takes for the data to go from the device. That means the IoT device to the cloud plus the time for data analysis plus the time; it takes for the data to travel from the cloud to the device. So, latency will be increased and from the action reaches the device accident may have already occurred if it is an emergency situation or a connected vehicle situation.

So, this is the reason why fog computing is very important.

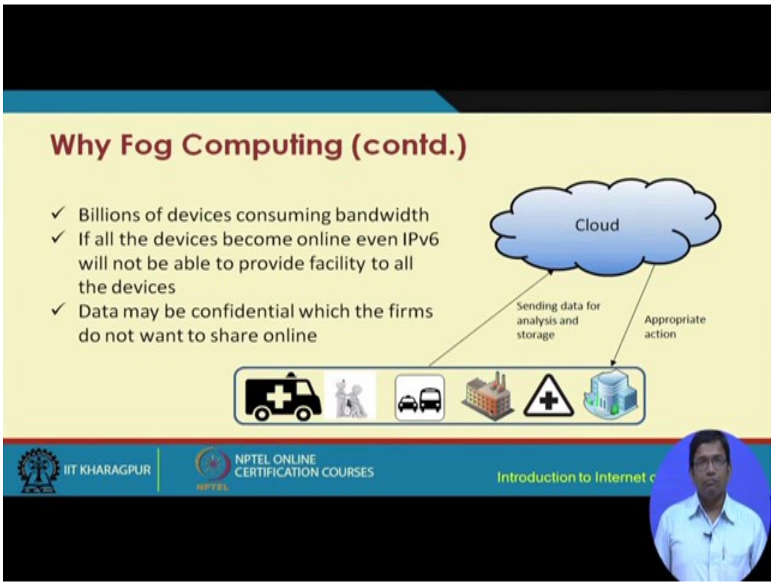
(Refer Slide Time: 16:45)



So, in terms of the bandwidth, the bit rate of the data; sorry in terms of the bandwidth, bandwidth is calculated as the bit rate of data during transmission. So, if all the data are generated by IoT devices and those data that are generated by these devices are sent to the cloud for storage and analysis, then the traffic generated by these devices will be simply gigantic.

So, these IoT devices are going to consume almost all the bandwidth because of this and handling this kind of traffic will be simply a very hard task.

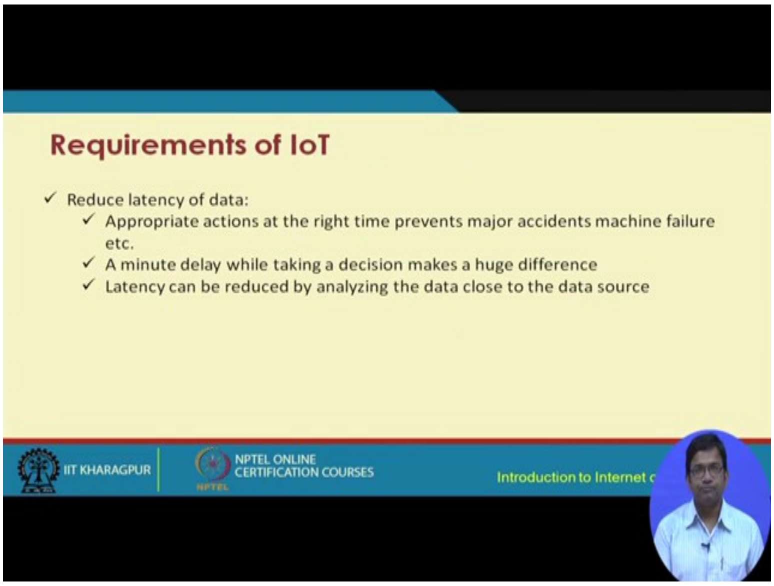
(Refer Slide Time: 17:27)



So, billions of devices consuming bandwidth if all the devices become online even IPv6 or IP based technologies will not be able to handle the facility to provide the facility to all the devices and the data may be confidential which the firms do not want to share online. So, these are the different problems. One is the privacy of the data. This is of concern to the firms and the second is that you know dealing with these kinds of problems with IP based technologies like IPv6 is a problem and also, the issue of having billions of devices consuming bandwidth.

So, you know; how do we handle them together in a synergistic manner.

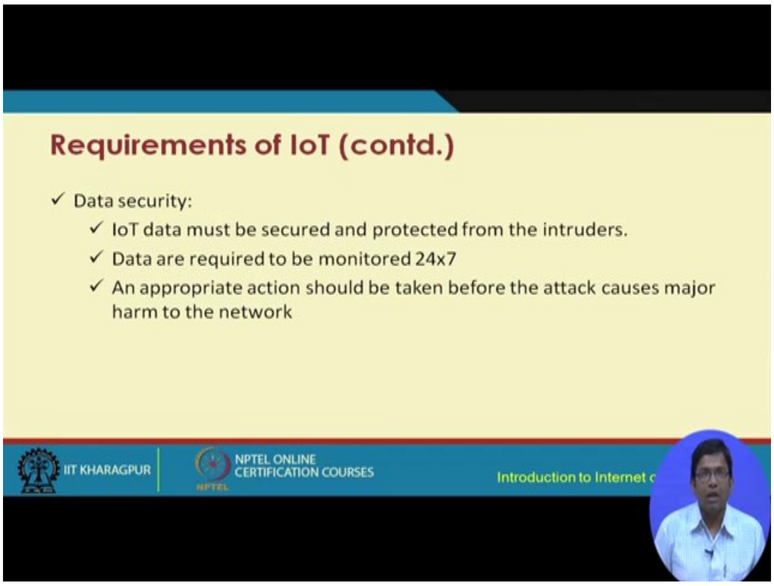
(Refer Slide Time: 18:20)



Reduced latency of data, appropriate action at the right time prevents major accidents, such as machine failure and so on. So, a minute delay while taking an action makes a huge difference and this is what I was explaining to you during the medical emergency scenario. A person might die if you know the decision making takes a lot of time compared to the time for sensing.

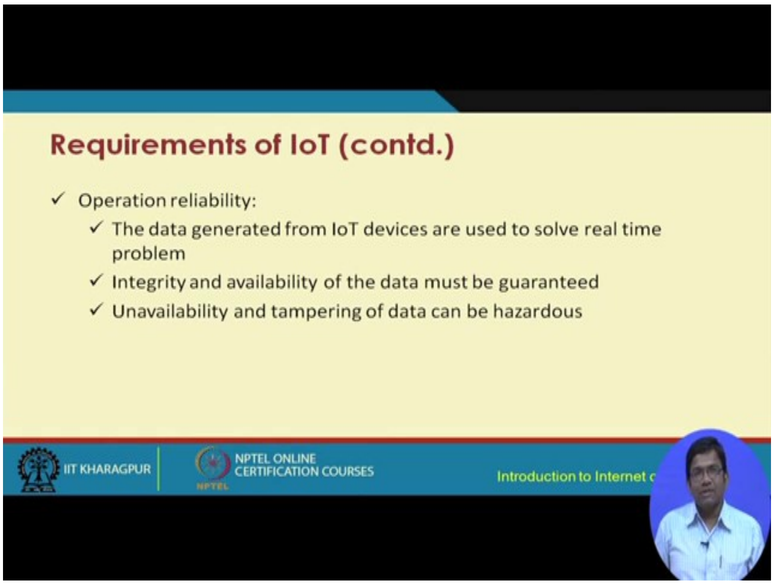
So, it has to be the time for decision making. That means, processing storage etcetera should be conformant with the time for sensing. So, the time it takes for sense is almost after something is sensed. Immediately thereafter it has to be disseminated and corresponding action also has to be taken in real time.

(Refer Slide Time: 19:13)



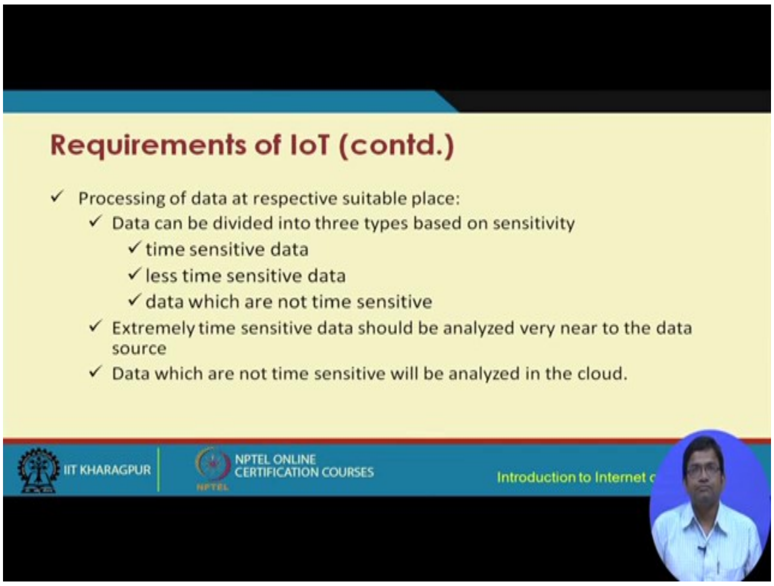
Data security, IOT data must be secured and protected from the intruders. Data is required to be monitored 24 7. An appropriate action should be taken before the attack causes major harm to the network and this is what I was explaining to you.

(Refer Slide Time: 19:26)



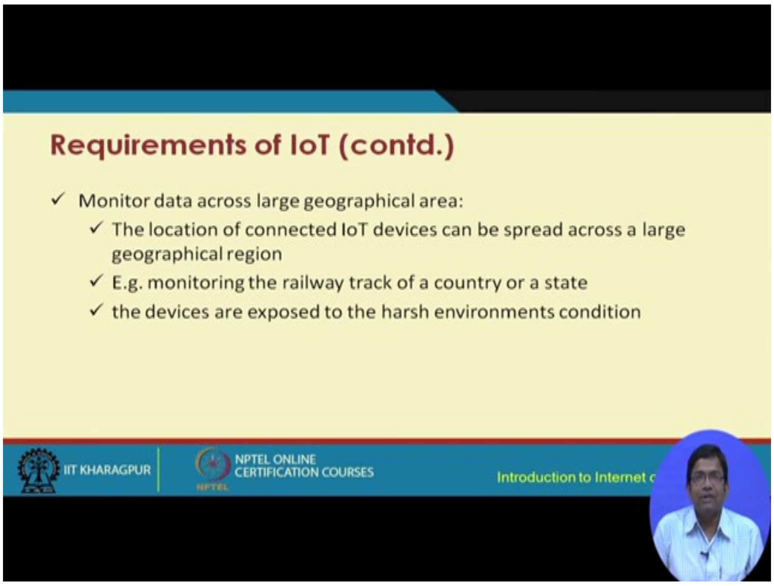
The operationals reliability, the data that is generated from the IOT devices are used to solve real time problems. The problems of integrity and availability of data must be guaranteed and unavailability and tampering of the data can be hazardous.

(Refer Slide Time: 19:45)



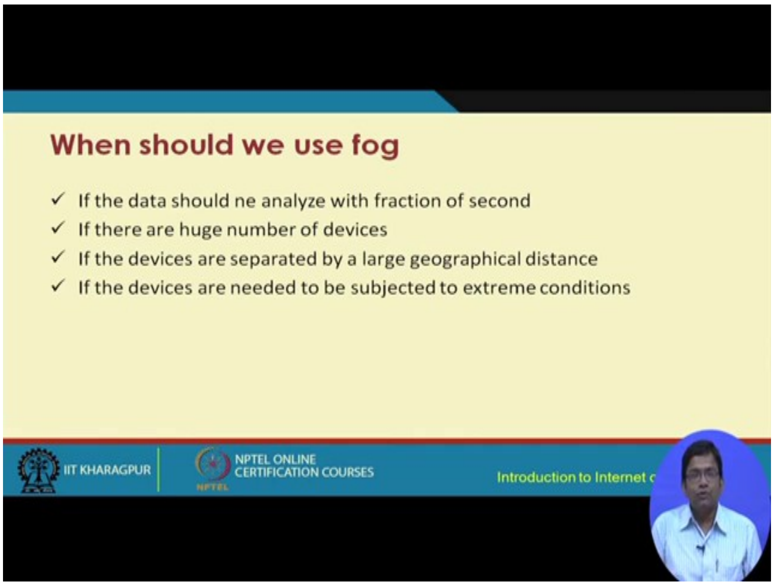
Processing of data at the respective suitable places, data can be divided into three types based on the sensitivity. One is time sensitive data, second is the less time sensitive data, and third is data which are not time sensitive at all. So, this kind of filtering has to happen with respect to the sensitivity of data. So, extremely time sensitive data should be analyzed very near to the data source and data which are not time sensitive will be analyzed in the cloud.

(Refer Slide Time: 20:22)



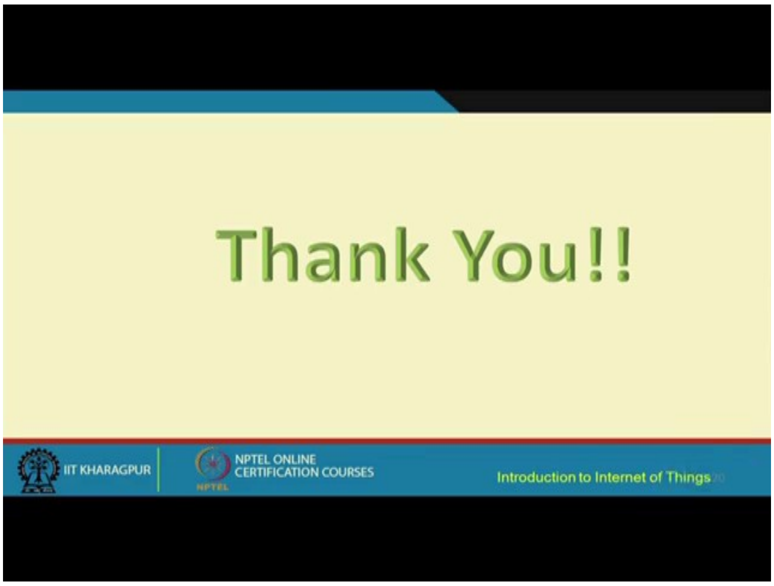
So, time sensitive data closer to the devices, non-time sensitive data send it to the cloud, monitor data across large geographical areas, the location of the connected IoT devices can be spread across a large geographical area. Examples, monitoring the railway track of a country or a state, the devices are exposed to the harsh environmental conditions additionally as well.

(Refer Slide Time: 20:48)



So, when should we use fog? If the data should be analyzed within a fraction a minute, fraction of a second, if there is huge number of devices in the network, if the devices are separated by large geographical distance or if the devices are needed to be subjected to extreme conditions.

(Refer Slide Time: 21:13)



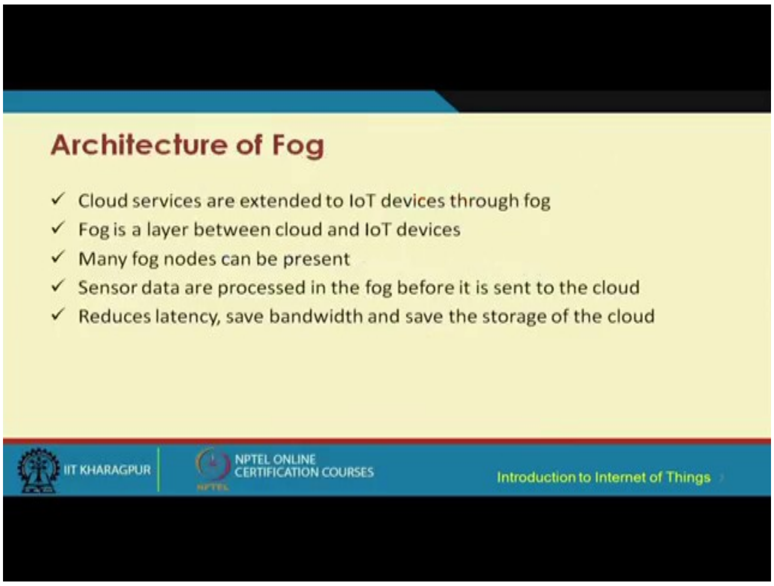
So, with this we come to an end of first part of lecture on Fog Computing. In this lecture, we have understood what fog is, the genesis of fog computing and also, about how fog computing can help in building internet of things systems. We have also in the process gone through some limitations of the use of IoT.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 45
Fog Computing – II

So, now in this lecture, we are going to discuss in further detail about fog computing architecture. So, in the previous introductory lecture on fog computing, we have already seen the basics of fog the whole premise under which fog operates and also the advantages of using fog computing. So, that we have already seen the advantages of using fog computing over the traditional cloud computing and we have also seen that in IoT, it is essential to have a fog platform in addition to the cloud platform. So, I should remain you over here that it is not like a substitute; it is not like fog is a substitute of cloud so that we should not think that way. So, fog is something which is complementary it complements the cloud technology. So, we need both fog and cloud along with the IoT devices and the architecture along with the IoT architecture.

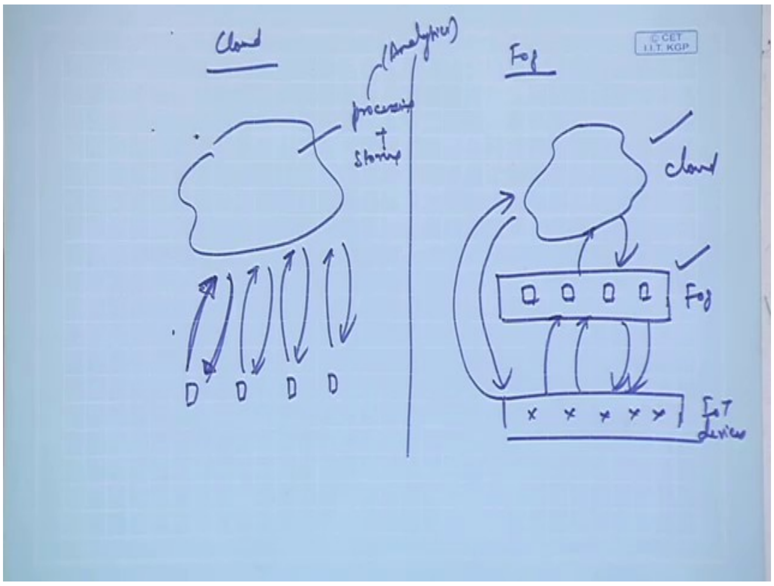
(Refer Slide Time: 01:48)



So, this is what we need. So, we need IoT devices the protocols the architectures plus fog plus cloud to have a complete platform for proper use. So, let us go through the details further. So, when we talk about the architecture of fog we have to keep in mind that the cloud services are extended to IoT services, IoT devices through fog. So, this is what is happening. So, what is so essentially I should explain this thing in a little bit different way? So, essentially earlier what was happening is we have the cloud and we have the IoT devices; IoT devices sending the data to the cloud and then getting a response back or getting getting the data back from the cloud if it is required for further actuation of whatever details. So, this is the traditional way of dealing with IoT devices with only cloud.

Now, what we are saying over here is we need to have some capabilities of cloud being implemented closer to the IoT devices layer.

(Refer Slide Time: 02:58)



So, we want essentially something like this. So, traditionally we had cloud and now we are talking about fog architecture in the cloud architecture we have these different IoT devices and data being sent and response received either response or even the data can be fetched. So, this could represent even the data being fetched and. So, on and so forth, right and here the cloud would take care of processing of the data plus storing of the data. So, processing could even include things like running different analytics right.

So, this is the traditional model now the problem over here is that you know one very important problem is that the problem of latency; that means, that it takes. So, much of time for the data that is sensed by this IoT device to be uploaded to cloud doing some processing over there and then getting the response back. So, the overall over basically this delays the whole process. So, in fog actually what we are saying is we still will have the cloud we will have the fog layer here.

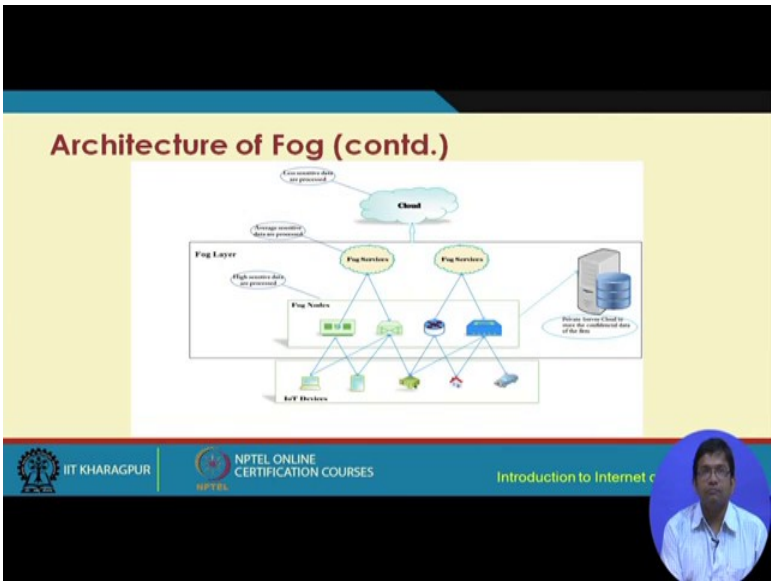
So, this is cloud, this is fog very closer to this devices the IoT devices some are going to happen here and some of the processing and computation and getting some responses in the form of let us say triggers or actuation signals those would be sent to the cloud directly and some would be like in between in between means that like in some case we need to have computations only in that fog in some case you know some basic processing will be done in the fog and the rest would be sent to the cloud and in some case we can send directly to the cloud without having the intermediate fog.

So, we have 2 different comparable architectures of IoT one using cloud the other using fog and the essence is that in fog we are not saying that we will get rid of cloud this is you know we still have to go through a go by using cloud, but in addition we are going to introduce a fog layer. This fog layer is going to have something known as the fog nodes we are going to talk about these fog nodes shortly and here we are going to have these IoT devices. So, this is the whole crux of fog computing and the next few slides we are going to discuss in different ways the different aspects of fog.

So, essentially what we are doing is we are trying to bring the cloud surfaces in the form of processing storage closer to the IoT devices layer through the introduction of fog. So, as I said fog is a layer which is between the cloud and the IoT devices where many fog nodes may be present and the sensor data are processed in the fog before it is sent to the cloud and as I was telling you before that only those data where the data are time sensitive those would be processed in the fog there could be some other data which are not time sensitive. So, those would be better processed in the cloud itself.

So, what we have basically is some kind of complementarity along with cloud by introduction of fog. So, what is the advantage number one reduction in latency, so the overall latency from the point the sensing is done till the point processing and storage and further response back is received at the source. So, that latency is reduced can be reduced significantly with the introduction of fog the second advantage is that because we are not flooding the entire network with all these different sensed packets we are sharing bandwidth and also we are saving storage at the cloud because not everything is sent to the cloud.

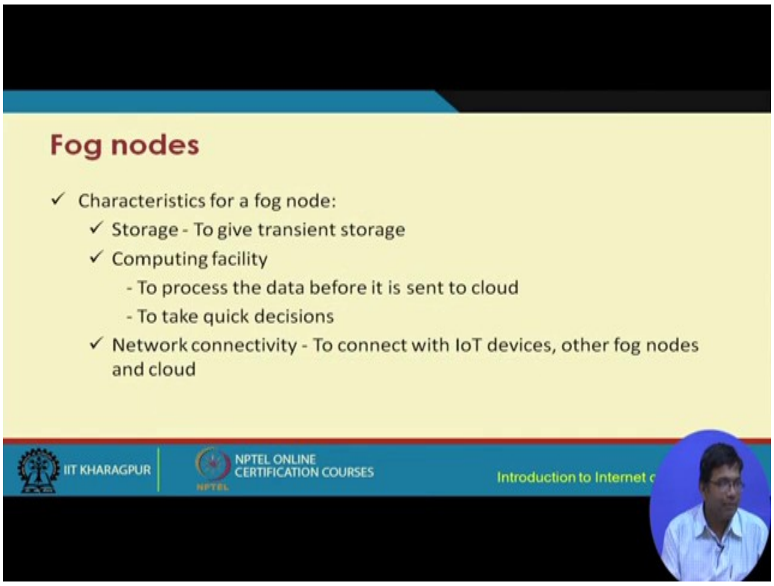
(Refer Slide Time: 07:44)



So, let us look at this figure; we have already gone through it from a different perspective in a different way. So, let us go through it. So, we have at the very bottom these IoT devices which are basically sort of like the physical layer of any network. We have these physical IoT devices over here then we have this fog layer this is the fog layer and then we have the cloud. So, IoT devices layer fog layer and the cloud this fog layer has these fog nodes which are sort of like virtual instances of the IoT devices these virtual instances are going to do are going to have better or improved processing capability improved storage capabilities and so on.

The fog layer I should mention over here has some transient storage capabilities transient storage. So, not like permanent storage. So, transient storage capabilities and permanent storage if required would be you know that kind of data would be sent to the cloud eventually. So, I should also mention over here another component that is very much important. So, the data that is fetched over here can we fetched from a private server or a cloud or the data can be basically pushed into these devices or this platform, the cloud platform the private cloud platform to store the confidential data of the farm former any organization which is basically adapting this technology.

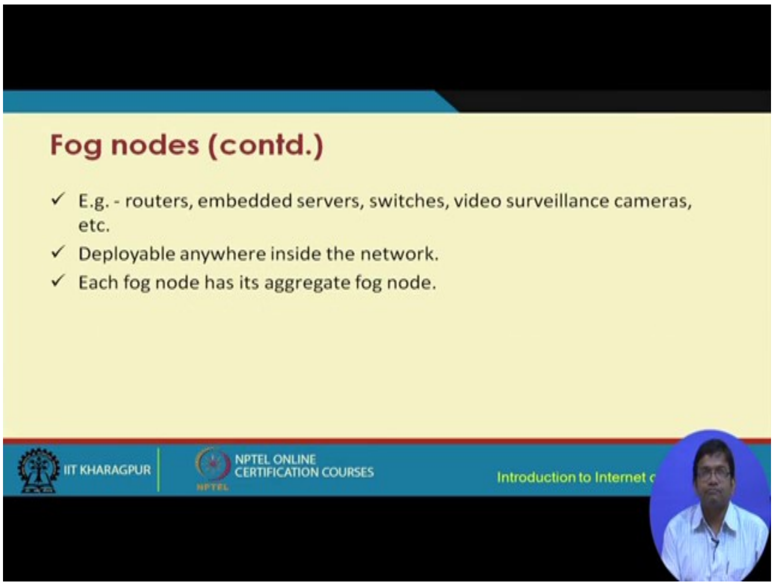
(Refer Slide Time: 09:35)



Now, the fog node that I just mentioned in the architecture in the previous slide has certain specific characteristics number one is storage. So, the storage over here is transient not permanent unlike in the case of cloud number 2 is the computing facility so which is about processing the data before it is sent to the cloud and that basically helps in reducing the time for taking decisions not taking decisions, but time for executing the decisions. So, quicker decision making and execution of the decisions because the processing is done close to the close to the IoT devices; that means, to the edge and that is why this reduction is going to happen compare to the traditional cloud.

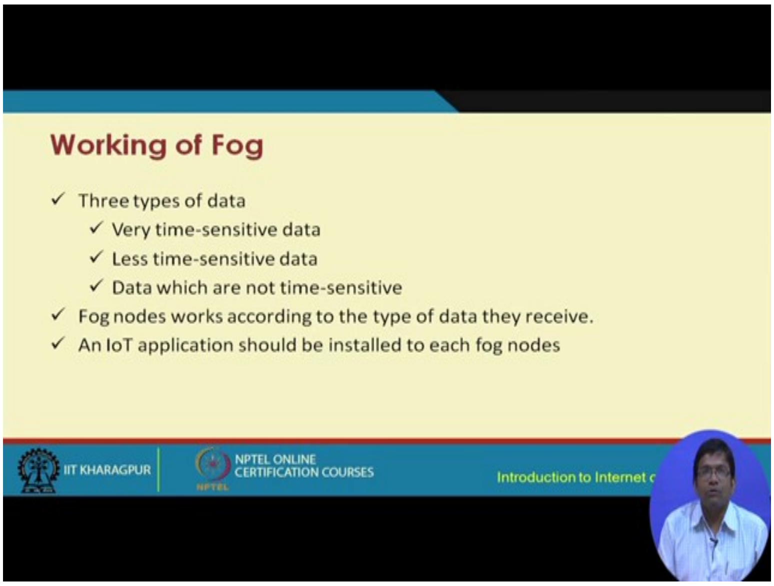
Network connectivity is another characteristic of the fog node where the IoT devices basically connect with each other and other fog nodes and cloud the IoT devices in the IoT devices layer they also connect by other fog nodes and the cloud. So, they can either connect directly or by other fog nodes or by other cloud.

(Refer Slide Time: 11:11)



These fogs nodes could be instances of routers, embedded servers, switches, video surveillance cameras, etcetera, which are deployable anywhere inside the network and each fog node has its own aggregate fog node. So, this aggregate fog node concept; I will explain to you shortly.

(Refer Slide Time: 11:32)

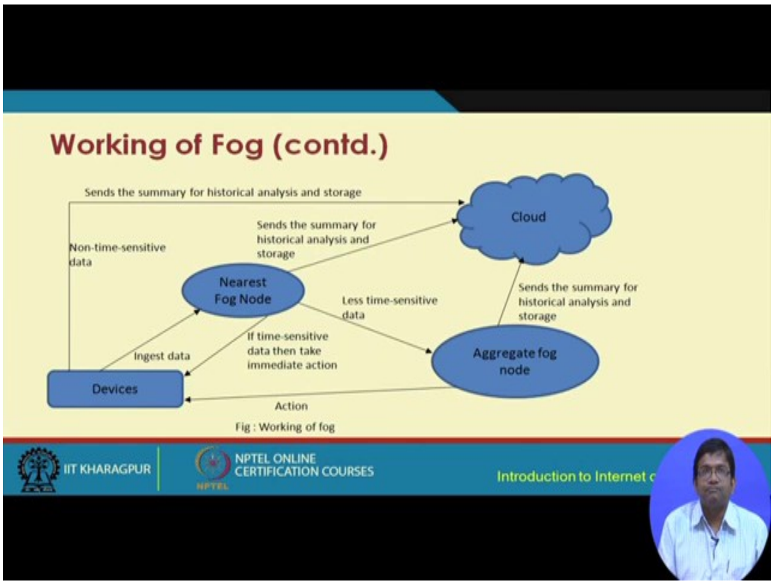


So, there are three types of data in any IoT application some data are very much time sensitive. So, we cannot really hold on to the data for too long. So, it has to be processed immediately and so on. So, for example, surveillance using cameras you know. So, it does not make sense, if we are acquiring the data and after three four seconds or maybe you know after several minutes the decision about doing something at the ground is that information is sent to the IoT device maybe some actuation or something is sent to the IoT devices.

So, it is mean surveillance is such an application where basically time is very critical and we cannot delay to long less time sensitive data you know one is very time sensitive data like the surveillance applications less time sensitive data. For example, some non critical health care data is less time sensitive data and data of which are not time sensitive at all like you know the health care data, but which does not concerned the life or death of a patient sorry of a death of a patient not life, but death of a patient.

So, that kind of data is not time sensitive. So, fog nodes is work according to the type of data they that they receive and the IoT application should be installed in each fog node to handle this various types of data.

(Refer Slide Time: 13:21)

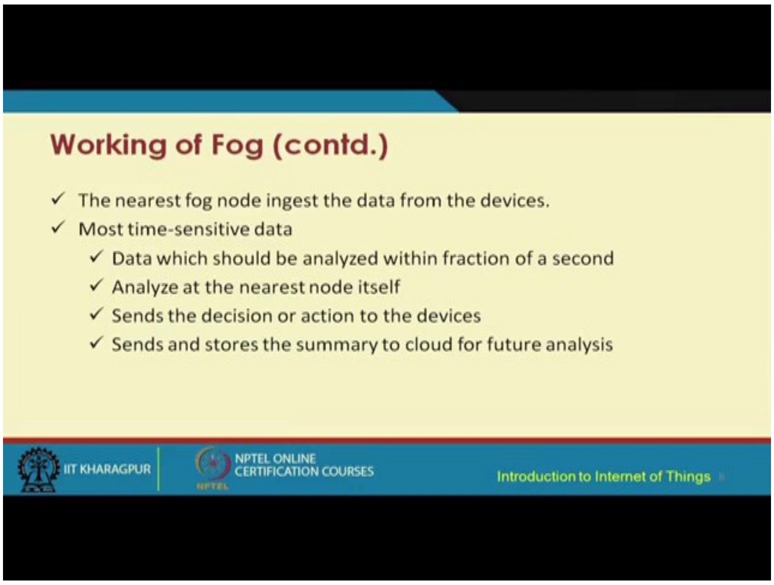


So, let us look at this particular diagram we have this IoT devices and these devices basically sent the data the data are ingested at the nearest fog node if it is time sensitive then some immediate action will be taken by the fog node and that result is going to be communicated to the IoT device the it sends the summary of the historical analysis and storage which are not very time sensitive to the cloud for longer term storage and processing.

Now, if it is a non time sensitive data then these devices send the summary for historical analysis and storage to the cloud because it is not time sensitive now in the previous scenario if the data is relative less time sensitive then it is aggregated at the fog node and that aggregated data is sent as summary for historical analysis and storage to the cloud and some action is performed on the IoT devices in the devices layer.

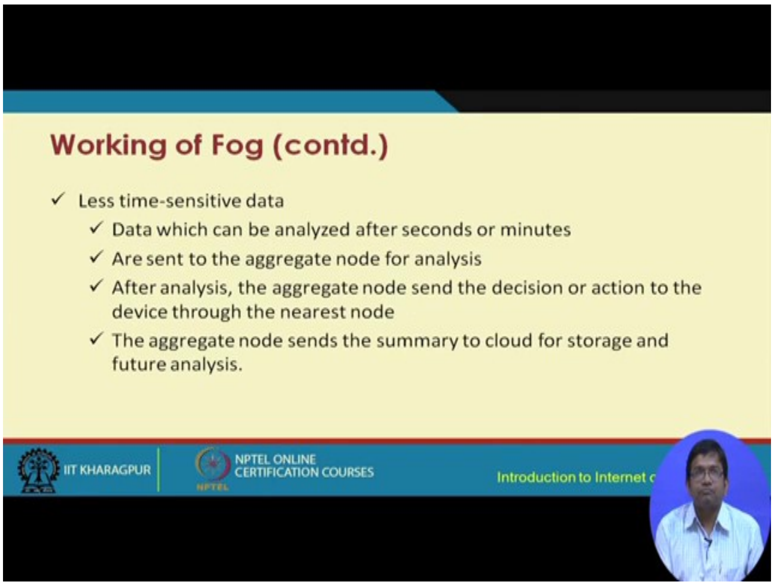
So, this is the whole idea behind fog. So, remember one thing that when we are talking about fog we are typically talking about low power resource constraint environments like IoT environments IoT environments directly with cloud not a good very not a very good solution as such. So, we need faster processing faster reactivity and so on. So, that is the reason we need some processing some storage capabilities at the age; that means, closer to the IoT devices. So, that is where fog comes as a benefit to this IoT technology.

(Refer Slide Time: 15:36)



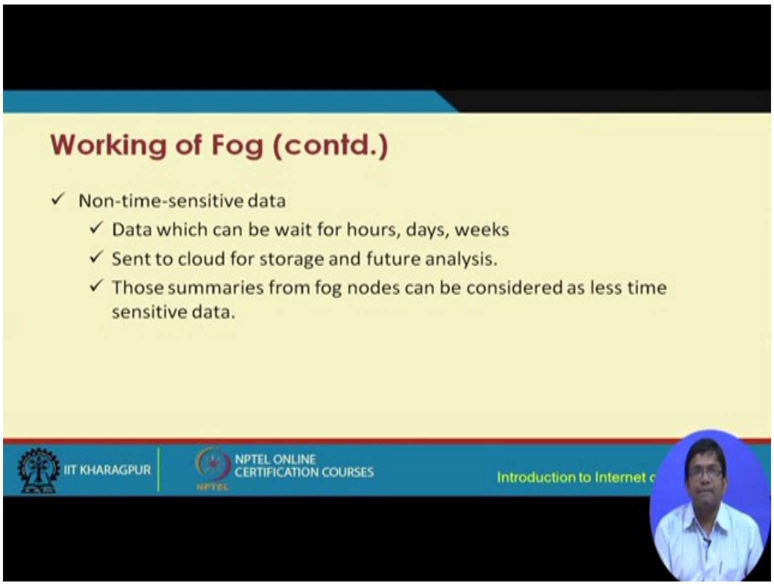
So, the nearest fog node basically ingests the data from the devices and the most time sensitive data are the data which should be analyzed within like fractions of a second and the analysis should be done nearest to the node itself and the decision about what has to be done after the analysis or the action that has to be taken based on the analysis is sent to the IoT devices like an actuator or something and a copy of it is sent and stored at the cloud for longer term storage and analysis for less time sensitive data the data of which can.

(Refer Slide Time: 16:20)



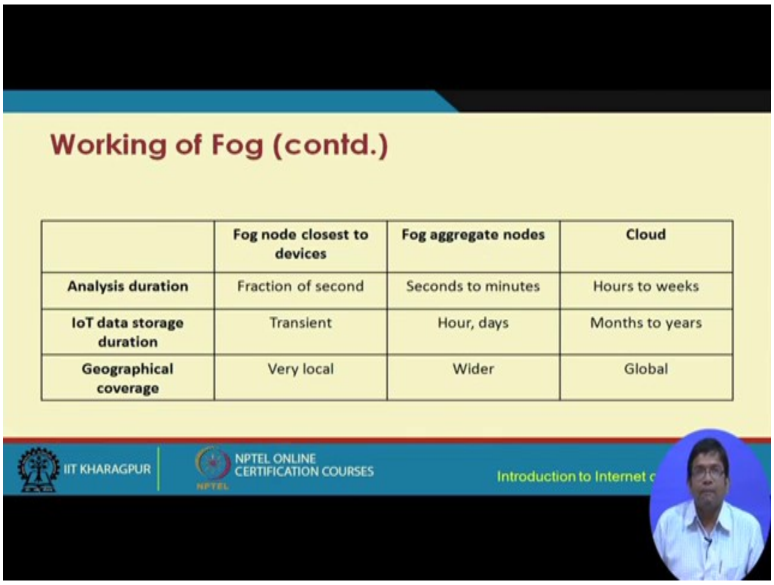
The less time sensitive data are the data which can be analyzed after seconds or minutes and they are send to the aggregate node the aggregate fog node for the analysis after analysis the aggregate node sends the decision or action to the device through the nearest node and the aggregate node sends.

(Refer Slide Time: 16:48)



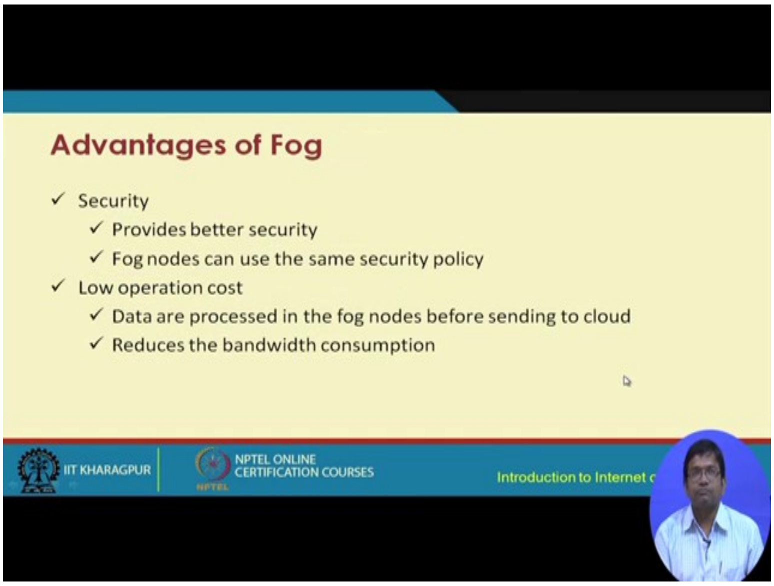
There is summary to cloud for storage and future analysis for non sense non time sensitive data which are basically data of which can wait for hours days weeks and. So, on these kind of data are sent directly to the cloud for storage and longer term analysis future analysis and the summaries from the fog nodes can be considered as less time sensitive data or even some kind of data from the fog nodes from the IoT devices can also be directly stored in the cloud and those are the ones where time is not an issue at all.

(Refer Slide Time: 17:25)



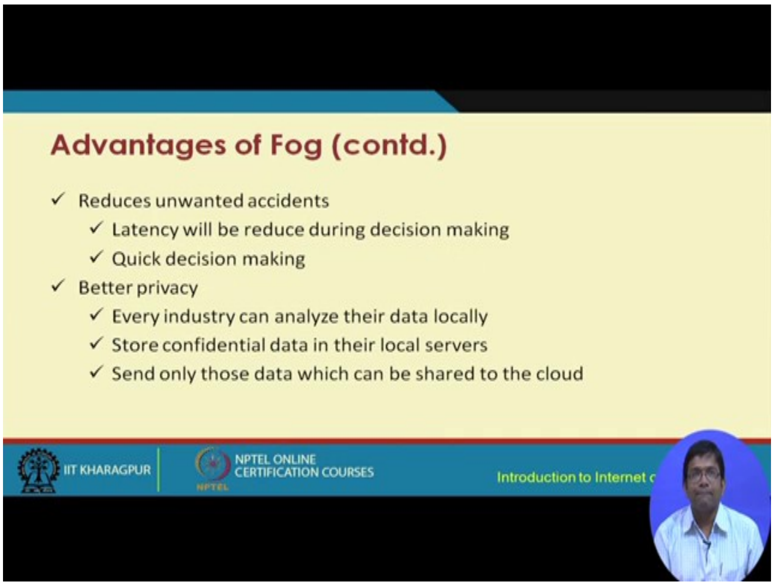
So, this is the summary of what action has to be taken at the fog node. So, analysis duration fraction of a second fog node closest to the devices does it seconds to minutes analysis duration the fog aggregate node does it and hours to weeks the cloud does IoT data storage duration is you know in the fog node this storage is transient it is in the order of hours or days for the aggregate nodes and months to years in the cloud for geographical coverage in a fog node what are closest to the devices the coverage is very local it is wider covered for the aggregate node the fog aggregate node and it is global for the cloud.

(Refer Slide Time: 18:27)



Advantages of fog security improved security faster processing low operation cost data are processed in the fog nodes before sending to the cloud. So, that way the bandwidth is also reduced bandwidth consumption is reduced and further the other important the most important I would think is that faster response time quickly the actions that are determine through the analysis can be executed in this kind of model that way the unwanted accidents.

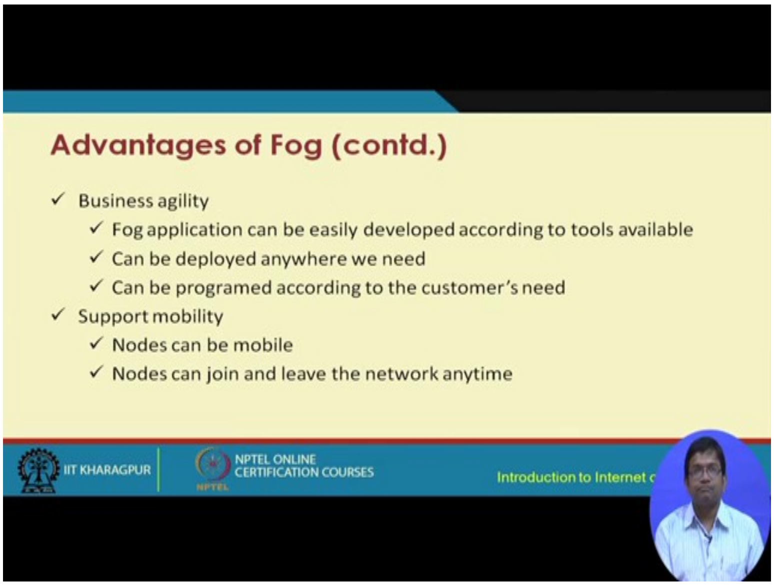
(Refer Slide Time: 19:02)



That are going to happen may be you know if the IoT devices are implemented in some safety critical platforms like you know industry; so, where there is industrial safety a prime concern.

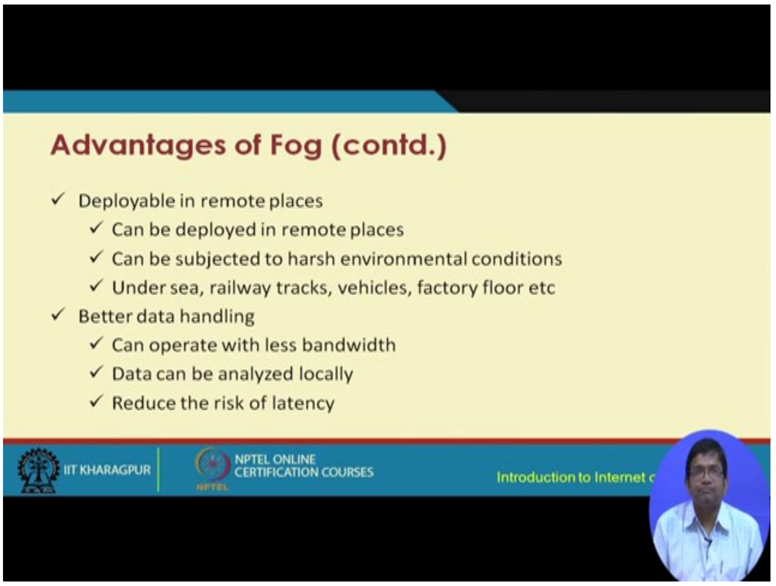
So, in such case such a case it is required to process fast you now we cannot wait until it is sent to the distant cloud for processing storage etcetera, etcetera, we have to do it close to the point of sensing and that is where you know if you do that the processing time reduces quite significantly the decision making is becomes very fast and the unwanted accidents can be reduced in this particular using such a such an approach privacy every industry can analyze their own data locally and the confidential data in this fog approach can be stored locally in the local servers and only those data which can be shared with others which are not very confidential they can be sent to the cloud business agility also improves.

(Refer Slide Time: 20:19)



So, you know faster we can accept the customer's needs and those can be programmed very fast into the network and that way the costumers satisfaction can be improved supporting nobility here in this fog model the nodes can be mobile and the nodes can join and leave the network at any time a true feature of any pervasive computing system any ubiquitous mobile ubiquitous system.

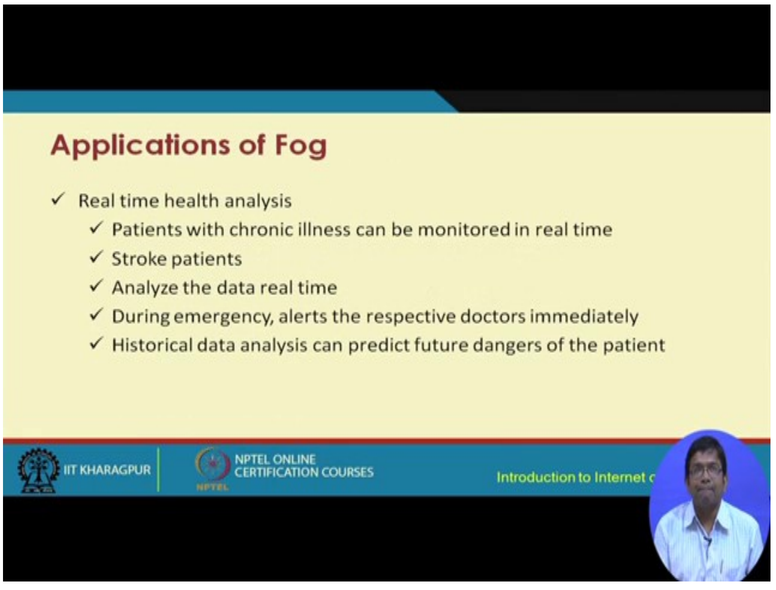
(Refer Slide Time: 20:57)



This solution the fog platforms can be deployed in a remote places and they can be subjected to harsh environmental conditions because typically this is what happens like environmental monitoring open environment you know different types of harsh environmental conditions snow fall rain fall hill storm etcetera, etcetera.

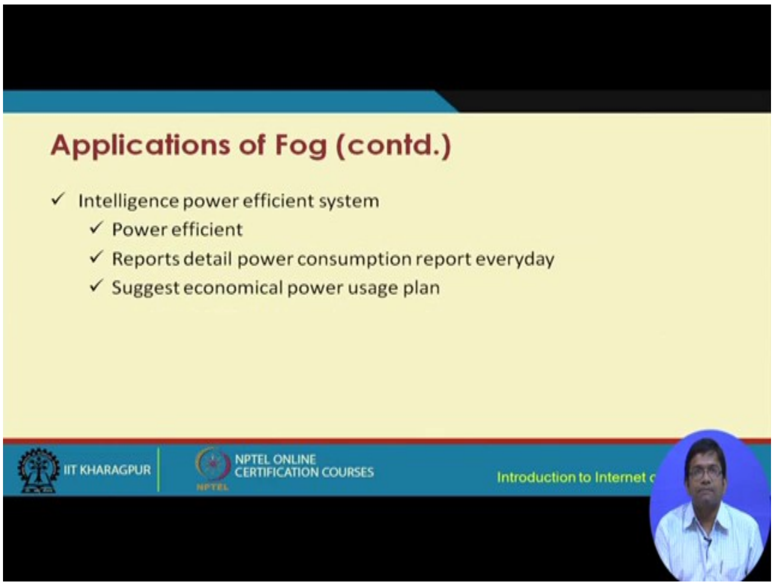
So, the devices the fog technology as a whole will have to go through this kind of you know harsh environmental condition better data handling because you know less bandwidth will be consumed for handling the data can be analyzed locally.

(Refer Slide Time: 21:43)



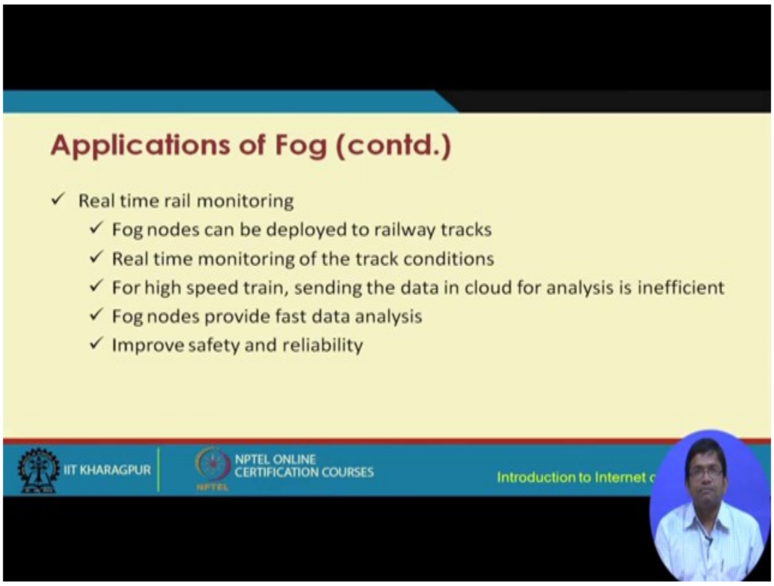
And that would reduce the risk of latency in terms of the applications of fog we can perform real time health analytics using fog technology where the patients with chronic illness can be monitored in real time patients you know undergoing stroke you know are any kind of medical emergency you know. So, this particular technology is basically good for use in such kind of situations.

(Refer Slide Time: 22:09)

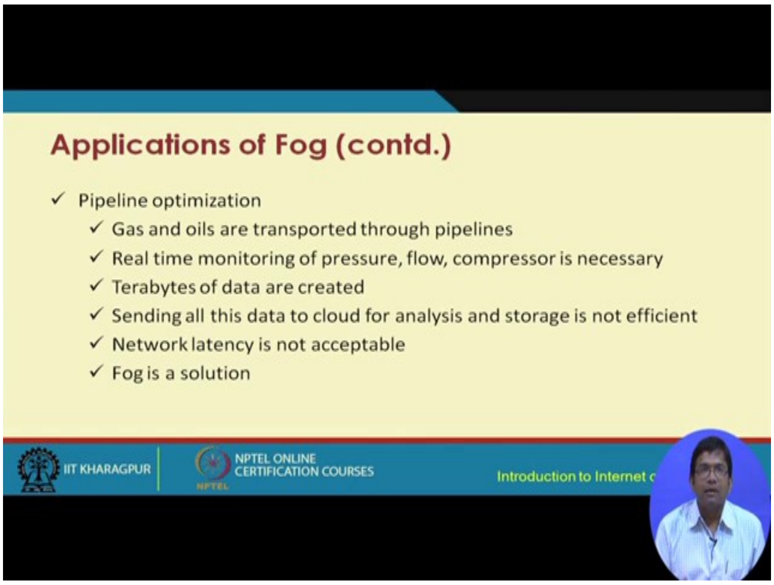


Intelligent powers intelligence power efficiency intelligence and power efficiency. So, fog is power efficient as we have seen before it reports the detailed power consumption report every day and suggest economical power usage plan a real time real monitoring is another application where the railway tracks in real time can be monitored on a day to day basis in an efficient manner. So, that is going to improve the overall safety and reliability of railway systems pipeline optimization.

(Refer Slide Time: 22:29)



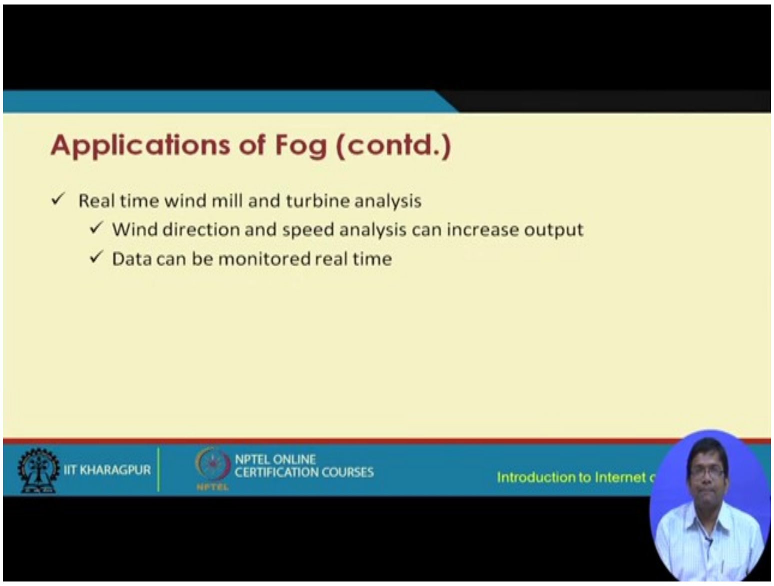
(Refer Slide Time: 22:51)



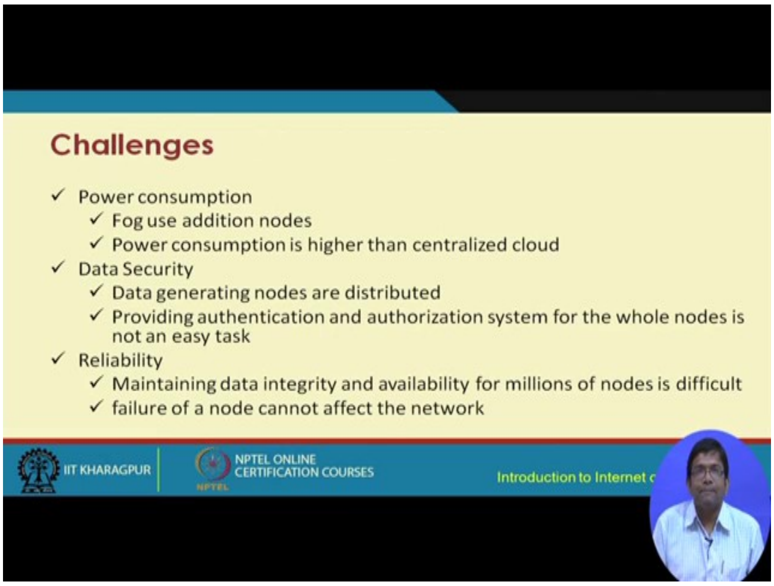
So, you know gas lines oil transportation lines are pretty common. So, real time monitoring of the pressure the flow the compressor you know compressor is necessary in such kind of gas pipeline systems.

So, Tera bytes of data are created and sending all these data to the cloud for analysis and storage is not sufficient and fog becomes a solution in such a scenario because latency to high latency is not very too much of high latency is not very acceptable in such cases because there could be pipe leakages gas leakages and so on and that is not a very good thing to happen real time wind mill and turbine analysis wind direction.

(Refer Slide Time: 23:34)



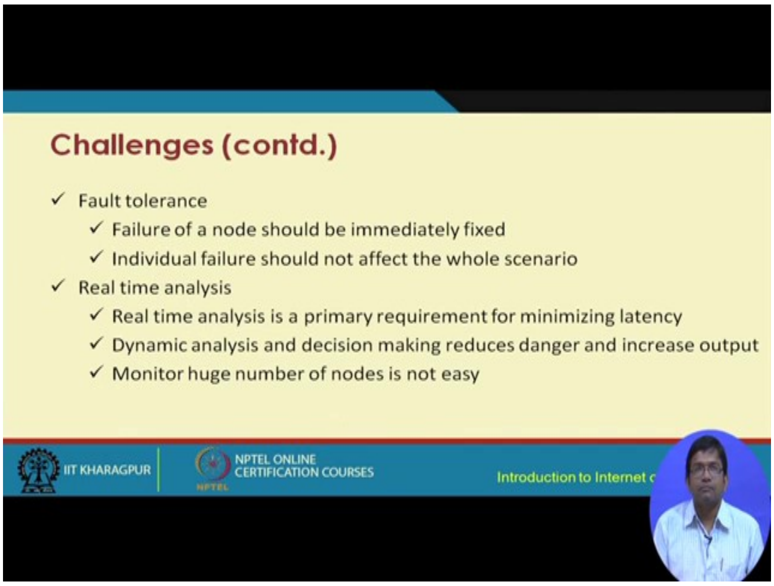
(Refer Slide Time: 23:44)



And speed analysis can increase the output data can be monitored in real time different challenges with respect to handling or consumption. So, additional nodes are used power consumption is higher than the centralized cloud and these are low power devices we are talking about and everything is done at the cloud. So, that is the reason why power consumption has to be taken care of you know as a challenge in this kind of environment.

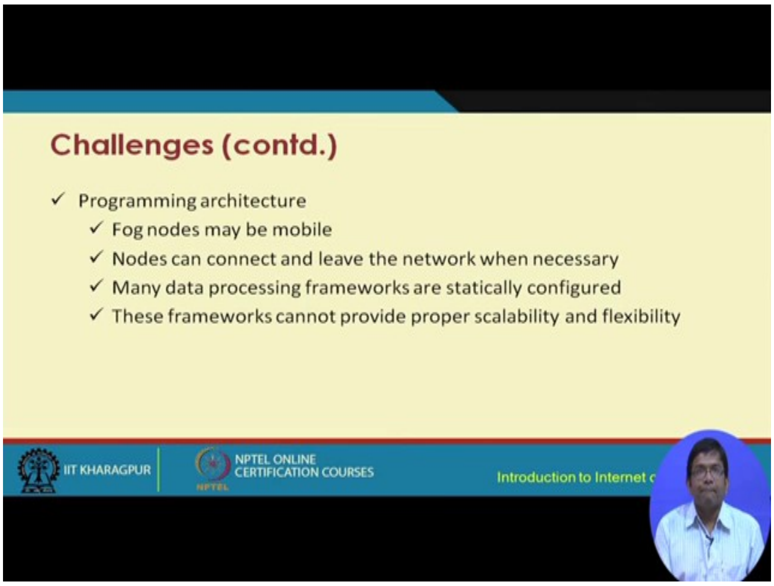
Data security; so, handling data security is a crucial challenge in fog platforms the data that are generated are distributed. So, it provides authentication and authorization system for the whole nodes and that has to be done for fog platforms which is not a very easy task in terms of reliability maintaining data integrity and availability for millions of nodes is difficult and the failure of a node cannot affect the network fault tolerance.

(Refer Slide Time: 24:50)



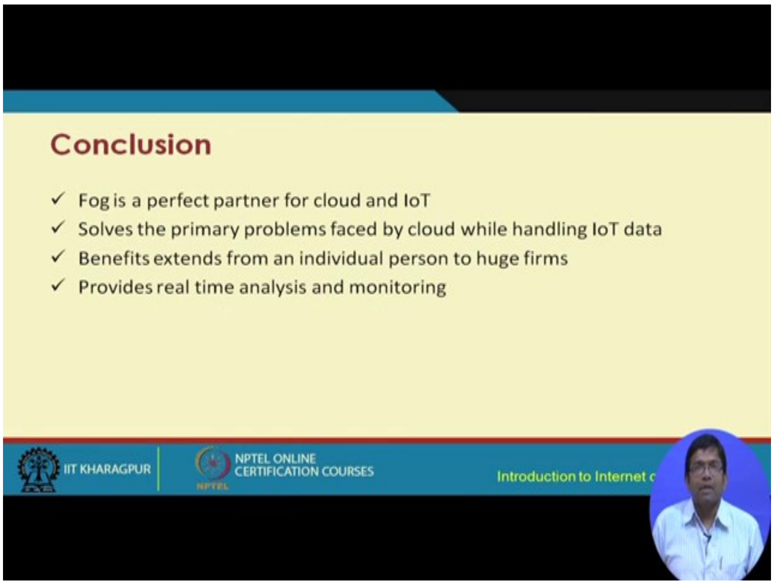
So, if there is some fault with a particular node and that should be immediately fixed and this fixation should happen ideally in an autonomous fashion. So, there should be autonomous fault tolerance fault detection also fault detection and tolerance and real time analysis real time analysis is a primary requirement for minimizing latency dynamic analysis and decision making reduces the danger and increases the through put.

(Refer Slide Time: 25:26)



In terms of the programming architecture fog nodes may be mobile nodes can connect and leave the network whenever necessary and many data processing frameworks are statistically configured these frameworks cannot provide proper scalability.

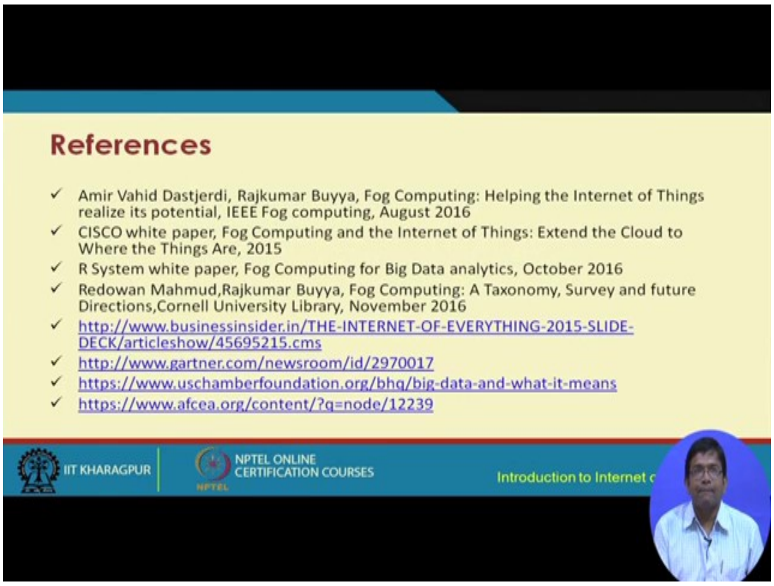
(Refer Slide Time: 25:42)



And flexibility in conclusion fog is a perfect partner for cloud and IoT. It can sit in between IoT and cloud to help IoT in the different functions that it has to perform it solves the primary problem that is faced by cloud with handling IoT data; it reduces it reduces the latency overall and that is one of the I would say that it is one of the most important benefits of the use of the fog technology.

The third is it benefits the benefits extends from an individual person to huge farms and. So, basically you know. So, this is a scalable architecture. So, it is not like only a few people who would be using it. So, the benefits can be extended to huge farms through the use of fog technology and this fog technology basically provides a real time analysis and monitoring.

(Refer Slide Time: 26:43)



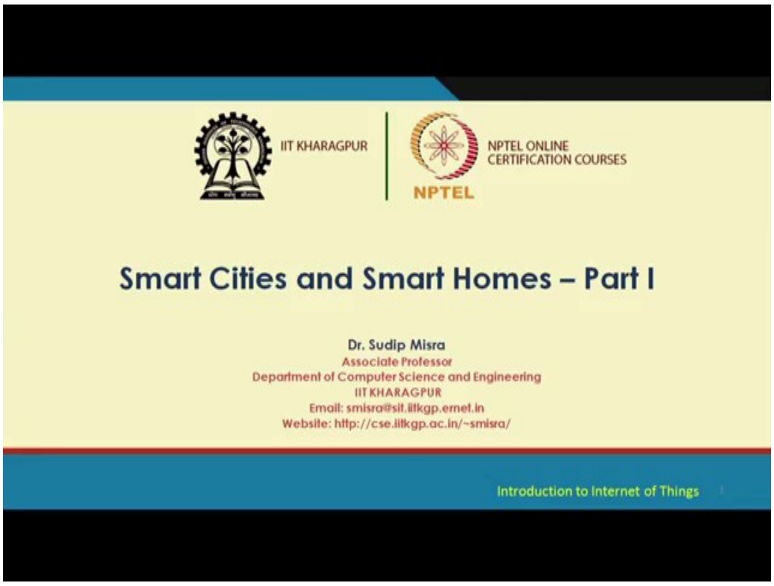
So, these are some of the references for you to go through further and if you are interested to understand fog and some of this contents have been taken from these references and the other references that have been mentioned at the bottom of the slides in the in this particular lecture.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 46
Smart Cities and Smart Homes – I

(Refer Slide Time: 00:25)

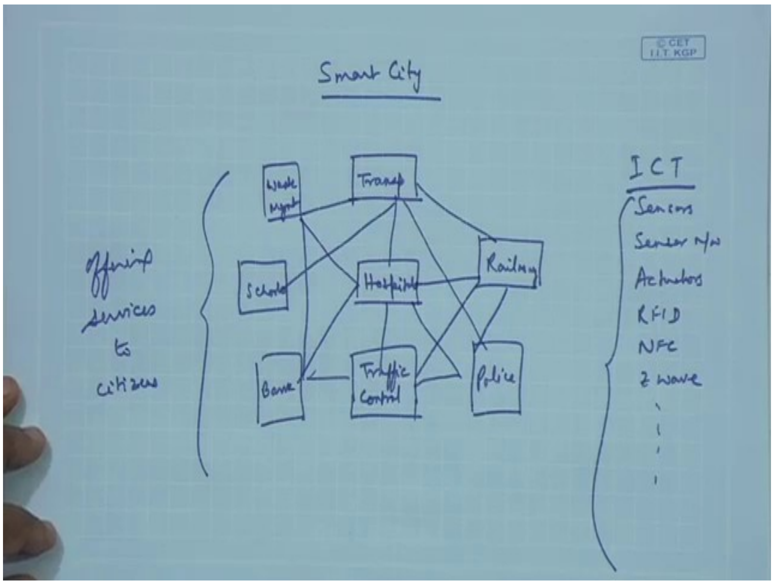


This lecture is on smart cities and smart homes and here we are going to talk about how IoT can help in building the smart cities and smart homes as you know that throughout the world and even in countries like India, there is a lot of focus on building smart cities. Of course, the scope of smart cities in each of these different countries is different and the scope again depends on the priority areas of each of these countries and their government. Now for instance in India, since the last few years, there have been a couple of cities that have been identified and phase wise these cities have been given funds to build or to transform them as smart cities.

So, when we talked about smart cities; what is it. So, in addition to the regular infrastructure that is there in any city for example, the urban infrastructure consisting of office buildings residential areas hospitals schools transportation police and so on you also need something in addition to make the cities smart. So, what is this in addition let us talk about. So, smart means what smart means that it is in terms of the services that are given to the respective stake holders of these cities. So, citizens are able to do things in a better manner in an improved manner then usual and how is that made possible that is made possible with the help of nothing, but the ICT technologies information and communication technologies which also includes electronics embedded electronics different other advanced topologies in electrical in a electrical sciences and so on. So, computers electronics put together can make these cities smart.

So, let me just take an example at the outset.

(Refer Slide Time: 02:59)



So, first of all let us consider any smart city. So, if we are talking about a smart city we need to have the basic components for example, transport there has to be a railways there has to be hospitals there has to be schools there has to be let us say traffic control traffic control waste management waste management banking then.

So, like this these are some of the different things in a smart city right and one thing I have missed which is very much essential is the police. So, as you can see that we have to transform all of these different components of any city to be smart. So, for which the technology is that we have studied. So, far in the previous lectures will have to be taken help of. So, definitely will have to take help of sensors sensor networks sensor networks then actuators then the different other communication technologies RFID, NFC, ZWAVE and so and so forth. So, many different things that we have covered in all these previous lectures of this course on IoT, so, all these will have to be used in order to make this transformation. So, these are the different ICT information and communication technologies that will have to be used right.

So, what is going to happen is in an IoT environment there has to be lot of these interconnectivities that have to be there? So, for you know although I am drawing these lines almost like randomly, but there has to be you know there has to be connectivity between all these different types different blocks and so on for different good reasons and the reason could be like offering different services to citizens. So, services means that in a smart way people would be able to do different things for example, if it is a health care facility.

So, from very easily you know if something goes wrong let us say let us say with the school child in during the school hours very easily the hospital can be contacted not over telephone any longer I mean of course, the telephone connectivity the traditional ones would be there, but in addition you know there would be smart messaging and so on the ambulances would come there would be continuous monitoring over the ambulance of the child who is being transported to the hospital from the school parents would be automatically informed about the status and so on.

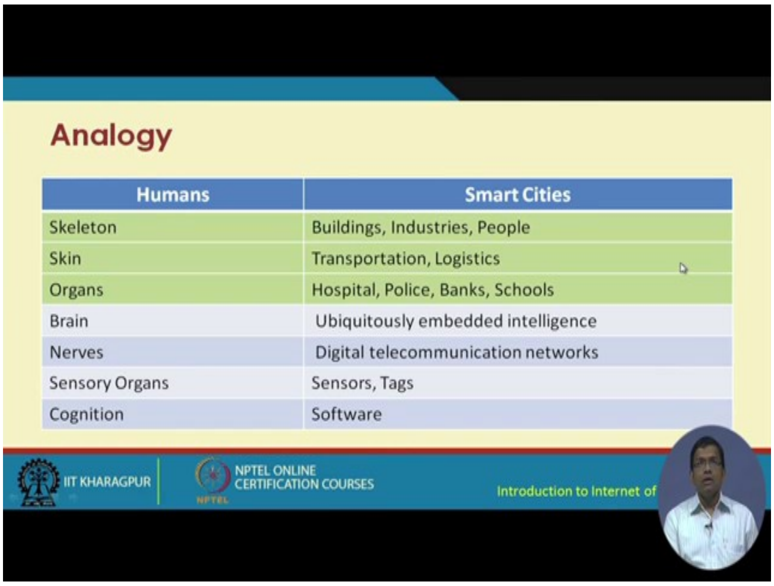
So, many things would be done seamlessly automatically and these are the different services that are going to be offered and normally these services would have to be offered for those or to those who have subscribed for these services only to the subscribers these services would have to be offered. So, whether it is on a paper you know on a on a payment basis or it will be free that depends on the implementation in the smart city, but generally offering different services advance levels of services to different citizens is one of the most important core objectives of the development of smart cities.

(Refer Slide Time: 07:28)

So, let us move ahead and see that what else is there for us. So, as I was telling you before that in a smart city you have an urban system which uses different ICT tools information and communication tools which makes the infrastructure very interactive efficient and accessible in an easier manner then before you know it; it should be you know easily accessible infrastructure and the need for smart cities arose due to different things.

So, first of all the there is an ever growing urban population throughout the world it is not limited to any country, but throughout the world there is an there is a rapidly growing urban population and at the same time the natural resources like coal you know and you know. So, in so many different natural resources that we all use these are depleting at fast rate. So, and at the same time there is change in climate change in environment all throughout.

(Refer Slide Time: 08:47)



So, all these basically necessitate the building of smart cities using advanced ICT tools. So, let us draw some analogy when we talk about a human when we talk about a human humans have the skeleton the skin the organs different types of organs brains nerves sensory organs cognition and so on in the smart city as well in the same way has as a human has a skeleton skin and organs smart cities or rather any city rather any city has buildings industries people transportation logistics hospital police banks schools. So, these are there, but on top of that if there is a human with skeleton skin and organs, but no brains no nerves no sensory organs no cognition. So, you do not have you know life in that human you do not have any life in that human.

So, same analogy can be drawn you know analogously we can say that in a smart city if you do not have embedded intelligence communication networks sensors tags software embedded in these different components and infrastructure of the city the existing cities then it also does not have any life. So, to bring in life to the existing cities having buildings industries transportation police banks etcetera, etcetera you need to embed ICT which includes ubiquity in embedded intelligence digital communication networks sensors actuators tags different software doing different things in a smart way making these different devices to act in a smart way and so on.

(Refer Slide Time: 10:46)

So, these are some of the application focus areas we have smart economy. So, because of the ever increasing competitiveness you need to improve you need to improve your infrastructure the economy to make it smart. So, I will talk about that in more detail shortly now you need to also improve the citizen participation in any good governance in any good governance you need to improve you need to increase the citizen participation and how is that possible you need to take help of the ICT tools.

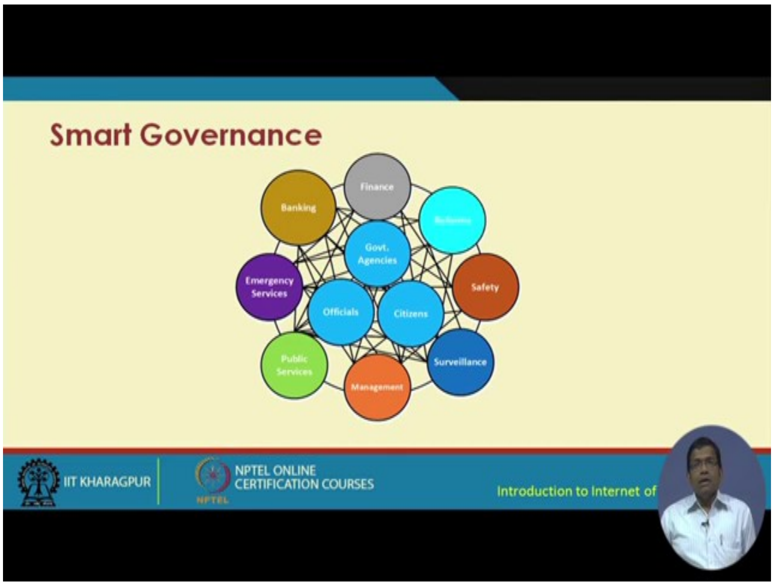
Social and human capital you need to make the social and human capital also smarter by giving them different technologies different tools the ICT tools then smart mobility to improve the transportation with the help of ICT with the help of ICT you know making the transportation smart mobility natural resources. So, smart environment you know. So, basically you know you need to make your environment smart there should be less you know harmful or toxic gas emissions or other sorts of waste disposals you know these would be a reduced and these should be done in a smart without basically effecting the environment that way conserving the natural resources smart living which would improve the overall quality of life of the citizens. So, these are some of the application focus areas of smart city.

(Refer Slide Time: 12:29)

Now, when a when we talk about smart city one of the most important things is smart economy. So, the economy has to be improved over what already exists. So, let us say that in any economy what do you need in addition to the existing economic infrastructure like industry of different types and different other economic domains including even like schools hospitals etcetera, etcetera you also need to improve the economy by including by involving the growth of startups then indigenous Diaspora and different founders of different technologies all of these have to be there and they have to be interconnected they have to be interconnected with different other components for example, a venture capitalist a venture capitalist have to be interconnected with them the international Diaspora along with the indigenous Diaspora then academic academia then public sector buyers worldwide buyers government agencies global MNCs and so on.

So, they all have to be interconnected inter networked together not just at the connectivity level, but. So, that this connectivity has to be there. So, that you know different types of information different types of services are made available to each of these different components in a smart manner. So, they should be able to get these services whenever they need you know whenever there is an useful use case you know from the different components they would be participating in order to improve the quality of fulfillment of the use case.

(Refer Slide Time: 14:24)



Let us talk about governance in governance there is at the core the government bodies the government offices and at the same time the citizens. So, these government agencies citizens and officials government officials these are all core to any governance or any government body now in addition you have all these peripheral ones like banking finance reforms safety surveillance management public services emergency services and so on.

Now, in a you know in a regular city what happens is typically traditionally they all they function sort of in isolation there is some minimal connectivity between them, but these are not a smart connectivity with the help of these ICT tools. So, in smart governance what is going to happen is they all are going to get connected they all are going to get connected. So, let us say that the officials are not only going to get connected to these government agencies and citizens, but also to the public services to the emergency services to the banking to finances you know surveillance citizens you know. So, all these different types of interconnectivities are going to be there. So, you have to make it possible in order to build a smart government system.

(Refer Slide Time: 15:55)

Let us look further ahead and see what is there in for us. So, we have the smart people. So, when we talk about the citizens you know education health care population overall is at the core of the; in of any city. So, and at the same time peripherally we have the transportation the shopping banking connectivity media safety current affairs social networks these are also like peripheral things. So, they all again have to be interconnected. So, that from any component it; it should be made possible to access information from other components of course, there has to some kind of policies of data you know floating across, but generally this has to be made possible. So, that the citizens get the information the citizens get the services from any of these components whenever they need and that has to be again identified in a smart city that has to be that need has to be identified intelligently with the help of cognition with the help of the different software the intelligence that is embedded in to the system.

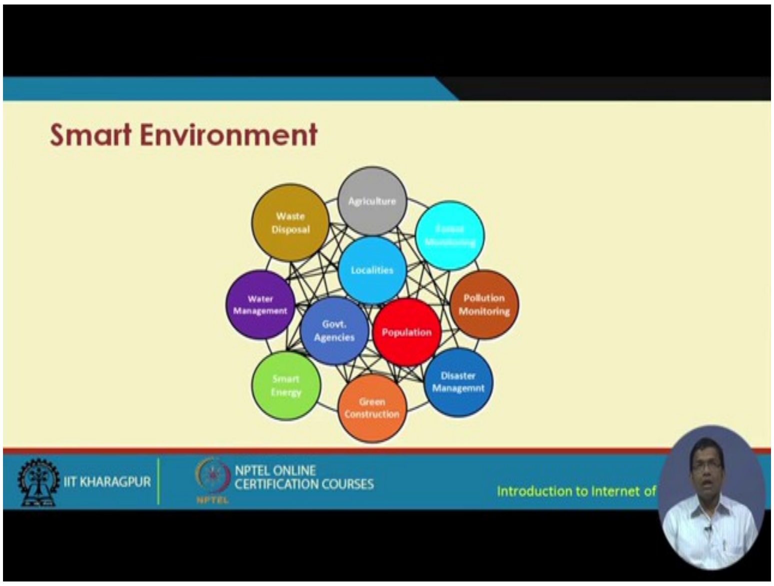
(Refer Slide Time: 17:03)

Smart mobility likewise we already have a addition to the population we have the cities the localities and so on. So, you need to have interconnectivity with the other peripheral components like vehicular networks transportation logistic emergency response railways airways you know electric vehicles and so on. So, these sort of because let me just talk about use case with respect to this. So, let us say that I want to go in a city from point a to point b not just in the city we can even go from one city to another city as well one city to another city.

Now, what should happen is that the information should be made available in such a way I am just giving a simple use case that let us say that I want to book a train from city x to city y or point x in a city to point y in a city and let us say that the road that I am going to take is going to be very much congested or it is going to be very expensive that particular root is going to be very expensive or maybe you know there are you know there are different.

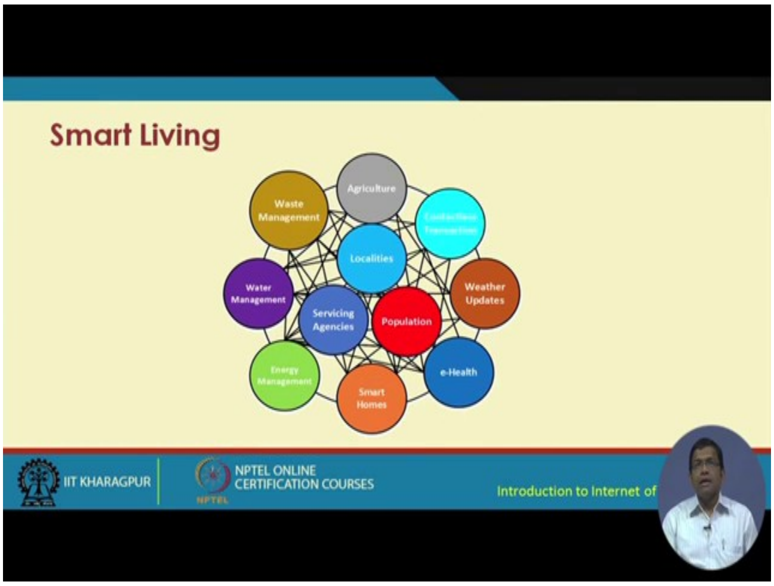
Other reasons for which you can consider the alternative options the alternative options would be that very easily instead of taking a train one could also get other options like taking a bus you know or taking another you know electric vehicle or you know and so on and these again the bus the train etcetera these also have to be connected with the police the police and the emergency vehicles. So, emergency vehicles because for obvious reasons if there is some kind of an accident etcetera, etcetera under that the emergency response team should be able to get information on the fly you know. So, whenever it is required they should be able to get information and then the action also has to initiate with the help of these tools in a smart manner.

(Refer Slide Time: 19:03)



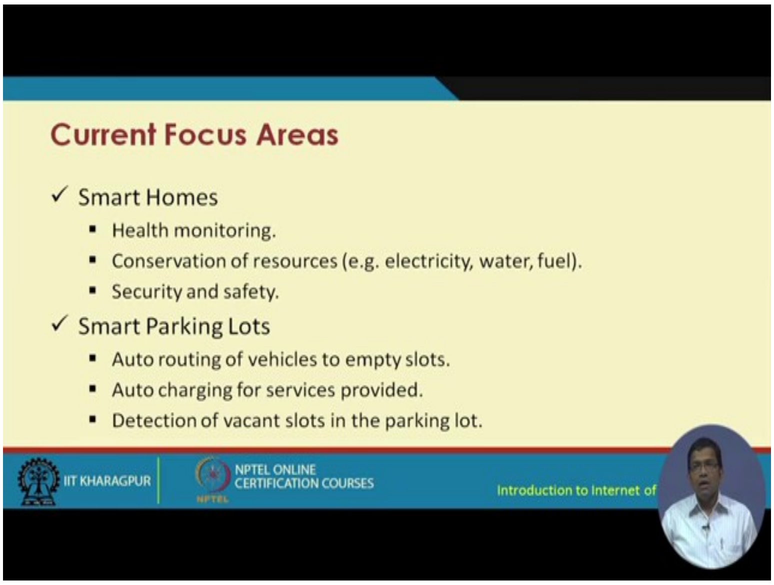
Then the we have the smart environment where in addition to the government agencies localities population there, there are components like waste management waste disposal you know agriculture you know forest monitoring pollution monitoring disaster management green constructions smart energy these all these different components inter internetworked together interconnected.

(Refer Slide Time: 19:24)

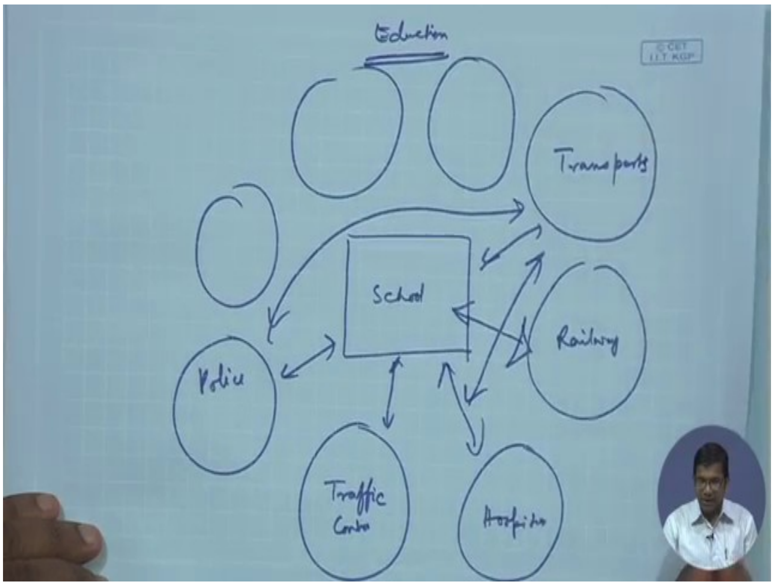


Together in a smart living kind of scenario you we have this we have the localities population serving servicing agencies these interconnected with all these different other peripheral components as you can see in front you in this particular slide.

(Refer Slide Time: 19:39)



(Refer Slide Time: 19:49)



So, let me just give another example before we go further ahead let us consider a smart city where we have a school; we have a school. So, apparently or rather traditionally in a school in any school what you know the school specifically function in isolation the school specifically function in isolation in the sense that you know they do not really have to interact with the other components of a city that much, but in a smart city what is going to happen is we have these other components like transports railways we have the hospitals we have traffic control we have the police we have did I say hospitals; hospitals I have already said like this actually we have different other things in this smart city.

So, you know what is going to happen is if you have this kind of inter connectivity or even between police and transport you know schools and hospitals; hospitals and transport you know railways and this thing and like this then let us say that when a school child from his home he wants to come to a school he has information about the different forms of transport that he can take and let us say in an un event in an you know in a in an emergency in the road while going there is some kind of accident or whatever then correspondingly the police has to be informed and also the traffic control also has to take over and also the hospitals have to be informed.

So, that the child can get health facilities on the road and the same thing can happen inside the school as well once this once the child is inside the school the same thing can happen. So, as you can understand now. So, this was from the education sector school education sector like this actually there are different other reasons why smart cities have become very popular.

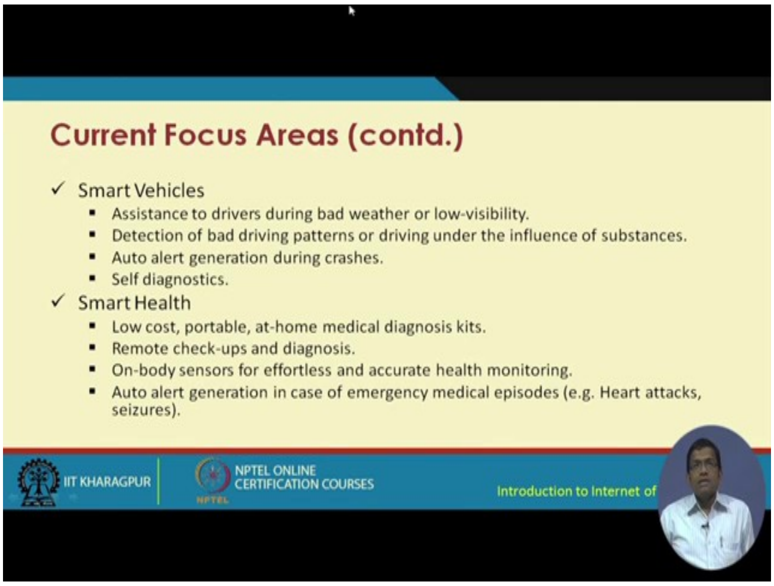
Now, we have the different focus areas we have smart homes smart parking lots in a smart home situation we need to have I will talk about smart homes in more detail later on, but in a smart home situation we have the health monitoring done in a smart way at home this you know the medical data made available to the doctors whenever there is a health criticality the corresponding house physician would be informed the physician can take requisite action based on the severity of severity or criticality of the of the health of the patient.

So, smart health monitoring then conservation of resources with respect to electricity water fuel you know. So, you know we should we can have a smart home where you know the water tap will be turned off if you know it is automatically it will be turned off may be with the help of ICT tools whenever it is not being used may be accidentally if I have turned on the tap the water tap it will be turned off similarly with the fuel consumption or conservation as well and like that and security and safety is very much paramount in a smart home security and safety for obvious reasons I do not need to elaborate on these, but safety at home security at home you know prevention of burglars from breaking into the house and so on. So, like that actually there are different other types of benefits of having a smart home.

Smart parking lots is very interesting smart parking lots is very interesting because you know. So, what happens is we all have experienced that when we are in the city and particularly when we are going in to the downtown areas or the central areas of a city typically parking is a huge problem. So, sometimes it might so happen that in some places you do not have any parking spot at all and maybe there are few other parking spots parking lots in the city which are vacant or relatively vacant and how do I get this information until I physically go there and get this information get this information, but you know that is basically infeasible.

However, if we have a smart parking solution in a city then one can one can from the mobile device inside the car one can get access to this information about which parking lots are available which ones are not and dynamically that information can be updated and made available to the users and other things like autorotation of vehicles to empty slots empty parking lots. Auto charging for the services that are provided detection of vacant lots in the parking lot and so on.

(Refer Slide Time: 25:17)

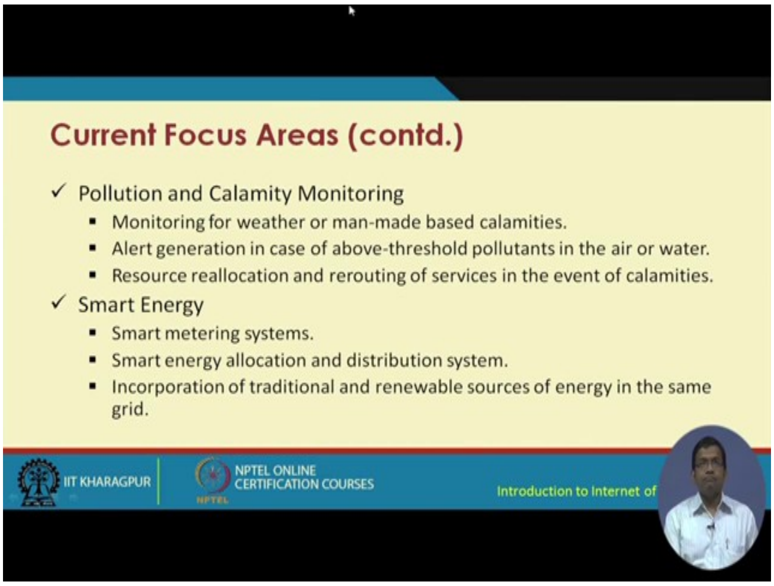


Smart vehicles with respect to assistance even to drivers during bad whether if there is a bad whether condition the low visibility condition the vehicles would be assisted about the you know how to drive ahead you know what are different ways the roots that can be taken from a particular point to the destination and so on detection of bad driving by patterns or driving under the influence of substances you know. So, the vehicle should be alerting the user of the vehicle driver and not only the driver may be the other corresponding stake holders like police or you know the respective dignitary bodies the authorities and so on auto alert generation duration crashes if there is accident auto alerts will be generated will be sent to the police the emergency personal and so on.

Self diagnostics of the vehicle you know if there is something some component going down something is going wrong with the engine or you know any of the other components of the vehicle you know. So, automatically it will diagnose and that information would be made available to the user of the vehicle similarly smart health low cost portable at home medical diagnostic kits be made available remote checkups and diagnosis would be made possible on body sensors for effortless and accurate health monitoring would be made available for use by the patients who need this kind of care.

Auto alert generation in case of emergency medical episodes like heart attacks seizers etcetera automatically the emergency persons in the hospital will be made available and that again is on the basis of subscription there might be several different several different hospitals with which the patient might get connected, but only to the hospitals with which the patient has a subscription you know. So, they will be getting notified and the emergency vehicles are going to the ambulances going to come to the home of the patient automatically without even having them to be informed.

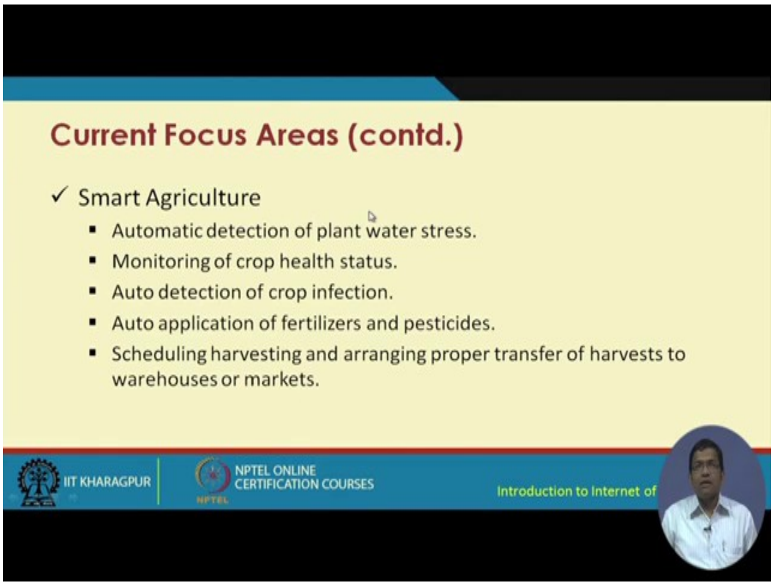
(Refer Slide Time: 27:25)



Pollution and calamity monitoring for whether or manmade based calamities alert generation in case of above threshold pollutants in air or water. So, on you know. So, nowadays actually we have all these air monitoring systems water monitoring systems these are in different isolation isolations basically this is monitor continuously we have the air quality index being monitored indifferent cities of our country. So, similar kind of thing is going on in different other countries as well. So, this sort of information from any point if I want to let us say from Kharagpur, I want to go to another place let us say Delhi. So, before I travel you know I can check that what is the air quality of that particular city; that means, Delhi and then I can make a decision about whether I should go there or not may be even better would be if I can get an advisory about whether it is safe to travel to Delhi because of this air contamination the air pollution and so on.

So, this is just an example like this actually these can be similar kind of thing can be done with respect to pollution and you know environment monitoring in a in any city smart energy like smart metering systems you know smart meters programmable meters through which you can do different things at your homes you know have differential usage being monitored and build accordingly in a smart grid smart energy kind of environment smart energy are allocation and distribution system incorporation of traditional and renewable sources of energy in the same grid.

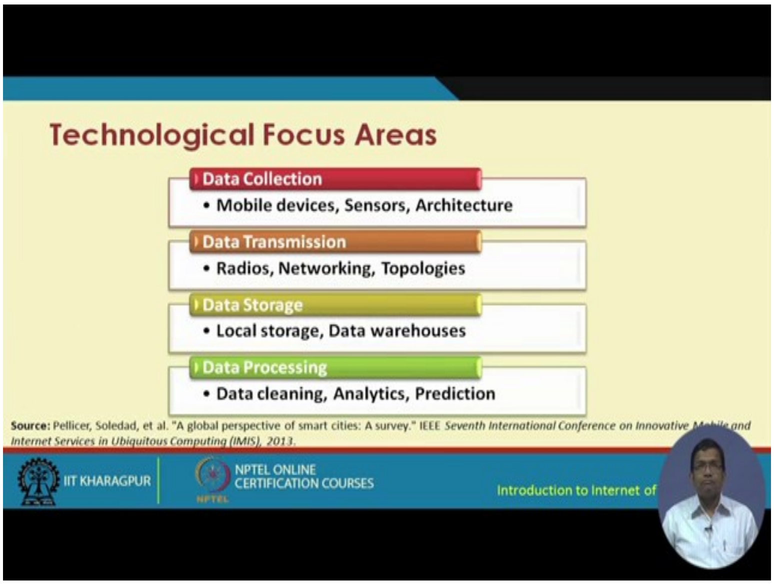
(Refer Slide Time: 29:07)



So, these are the different components these are the different benefits of smart energy; smart agriculture likewise automatic detection of plant water stress monitoring of crop health status auto detection of crop infection auto detection auto application of fertilizers and pesticides scheduling harvesting and arranging proper transfer of harvests to warehouses or markets. So, some of these actually as you will see in the case studies when we talk about case study on agriculture you will see that we are already implementing these in our lab in the swan lab of the department of CSC at IIT, Kharagpur we are already implementing some of these different things for smart agriculture we have projects by which the agricultural field are monitored with the help of censors and different other ICT tools and that information about the field cognition is made available to farmers so that the farmers can decide accordingly about what to do next.

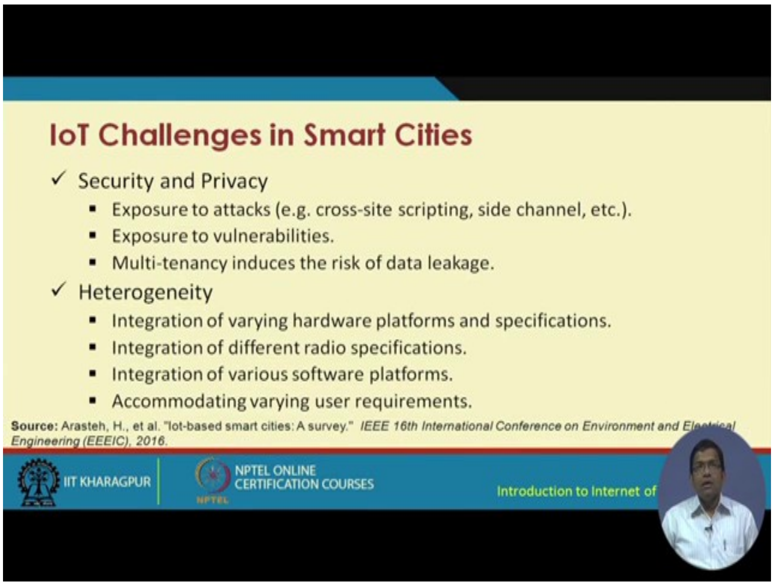
So, like this auto application of fertilizers is also possible and air born application of fertilizers with the help offspring or pesticides with the help of autonomously automatically you know this sort of thing is made possible in a smart environment smart city.

(Refer Slide Time: 30:18)



So, different technological focus areas include data collection with the help of mobile devices sensors and architecture I do not need to elaborate on these same thing I also do not need to elaborate on the need for the transmission of the data after collection of data through the above means with the help of radios networking topologies and so on different types of topologies communication and networking topologies consideration of those different topologies then the data that is collected and transmitted have to be stored locally and then remotely and as well in the form of data warehouses you know cloud storage and so on and they also again have to be analyzed to first of all cleaned analyzed and predicted.

(Refer Slide Time: 31:03)

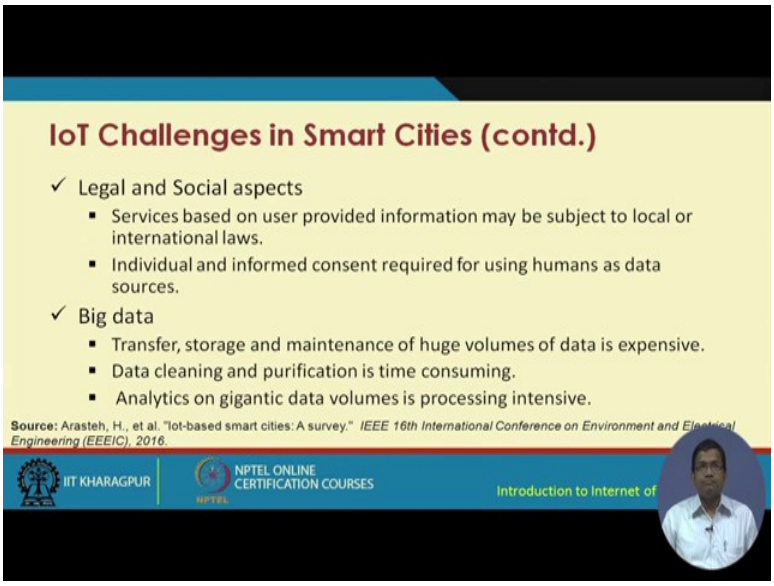


So, there are different IoT challenges in smart cities security and privacies one. So, because you know all these different infrastructure are made available to all different types of citizens. So, you know you expose yourself to different types of attacks the government officers there are different files etcetera you know you make yourself vulnerable to different types of attacks privacy leaks and so on when you open up more and more. So, that also has to be taken up concurrently while building smart cities and the same thing exposure to vulnerabilities multi tenancy of you know. So, the same devices are basically you know accessed by different tenants by different users and that multi tenancy basically induces the risk of data leakage the risk of data privacy leakage security data security and so on.

Heterogeneity integration of varying hardware platforms and specifications is a very you know important challenge and when we talked about IoT interoperability we spoke about some of these issues integration of different radio specifications integration of various software platforms and accommodation of varying user requirements are some of the different other heterogeneity and interoperability issues in IoT and we already spoke about this thing in detail in the lecture on interoperability of IoT in this in this particular course.

Reliability unreliable communication due to vehicle mobility is not good similarly device failures can happen and that has to be taken care of large scale deployment also has different challenges. So, there would be delay due to large scale deployment itself delay due to mobility of deployed notes and the distribution of devices can also affect the monitoring tasks.

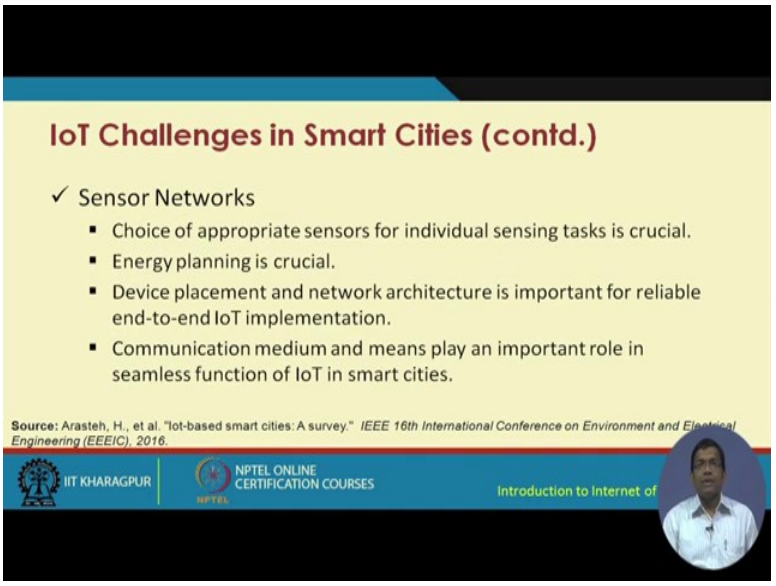
(Refer Slide Time: 33:02)



There are legal and social issues as well for example, services that are based on users user provided information may be subject to local or other national and international laws and that also has to be taken care of in a very smart way individual and informed consent is required for using humans as data sources big data issues are there you know huge volumes of data coming at high speeds and you know different types of vary various types of data media you know text data and so on.

So, these have to be clean in a purified and that is a time consuming process and then data it also has to be analyzed you know in real time to make sense out of it and the corresponding actuation has to happen.

(Refer Slide Time: 33:56)



So, big data issues are there big data in a real time environment is a very important and difficult challenge sensor networks you know we already spoke about sensor networks in detail earlier the deployment of sensor networks in a smart city comes with different-different challenges. The choice of different sensors for sensing is also very crucial energy planning is very much required different devices consuming different energy levels how you are going to schedule how you are going to do the duty cycling these are all different issues in sensor networks.

So, with this we come to an end of the smart cities you know smart cities and smart homes focusing on smart cities specifically in this particular lecture we have seen that there are different good use cases by which we can understand that smart cities is very much required and nothing else other than IoT and IoT constituent technologies can help in the building of smart cities and that is why there is so much of up search on not only research, but also deployment and investment on building smart cities throughout the world and there is lot of opportunity that is ahead in the building of smart cities and we are going to go through some of these different opportunities we have already seen the different challenges ahead some of these different other opportunities we are going through going to go through in the next lecture.

Thank you.

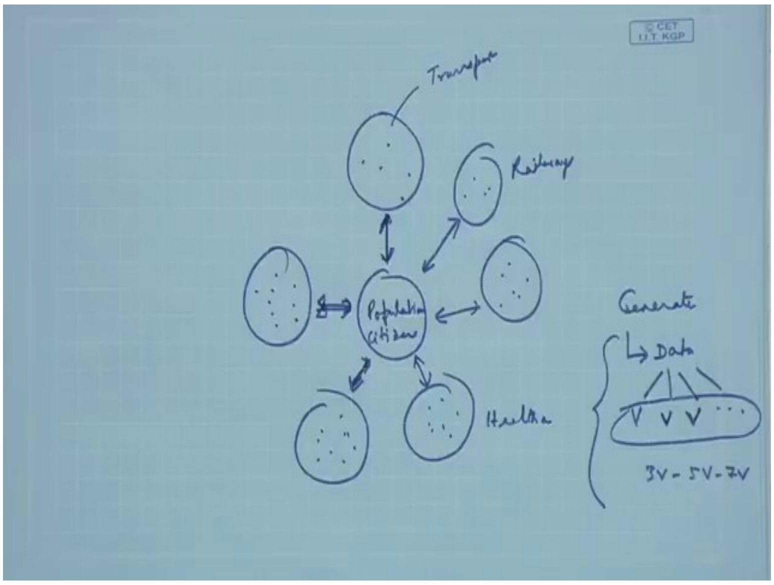
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 47
Smart Cities and Smart Homes-II

Now, we come to the second part of smart cities and smart homes. In part one, we spoke about the need for smart cities, the challenges in building smart cities, and few of the different issues with respect to building smart cities. So, in this particular lecture again we will be focusing on smart cities. And these again you know what ever we will be discussing on smart cities are also applicable for smart homes as well, but we will have you know a focus on smart of home in another lecture. But here we are going to discuss some of the technical issues behind enabling smart cities, some of the technical issues.

So, let us consider something before we go further. We have already seen that we have all these different components the transport, railways, schools and etcetera, etcetera.

(Refer Slide Time: 01:13)



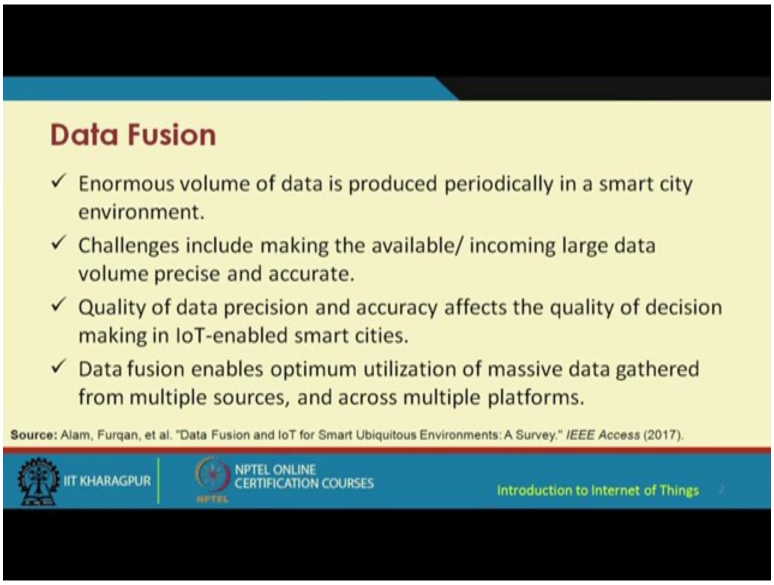
And let us say in between we have this population, population means the citizens right. So, all of these things these different components, let us say this is transport. So, transport component has different sensors has different actuators. These, this is let us say railway, railways, all source has the same other components schools, hospitals, they all have different sensors, and different other IoT devices. Which generate, which generate data, which generate and data. And this data has different you know characteristics with respect to volume this is gigantic, you know huge volumes of data, that each of these different components they are generating coming at high velocities, has different you know different types of data media data you know, multimedia data text data and so on and so on and so forth. They are at a these different characteristics of big 3 V to 5 V to 7 V, and this is something that we spoke about in a previous lecture already.

So, I not going to elaborate on these, but what is required is to do some good planning. So, what are you going to do with all this data? So, you know one possibility is that these data can be made available to the population, to the citizens. But making the data available just like that will not help. So, you have to do some processing. So, let us say that that processing is also done. Then you have to you have to fuse these data that are made available from these different sources, let us say transportation data and health care data sense from different points made available from these different locations, has to be this data have to be fused together in order to give better insight about different things in a smart city so that part is really challenging.

So, one thing is to deal with this kind of data, you know this big data that is coming in real time analyzing you know cleaning up processing, analyzing this kind of data in real time this is one thing. But in addition you have to fuse the data that are cross to (Refer Time: 04:15) that are coming from different sources, and that is a highly challenging issue. And like this there are different other issues in the building of smart cities, in the previous lecture we spoke about the overall idea the philosophy behind smart cities. But then you have to make it technically made possible, it is not like you know you connect few sensors and then, you know communication will be ZigBee Wi-Fi etcetera and then you make the data available no that data is going to be of limited use to the corresponding users of the stake holders so that is going to be of limited use.

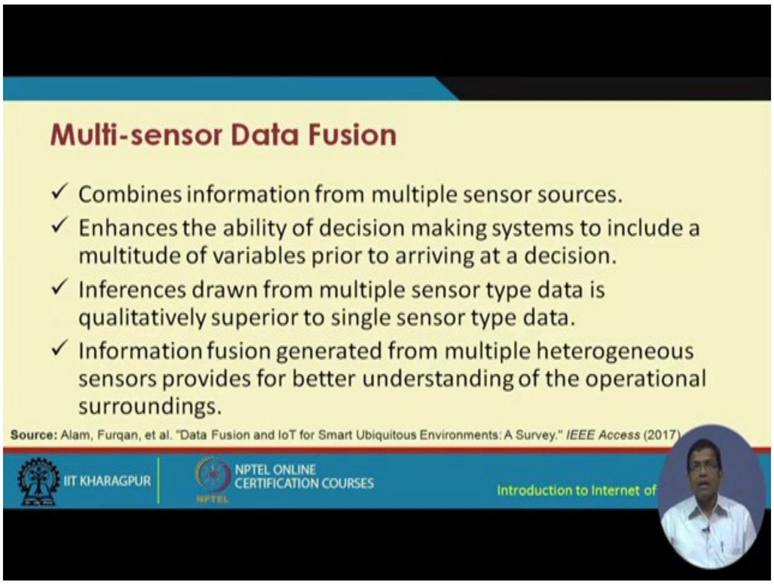
So, you have to you have to do some better job by fusing the data together, and then making that kind of fused data which has more in sight which will give more insight, you know that will be more useful.

(Refer Slide Time: 05:12)



So, let us look ahead and see what we have for us in data fusion. So, data fusion basically you know you are talking about in a smart city environment, we are talking about enormous volumes of data, that are produced periodically. And the challenges include making these particular type of data available. And so that the incoming larger data can make more sense can make more sense. And with the help of this data from these different sources, the large volumes of data from this different sources, different predictions, different analytics should be should be executed. So, the quality of data precession and the accuracy basically affects the quality of decision making, in this kind of IoT based smart city environments. So, data fusion basically enables optimum utilization of this massively collected data from different sources across different platforms.

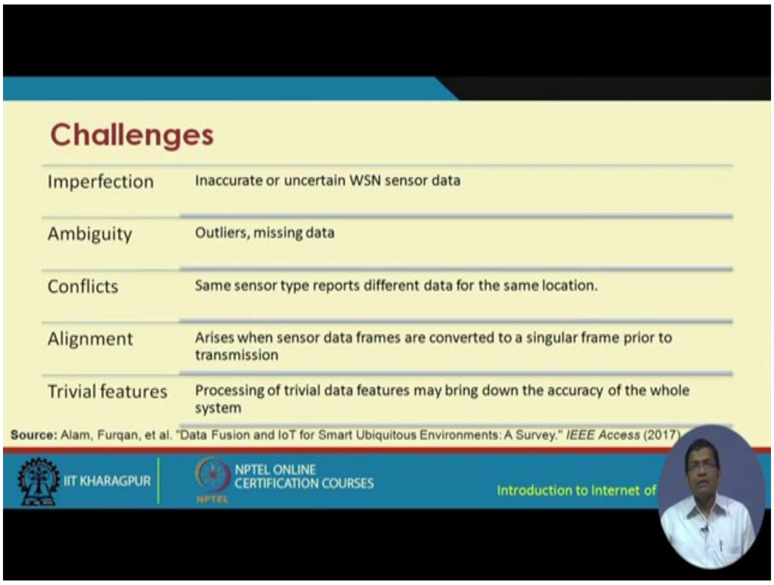
(Refer Slide Time: 06:18)



So, multi sensor data fusion is very important, which basically combines information from multiple sensor sources. It enhances the ability of the decision making system to include a multitude of variables prior to arriving at a decision, this is what I was telling you. So, it is not like clubbing two data together alone, but you considered the different you know different issues and considered the different variables that are affecting these systems, and you know taking all of these into account not just the sensor data taking all of these multitudes of you know, variables effecting the data and affecting the system together you come with you arrive at a decision, and make that decision made available not just decision, but may be different options and make that decision or the different options available to the users.

So, data fusion basically will help you in doing this. Inferences are drawn from multiple sensor type data and these are typically you know, qualitative the inferences are qualitative and you know, these basically are of more insight these are more insightful these are more meaning full than the single sensor type data. So, these putting these different types of it you know different types of data together and trying some kind of you know arriving at some kind of intelligent decision that is more insightful than the individual data. Information fusion generated from multiple heterogeneous sources provides for better understanding and understanding of the operational surroundings.

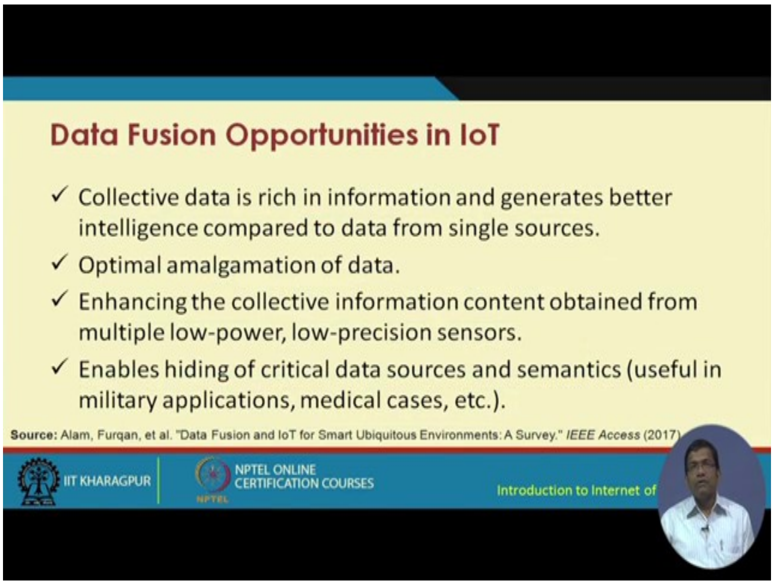
(Refer Slide Time: 08:05)



The challenges include, we are dealing with an environment where the data has lot of imperfection, imperfection due to inherent devices, devices like sensors etcetera, where there is lot of uncertainty around the environment there are lot of inaccuracies that can keep in. So, there is lot of inaccuracy uncertainty in the data and that basically leads to imperfections. Ambiguity is another we are talking about an environment where there are you know data that that are collected have lot of different outlets. Outlet means that there would be some data points which will be far away from the similar data points in the cluster. And there could be some missing data as well.

So, a ambiguity in the data can also creep. Similarity there can be conflicts in data that are connected from different sensors about the same thing, they might be conflicting they might be contradicting, alignment is like this that it arises when the sensor data frames are converted to a singular frame prior to transmission so that also has to be done, you know so that alignment you know into singular frame that is challenging. Different other trivial features for example, processing of trivial data features may bring down the accuracy of the whole system. And these are some of the challenges that have to be talked on when you are talking about data fusion in an IoT environment.

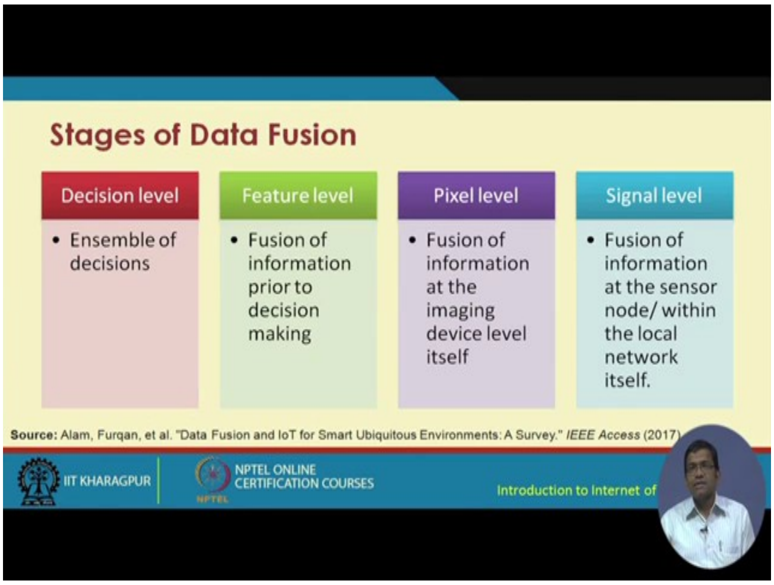
(Refer Slide Time: 09:38)



So, what are the opportunities? So, collective data is reaching information and it generates better intelligence better insight compared to the single source data from different individual sensors. So, putting these data together you know will make you to get better insight. So, you know what is the required is to optimally amalgate, optimally amalgate means that integrate optimally integrate the data, because you know the more and more you integrate you know it is possible to get more insight, but at the same time you know that also has to be done in real time to be you know, for that decision to be more meaning.

So, optimal amalgation of amalgamation of data, then enhancing the collective information content obtained from multiple low power low precision sensors. And enabling data fusion basically enables the hiding of critical data sources and the semantics.

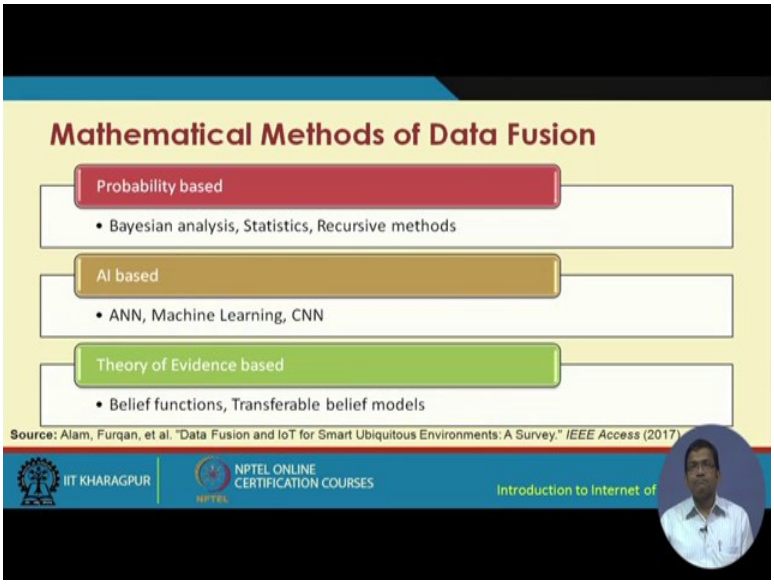
(Refer Slide Time: 10:43)



And that is useful for military applications for medical use cases. The different stages of data fusion include, decision level which is basically an you know talking about an ensemble coming up with an ensemble of decisions. Then feature level you know; that means, that the different features you know you fuse with respect to the different future features, at the feature level the integration is done the fusion is done.

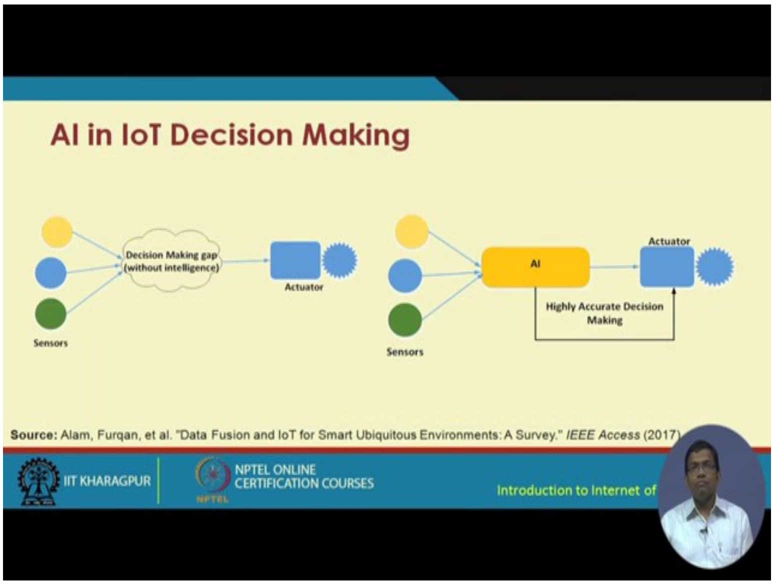
So, it is basically fusion of information prior to decision making. And pixel level is fusion of information at the imaging device level itself.

(Refer Slide Time: 11:28)



So, at the imaging devices that fusion is done in the device itself. And single level basically fusion of information at the sensor node or within the local area network itself. The mathematical methods of data fusion include using probability based schemes such as Bayesian analysis, statistics, recursive methods, EI based schemes such as artificial neural network, machine learning algorithms, deep neural networks, convolutional neural networks, theory of evidence based you know, evidence based schemes. For example, belief functions taking use of belief functions transferable belief models. So, these are the different mathematical methods that are used in order to come up with these intelligence from the different data that are you know that are secured from the different IoT devices.

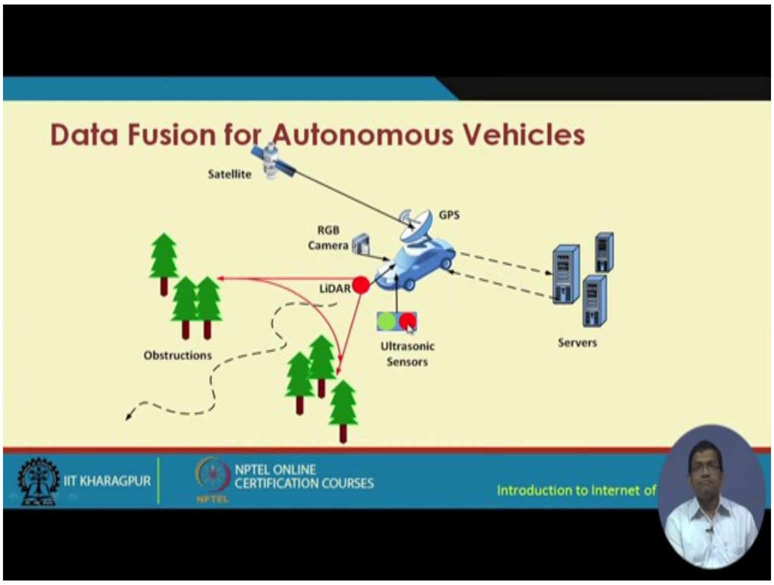
(Refer Slide Time: 12:14)



So, AI artificial intelligence comes as a big helper in enabling this. So, you know let us consider this particular figure. So, traditionally what happens is you have these different sensors and the sensor data has to be transmitted over the communication medium and has to be you know based on that some actuation is going to happen. But how that actuation is going to be made you know made possible, is it from one or 2 of these sensors in a based on these sensor value you are going to actuate, or can we do something better.

So, for betterness betterment what can be done is some kind of decision making has to be done with the help of intelligence by, by adding intelligence between these different sensors and the actuators we can make things better make things improved. So, how is that made possible? With the help of artificial intelligence tools methods algorithms and so on.

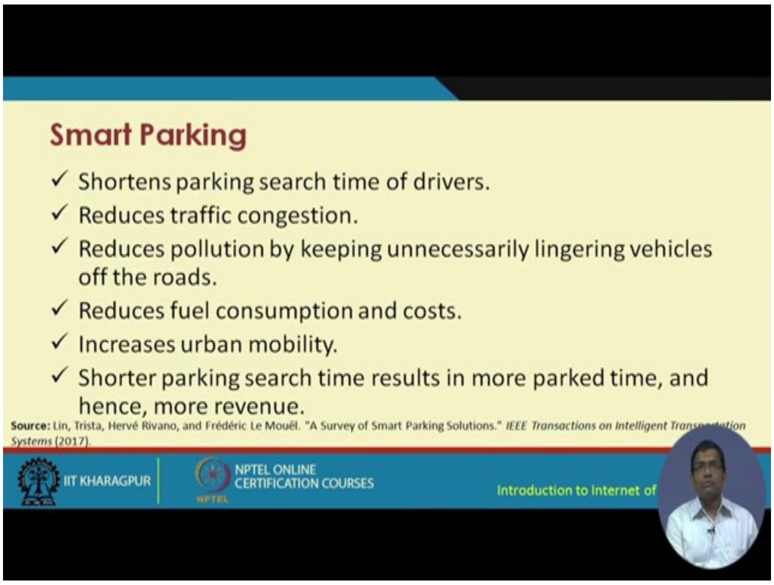
(Refer Slide Time: 13:23)



So, AI come as a rescuer over here, and what AI can do is it can make highly accurate decision making possible between the sensors and the actuators. So, let us consider the scenario of decision fusion for autonomous vehicles. So, for autonomous vehicles like autonomous cars etcetera, etcetera. They interact a lot with the environment you know, when there is a driver less car for instance. They need to take help of this different sensors they need to also communicate with you know the with the satellite with the GPS with the help of technologies such as you know LiDAR technology for obstruction you know, for getting a map of the obstructions ahead, or the ultrasonic sensors can help in even checking some different obstructions that are ahead of them in a small scale. LiDAR can give a bit bigger picture whereas; ultrasonic sensors can give a small scale picture of what is ahead of the autonomous vehicle.

So, autonomous cars you know they basically are collecting different data from different sources through different technologies like LiDAR sensor networks you know, from satellites through GPS and different cameras ahead of you know, in front of them. So, they all these different data of different types as you can see are connected and they are sent to the server. Now you know these data of different types you know, individually they do not make much sense they are of limited help, but together can these data be fused together, so that the car the autonomous car can get some kind of decision making, about how it is going to proceed or whether it is going to turn left or right or what it is going to do. If it sees some pedestrians in front, then what it is going to do? Like this kind of thing is made possible with the help of data fusion data fusion technology. So, all these decision making through you know of the data that is connected from the different sources you know that is basically made possible with the help of data fusion.

(Refer Slide Time: 15:26)

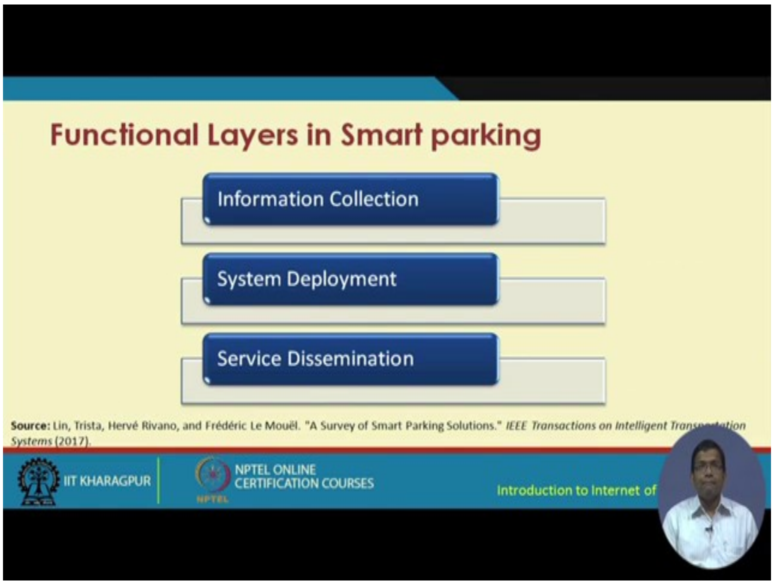


Smart parking, I already spoke about smart parking in a in the previous lecture, but let us dig into this smart parking little bit further. Smart parking is very much an important component now a days we have smart parking solutions in different cities already started to be deployed. So, in a smart parking environment what happens is, you know the user knows ahead of actually going to that particular spot, that which of the spots in the cities have free parking spots right. Which of these different parking lots have free parking spots. And then accordingly the driver can make a decision about where to go and park the car.

So, smart parking basically shortens the parking search parking search time of the drivers. So, basically you know searching for the different parking lots that search time would be reduced will be shortened and you know it the parking is going to be made efficient. It reduces the traffic congestion, reduces the pollution by keeping unnecessarily lingering vehicles off the road. So, you know So, what would happen is in a smart way you know where to go and where to park that way it is not going to happen that you are in a queue waiting for your parking your engine is on you are polluting the environment.

So, in a smart parking basically also helps in reducing pollution unnecessarily in a city. It reduces the fuel consumption and costs as well and these are all actually interlinked, so that you know fuel consumption more fuel consumption more pollution. More costs are involved you know so, like this these are all interlinked. Increases the urban mobility and the shorter parkings search time results in more parked time and hence more revenue.

(Refer Slide Time: 17:10)



So, in a smart parking scenario we are talking about you know information collection, system deployment, rather I would start with the system deployment system is deployed information is collected, and the surfaces are disseminated to the end users.

(Refer Slide Time: 17:28)

So, these are the different functional layers of smart parking. In terms of information collection information is collected from the sensors the individual sensors in the car in the parking lot, there are different parking meters the sensors are networked together. So, you have the sensor network, and also the crowd sensing, crowd sensing basically is from the crowd the from the different sensors in the mobile force in the smart phones for instance you are able to collect the different data, and these data will help in decision making.

So, all these data taking together and fusion of these data will help in decision making.

(Refer Slide Time: 18:03).

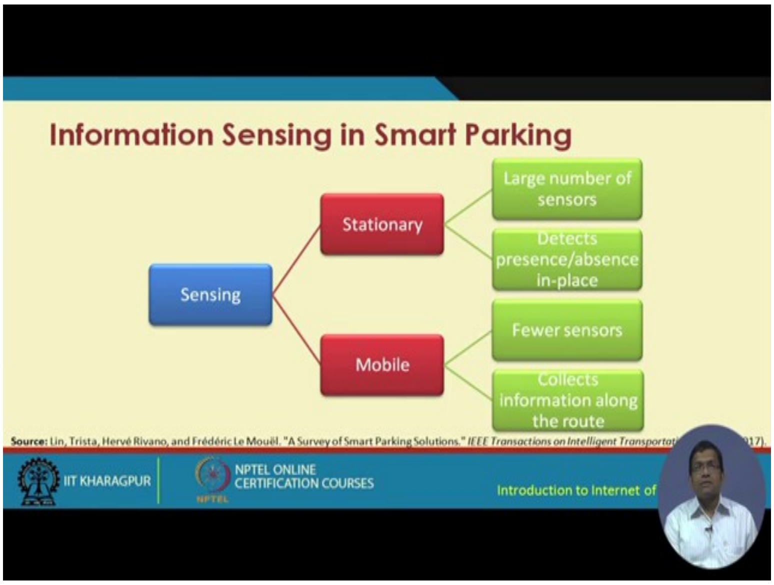
Then we have the system deployment with respect to the software system that has to be developed, the information management of the data, the E-parking you know guidance system that will help in guiding the vehicle, about where to go how to go and you know and parking the car there then the data analytics over all.

(Refer Slide Time: 18:28)

So, these are the different system level deployment issues in smart parking. Service dissemination with respect to dynamic pricing, strategizing, infrastructure based information infrastructure free information.

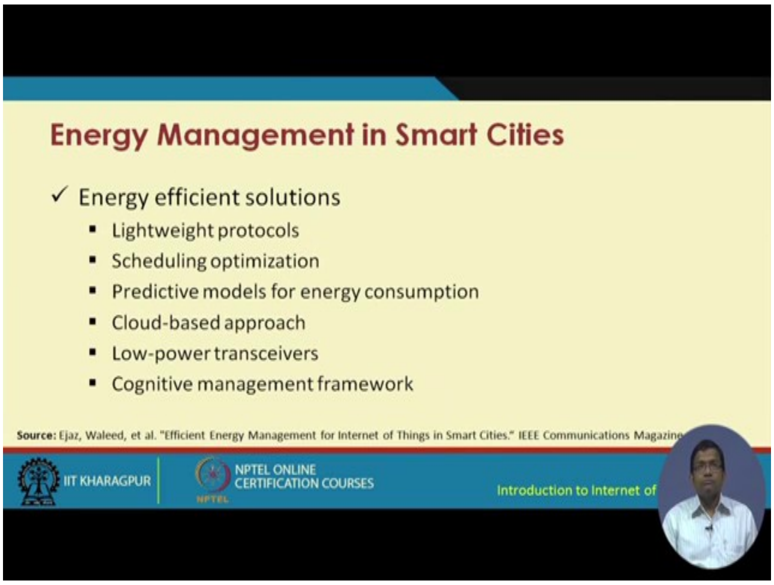
So, infrastructure based and infrastructure free. So, infrastructure free from the different sensors you know these are not connected to the regular infrastructure like Wi-Fi etcetera, etcetera. This is infrastructure free infrastructure based means like from the regular internet infrastructure from the regular city communication infrastructure like Wi-Fi and you know like 3G, 4G you know, the cellular networks. So, on these are all like the infrastructure based, and then infrastructure free is what I just told you with the help of sensors ad hoc networks formed out of these different mobile device of different users etcetera. Then parking choice and vehicular activities these all contribute to the building of services required for smart parking.

(Refer Slide Time: 19:22).



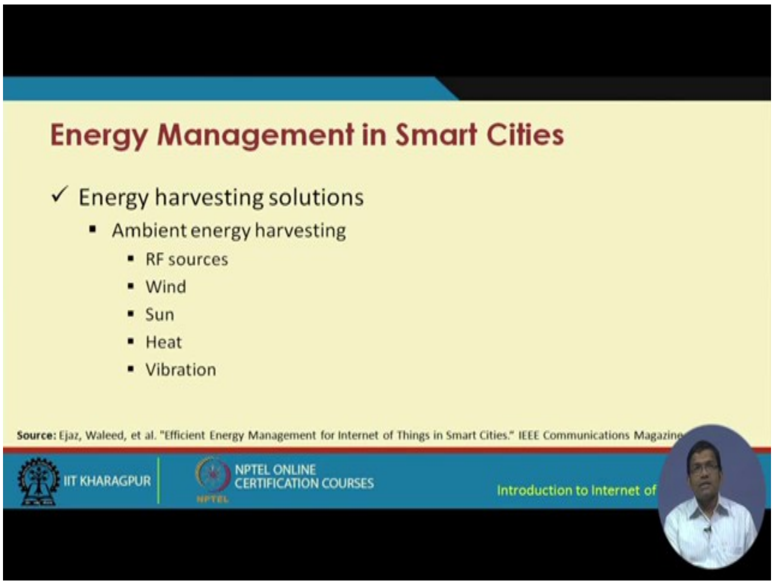
In terms of information sensing in smart parking, the sensing can be done from stationary sensors or from mobile sensors. Stationary sensors like you know if you are collecting the data from stationary sensors you need large number of sensors to be deployed at different points, which will detect the presence or absence of different vehicles or from mobile sensors where fewer sensors would be required compared to the case of stationary sensors, and these mobile sensors the fewer mobile sensors would collect information along the root when they go by.

(Refer Slide Time: 20:00)



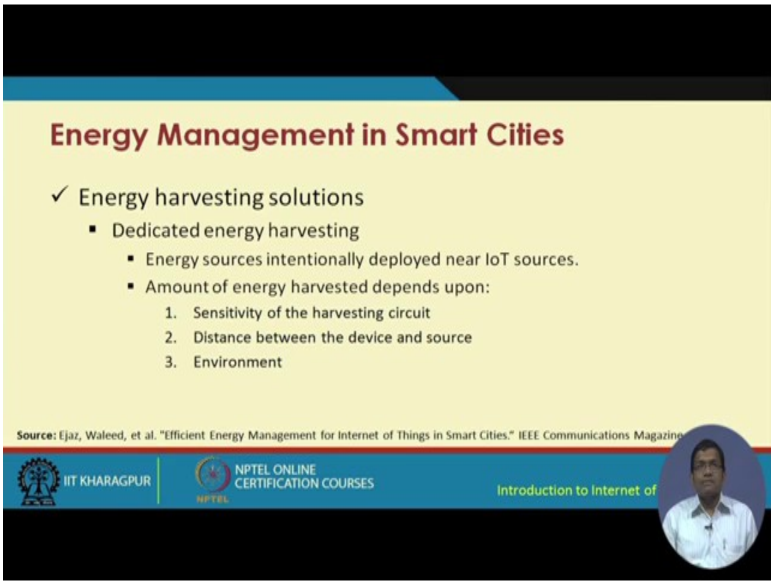
Energy management in smart cities you need energy solutions. So, energy efficient solutions it is required to light weight the protocols because you are dealing with a highly resource constraint environment, and at the same time energy consumption has to be reduced for you know reasons of greenness environment and so on. So, lightweight protocols are required, it is required to schedule the optimization of you know optimization of energy consumption. And then predicting models for energy consumption is another important thing. Then you have the cloud based approach, low power conceivers, cognitive management framework these are the different energy efficient solutions for energy management in smart cities.

(Refer Slide Time: 20:47)



Energy harvesting solutions would include technique help of these you know harnessing energy from these renewable sources of energy, such as sun, wind, heat, vibration RF sources. Now a day's people are talking about harvesting energy from radio frequencies as well. So, from RF sources harvesting energy from sun wind heat vibration and like this. So many different types of you know sources of energy ambient sources of energy are there, and how you can harness the energy from all of these different sources.

(Refer Slide Time: 21:24)



Energy harvesting solutions would include dedicated energy harvesting by the deploying different you know different sources like solar panels, etcetera; you know deployed pre deployed. Energy sources are intentionally deployed near the IoT sources to power these IoT devices for example, in our agricultural field, closer to the sensor node very close to the sensor node, we have these solar panels. And these panel solar panels basically power the sensor nodes that we have deployed in our agricultural field and these sensor nodes are basically deploy you know, were developed in the swan lab of our institute. So, the distance between the device and the source, the sensitivity of the harvesting circuit and the environment these basically are contributors to determining the amount of energy that is harvested.

So, with this we come to an end of the second part of the lecture on smart cities. Here we have mostly covered issues such as, how to handle the data that is received from this different sources. We can try to make inferencing with the help of these standalone sensor data that are received the separate individual data that are received. Or is it possible to do better, you know it is possible to do better by fusing the data from the different sources together with the help of intelligence and so on. So, this is the end of the smart cities part 2. The next in the next part we are going to talk about few other different issues of building these smart environments and there the focus will be on smart homes.

Thank you.

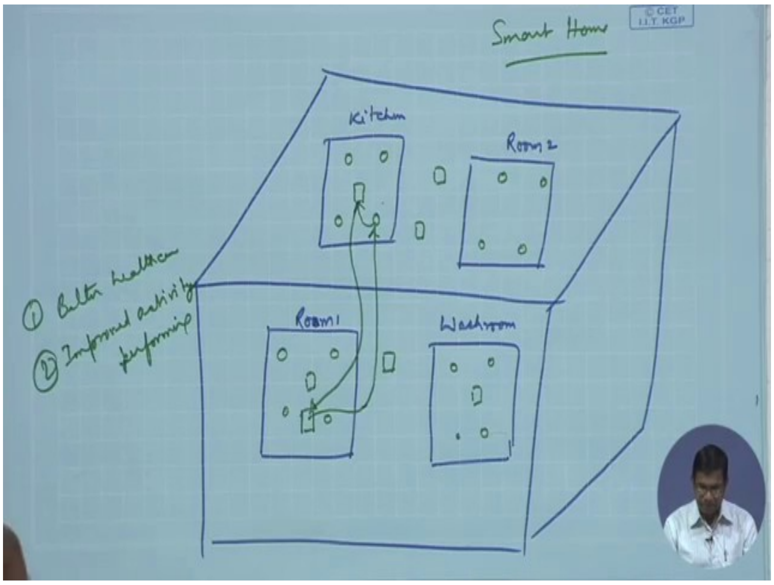
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 48
Smart Cities and Smart Homes – III

So, we now come to the part 3, the third part of smart cities and smart phones and unlike in the previous 2 lectures where we focused mostly on smart cities. Here in this particular lecture, we are going to focus on smart homes. So, when we talk about smart homes we are talking about the integration of ICT technologies like the once that I mentioned as part of the previous 2 lectures or even the once that we spoke about throughout in this course taking help of these different technologies, how we can make our home homes smart.

So, let us consider a scenario like this. So, we have, we have, let us say a smart home in a home.

(Refer Slide Time: 01:02)



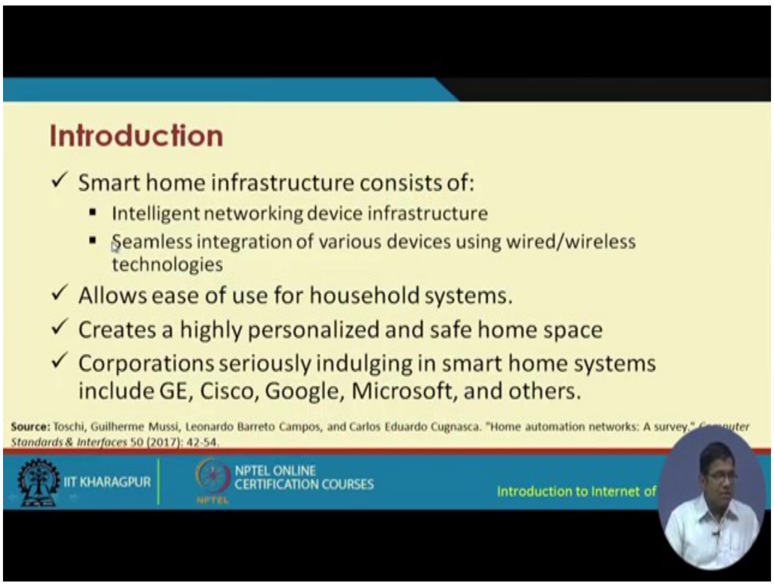
We have different rooms, we have you know, let us say let me let me just for simplicity. Let me just denote these different rooms here and so on. I am not as you can see I am not very good in this art particularly when it comes to 3 D pictures. So, let us say that this is a room 1, this is room 2, then you have a kitchen, then you have the wash room.

So, in a smart home you have different, you have different sensors that are basically deployed in different places. Then the same time you also have some actuators as well let us say that these are the different actuators which can be could be even some could be in the room itself. So, you have different sensors actuators and different types of other like NFC devices or you know, different other IoT devices and they talk to each other.

So, let us consider that you know we have in a smart home. We have to do something better. So, do what let us say that we have to you know cook something in a better manner. So, what can be done is you know from a particular room where we are sitting. So, from that point on there could be some kind of a device which can go and which can which can go to the kitchen you know, and from the refrigerator of the kitchen it can take out something. And then you know in kitchen there is a microwave device it is going to put that in the microwave device then it is going to boil it or you know it is going to you know warm up in the micro wave oven and then it is going to serve me right.

So, this is one example, like this you know there are different other things at home different activities that we do at home these could also be made smarter. So, this is an example of smart home, in smart home you need better health care, better health care you know improved activity ah, you know improved activity, I would say that; you know performing and so on like this you know. So, whatever regular activities that you do those can also be improved. So, that the activities can be done you know efficiently.

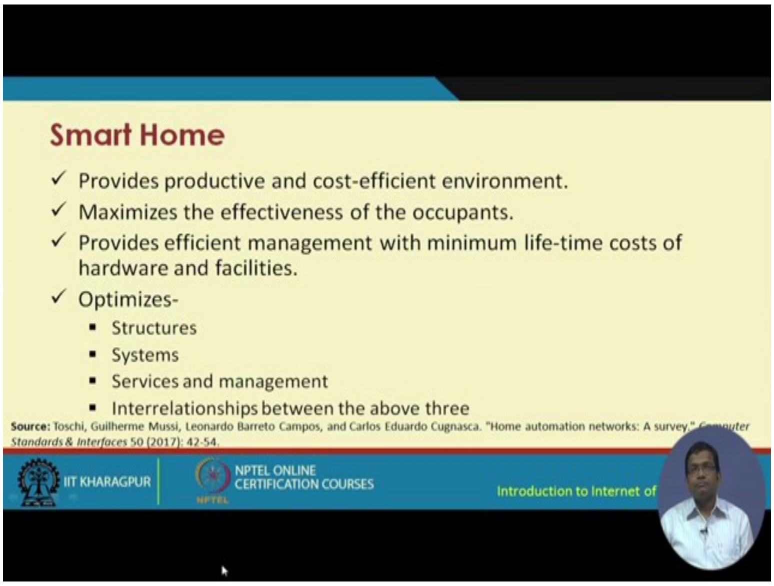
(Refer Slide Time: 04:49)



So, going back let us look at the smart home infrastructure. So, you need these different infrastructure, these infrastructure as I telling you so far, that you have these different sensors actuators different robotic devices that are there at your home. And also you need the networking infrastructure. So, you have intelligent networking device infrastructure, there is seem less integration of this various devices the sensor actuators etcetera, using wireless typically wireless technologies are used, but wire technology could also be used in addition.

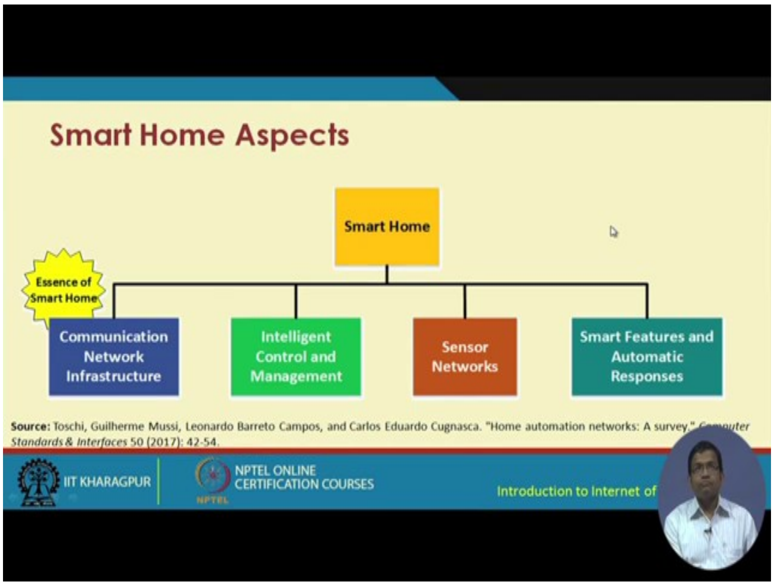
So, this basically allows the ease of use of house hold systems. So, improving the efficiency of performing different activities in a smart home or the use of these different house hold systems can be improved. It creates a highly personalized and safe home space so, you know whatever I need you know I can do things efficiently you know, and why it is efficient? Because let us say that you know if I have run out of the groceries the grocer is going to be informed. So, that will make it more efficient. So, corporations like you know; Cisco, Google, Microsoft and many others they are seriously thinking about building smart home systems, they are seriously thinking about they are inversing on building smart home systems. So, smart home systems have become very popular in the recent years.

(Refer Slide Time: 06:18)



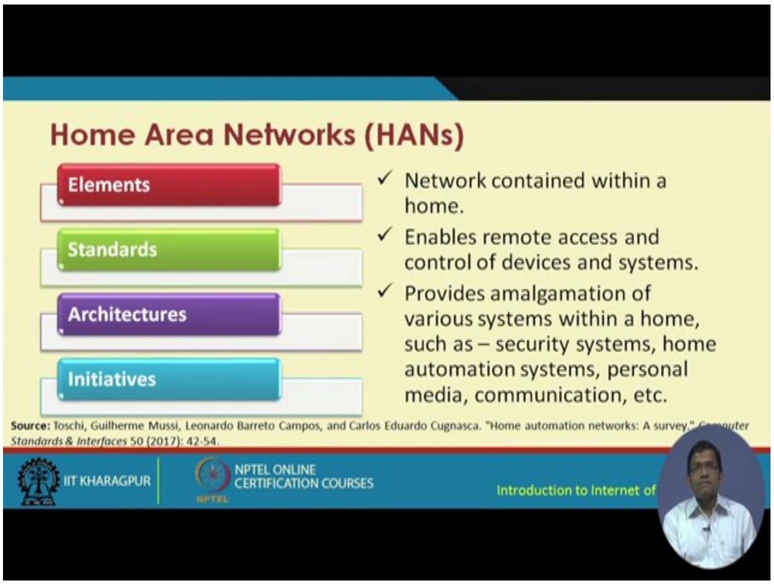
So, smart home basically provides productive and cost effective environment, because you know if you are doing things efficiently the cost is going to improve you know is going to reduce. So, it is going to be cost efficient maximizes the effectiveness of the occupants provides efficient management with minimum life time costs of hardware and facilities and optimizes things such as structures systems services and management interrelationships between the above three. So, all these are going to be optimized in a smart home environment.

(Refer Slide Time: 06:54)



So, in a smart home basically the different components are sensor networks, sensor networks, intelligent control, intelligent management, communication network infrastructure and smart features and automatic responses.

(Refer Slide Time: 07:11)

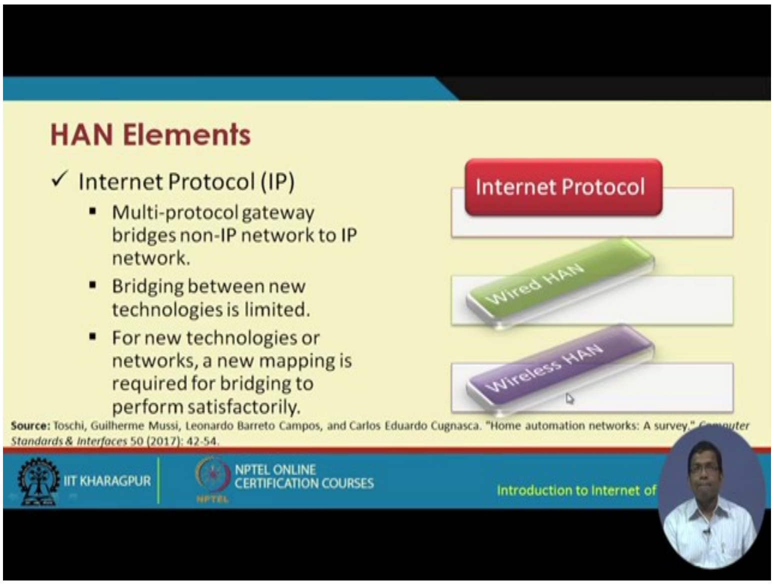


So, in a smart home we are typically talking about something known as home area network, which is analogous to something like a local area network in a building or couple of buildings together when you know typically we have these local area networks. So, smart sorry, and then we have this personal area network. So, personal area network is very much like you know small in terms of the range typically you know human bodies have the personal area networks, or then we can have this personal area networks out of this different peripheral devices in a computing system.

So, personal area networks is too small. Then the local area networks are much bigger. Then we need something in between for use in smart homes and this is known as the home area network. So, in a home area network we have different components we have these home area network elements which we are going to talk about in more details shortly. So, the network is basically content within a particular home in a home area network. Then we have there is different standards, the architectures then we have the different initiatives.

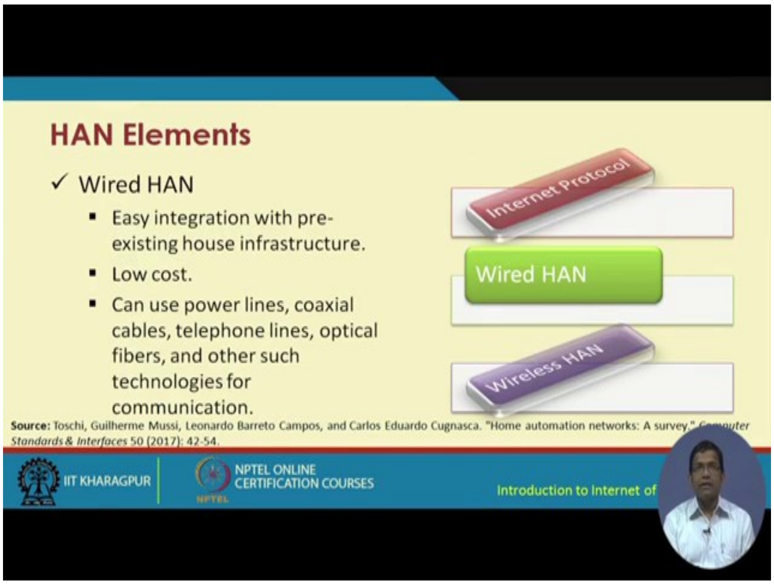
So, basically you know. So, we are going to talk about each of these in further detail with respect to the home area network home area network elements home area network standards home area network architectures and the different other initiatives we are going to talk about shortly. So, the network is contained within a home it enables the remote access and control of devices and systems, and provides amalgamation of various systems within a home such as security system home automation system personal media communication and so on.

(Refer Slide Time: 09:00)



So, let us start with the home area network element the first one is IP protocol. So, we have multi protocol gateway bridges the non IP network to IP network. In other words you know, so you have in a home area network, support for both IP based networks the traditional internet based networks as well as there are some non IP based networks as well. And there are gateways that would bridge multiprotocol gateway; that means, support you know those gateways basically support they understand the language of different protocols both IP based protocols they understand as well as the non IP based protocols both they understand. Bridging between new technologies is limited with the help of you know, IP based a thing; IP based protocol and for new technologies or networks a new mapping is required for bridging to perform satisfactorily.

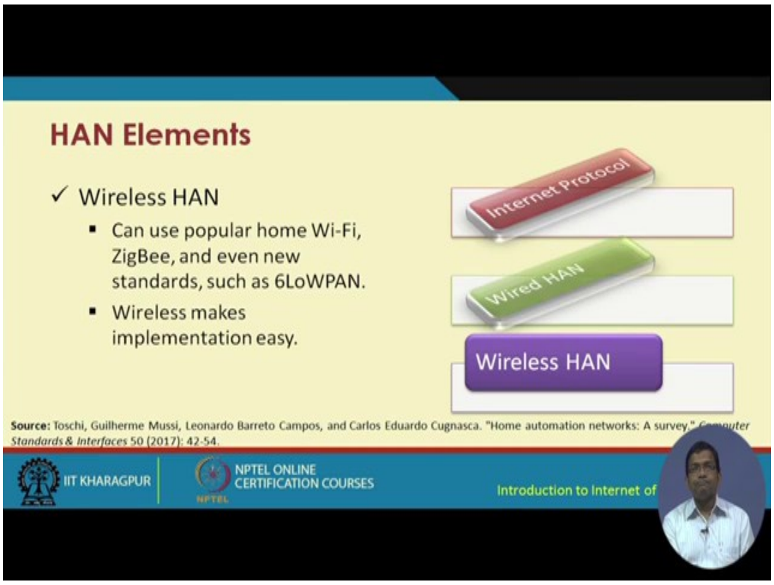
(Refer Slide Time: 10:05)



The next one is the wired home area network. So, these basically enables easy integration with pre existing house infrastructure like existing telephone systems existing cables you know cable television cables and so on. So, easy integration is possible with the help of this it is low cost because you know, you do not need additional wiring additional infrastructure you know with the help of these existing systems it can be done. And you know this is cheaper, but at the same time you know it is it has you know different limitations it has different limitations because mobility is one issue.

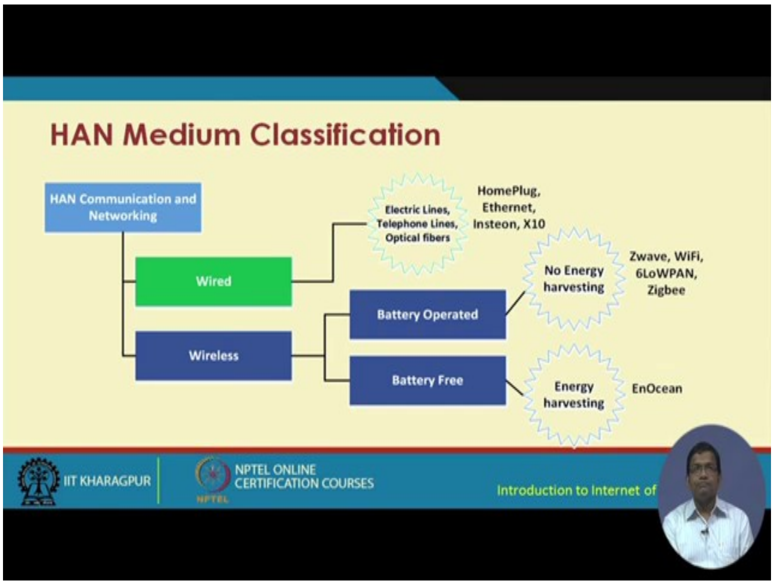
So, if it is all wired you know you cannot move around and mobility is very important you know, where easy ease in mobility is very important in a in a in a smart environment in any smart environment and in a smart home as well. So, you know all though wired technologies in a home area network are less expensive compared to the wireless counterpart but at the same time it also restricts the mobility of the users at home.

(Refer Slide Time: 11:15)



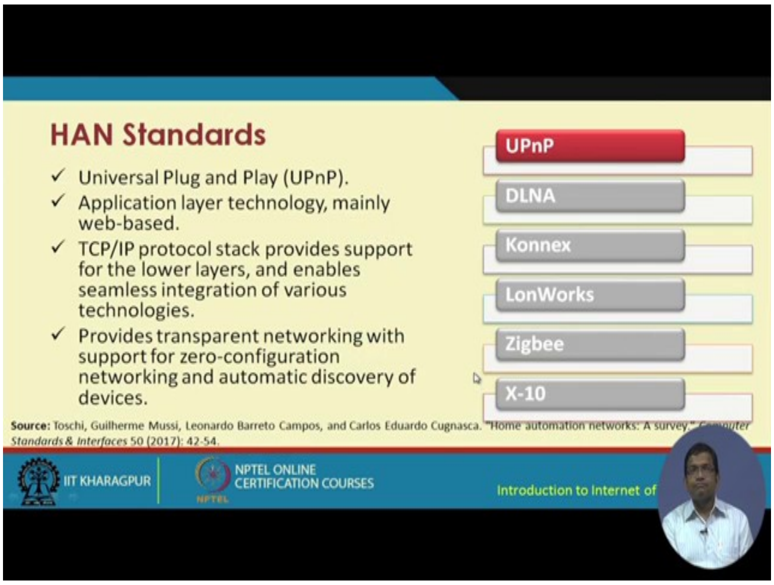
Wireless home area network uses different technologies like Wi-Fi, ZigBee and the different others that is spoke about in this course by earlier part of this course. For example, the ones that we covered in module one the different technologies those can be used for wireless home area network. So, wireless makes implementation easy it improves the mobility of the users there by improve the satisfaction and the utility of home networks you know over all this utility is going to improve.

(Refer Slide Time: 11:51)



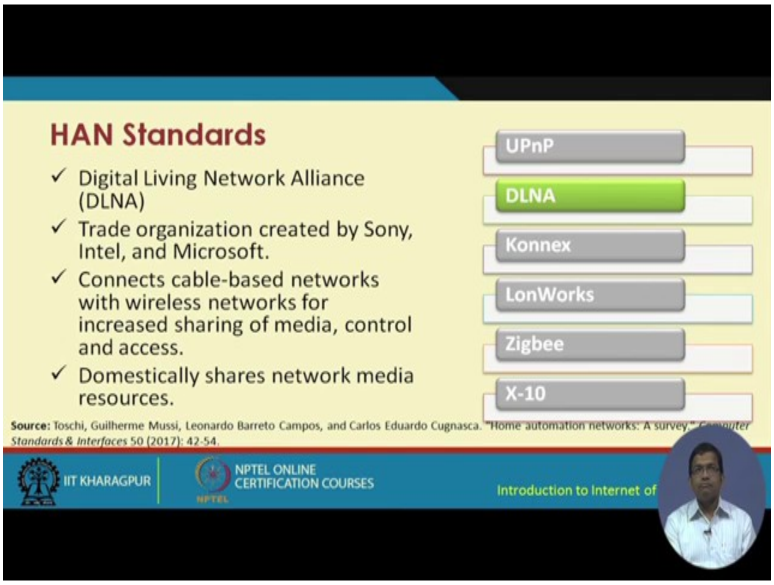
So, the classification of home area networks. So, we have the home area network communication and networking technologies which are wired or wireless. Wired would take help of electronic sorry electric lines, telephone lines, optical fibers that are already existing at home, even the cable television cables cable TV cables and so on. Wireless basically are typically battery operated or they can even be better if free, and the battery operated there is no energy harvesting in battery free there is energy harvesting. And some of this protocols that basically help in this battery operated energy harvested communication in a home area network are given over here. So, we have Zwave, Wi-Fi, 6LoWPAN, ZigBee and so on. In enocean basically harvests energy and it is battery free wireless technology.

(Refer Slide Time: 12:52)



Now, the different standards that are supported. We have the most important one the most popular one the UPnP, universal plug and play. Universal plug and play is a protocol standard that is used typically in most of the smart environments and particularly for building smart homes. See universal plug and play is an application layer technology particularly for web based applications it is used.

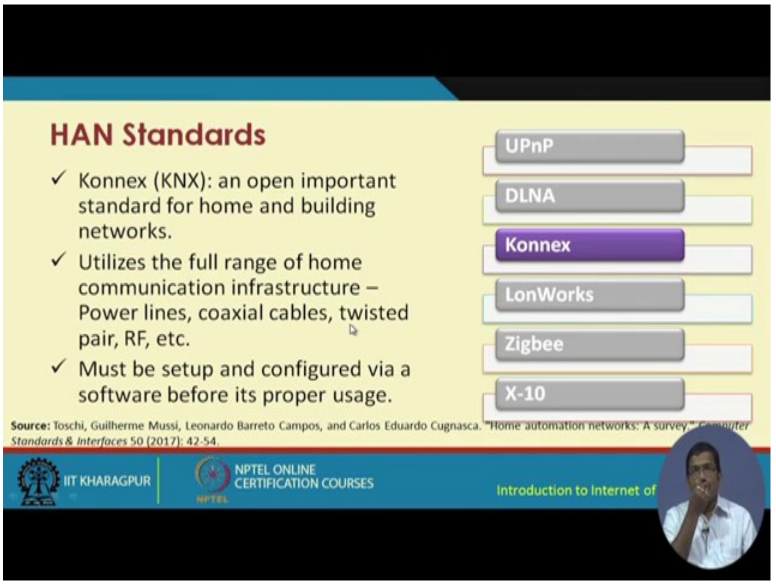
(Refer Slide Time: 13:46)



So, the TCP/IP protocols stack provides support for the lower layers and enables seamless integration of the various technologies and provides the transparent networking with support for zero configuration networking and automatic discovery services.

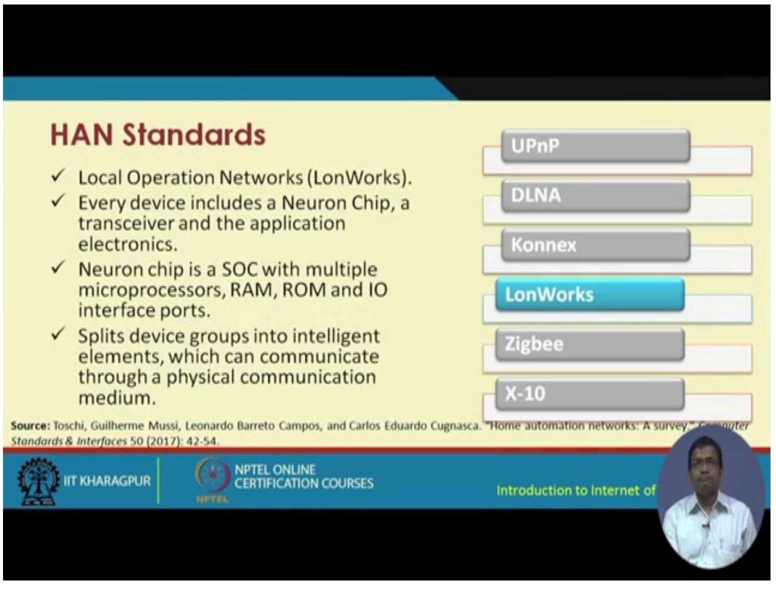
Then we have the DLNA the full form of which is digital living network alliance DLNA. It is a trade organization that is created by companies like Sony, Intel and Microsoft. It connects cable based networks with wireless networks for increased sharing of media control and access. So, cable networks come up with lot of media content, sharing those with the help of other wireless networks with the users. So, the DLNA digital living network alliance basically this helps in this kind of content being made available the media reach content being made available in domestic front for use by the domestic users at home.

(Refer Slide Time: 14:40)



Then we have this Konnex standard in short it is also known as the KNX standard, which is an important standard for home and building networks. Which utilizes the full range of home communication infrastructure including power lines, coaxial cables, twisted pair, RF etcetera. When whatever is existing those existing infrastructure the communication infrastructure at utilized in Konnex. And this must be set up and configured via a software before it is proper usage.

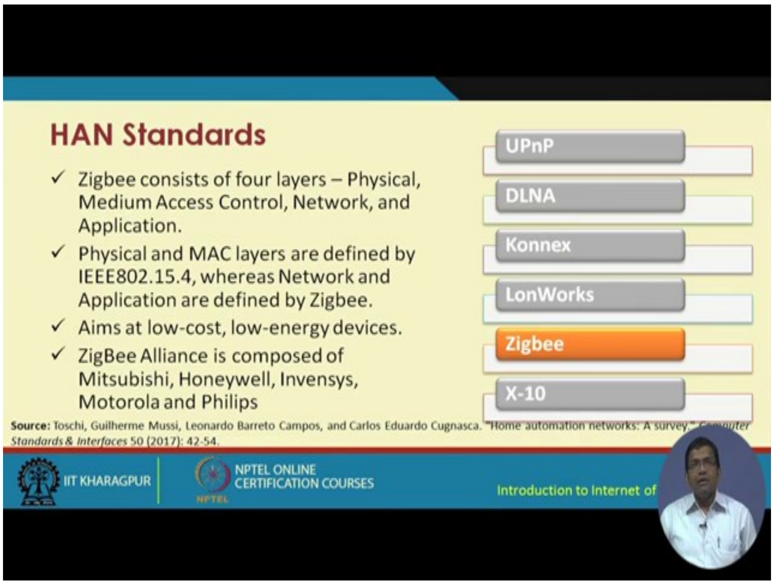
(Refer Slide Time: 15:13)



Then we have the LonWorks, local operation networks LonWorks, where every device includes a neuron chip. You know, LonWorks has different devices which include something known as the neuron chip which has a transceiver and the application electronics.

So, then neuron chip is a system on chip with multiple microprocessors RAM, ROM, I/O interface ports and so on it is split is the device groups into intelligent elements which can communicate through a physical communication medium. Then we have the ZigBee and ZigBee. We have actually discussed in a lot detail in module one.

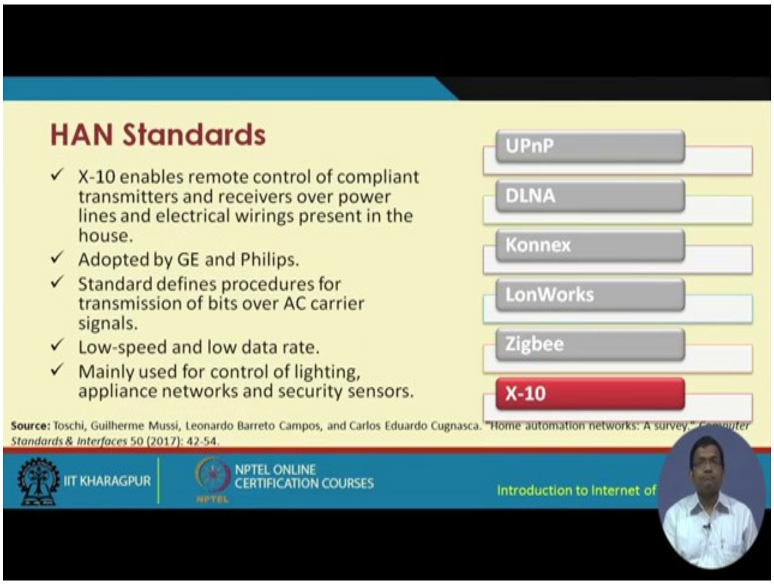
(Refer Slide Time: 15:49)



So, I am not going to talk about in too much detail here. But from a home area network perspective ZigBee is very commonly used. It has the different layers the physical layer, the mac layer, the network, layer and the application layer as you already know. By virtue of your existing knowledge of ZigBee in the module one of this course.

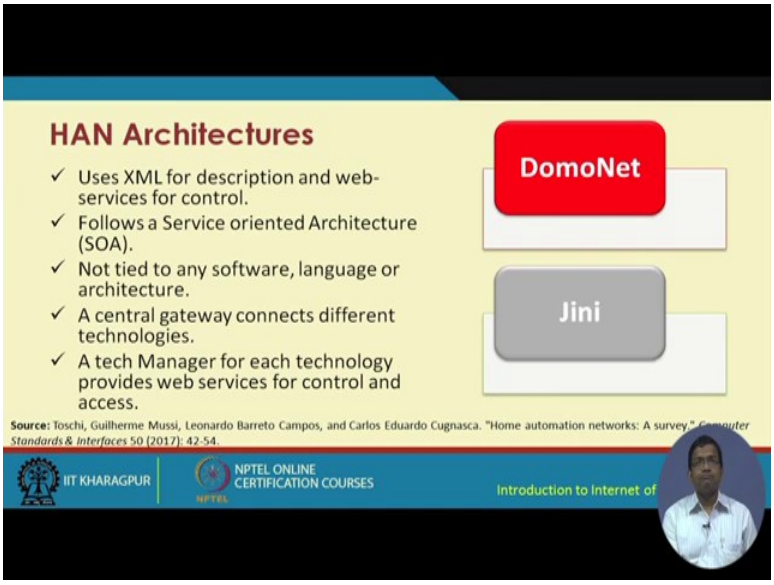
Physical and mac layers in ZigBee are defined with the help of the 802.15.4IEEE standard whereas, the network and application layers are defined by ZigBee, ZigBee itself. It aims at low cost low energy devices and there is a ZigBee alliance comprising of the companies such as Mitsubishi, Honeywell, Invensys, Motorola and Philips.

(Refer Slide Time: 16:44)



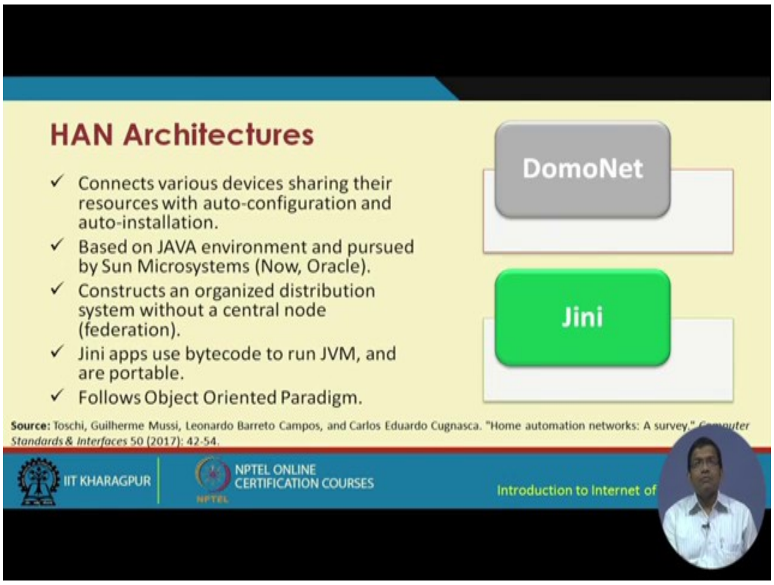
So, this basically guides the development of the ZigBee standard forward. X-10 is another standard that enables remote control of complaint sorry, of compliant transmitters and receivers over power lines and electrical wirings that are already present at home. It was adapted by GE and Philips, and this standard defines the procedures for transmission of bit is over carrier alternating carrier current carrier signals. And it has low speed and low data rate and is mainly used for control of lighting appliance networks and security sensors.

(Refer Slide Time: 17:22)



Now, let us talk about in brief about the different home area network architectures. The home are network architectures two of them are quite popular, the first one is the DomoNet which uses xml for description and wave services for control follows, follows a service oriented based architecture. And it is not tied to any specific type of software language or architecture. Here in DomoNet a central gateway is there which connects different technologies. And there is also a tech manager for each technology that provides a web services for control and access.

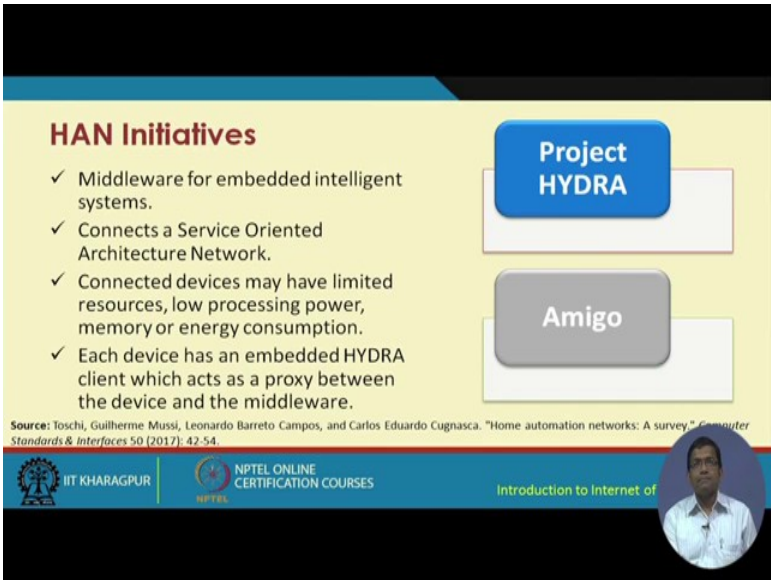
(Refer Slide Time: 18:01)



Then we have this Jini architecture that helps in connecting various devices sharing their resources with auto configuration and auto installation. It is based on the java environment and is perused by the company sun microsystems which later one became oracle.

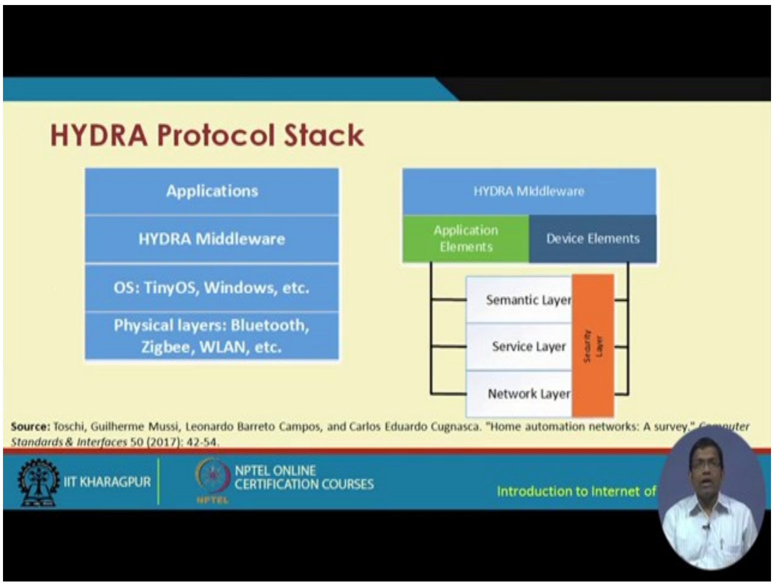
It constructs an organized distribution system without a central node Jini applications use the byte code and the JVM. So, this is basically java environment compliant that is the reason actually it is using the JVM and the byte code and are portable. Because you know it is it is based on the use of JVM and byte code byte code based technologies. So, where ever this JVM is installed So, you know byte code is basically portable technology in java and that is the reason Jini is also very much portable it follows the object oriented paradigm.

(Refer Slide Time: 18:54)



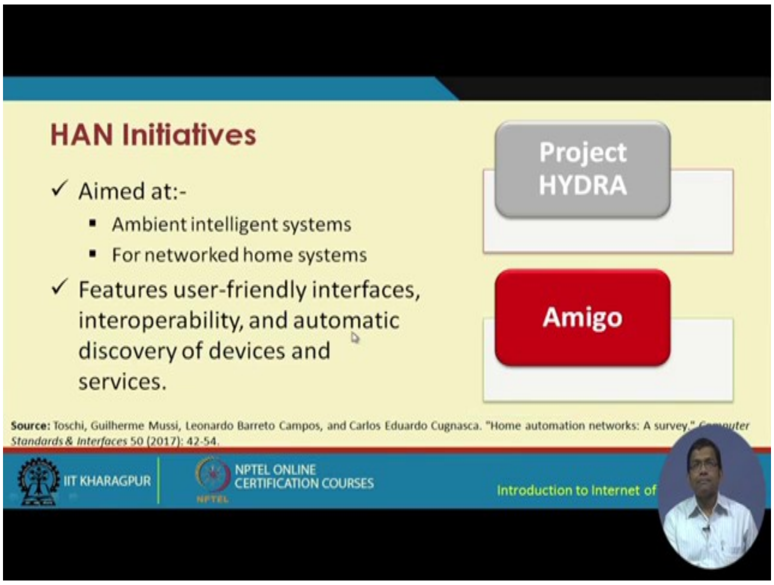
In terms of the initiatives there is that HYDRA project which is about some middle ware for embedded intelligent systems. So, that middle ware was you know was proposed a for a use in IoT kind of environments, where there are embedded intelligent systems or intelligent devices. It connects a service oriented architecture network, the connected devices may have limited resources low processing power memory or energy consumption. Here in HYDRA each device has an embedded HYDRA client which acts as a proxy between the device and the middle ware.

(Refer Slide Time: 19:33)



So, in the HYDRA protocol stack there are these different there are different layers. We have at the very bottom, we have the physical layer you know. Having Bluetooth ZigBee wireless local area networks and so on top we have the operating system comprising of TinyOS windows etcetera. So, TinyOS is an operating system of window as of sensors. So, it is commonly used along with the sensors. So, TinyOS operating system then we have the HYDRA middleware and then we have this applications. In the HYDRA middle ware we have this application elements and the device elements and they basically handset with respect to this different three layers, the network layer the service layer and the semantic layer and there is a vertically cutting across security layer in HYDRA.

(Refer Slide Time: 20:29)



So, this is how the overall HYDRA protocol stack looks like. And then comes the other you know architecture which is the Amigo architecture sorry, Amigo initiative not architecture the Amigo initiative which is aimed at ambient intelligence systems for networked home environments. Amigo basically features user friendly interfaces it takes care of interoperability and also the issues of automatic discovery of devices and services, which are very important in IoT environments particularly when we are talking about home area networks, home users and home you know smart homes.

So, with this we come to an end of this lecture. Specifically focusing on smart homes, we have seen the different protocols that are used in smart homes, the different architectures of smart homes and also the different initiatives the HYDRA, and the Amigo initiatives that use that that are that have that these initiatives are therefore building smart homes.

Thank you.

Introduction to Internet of Things

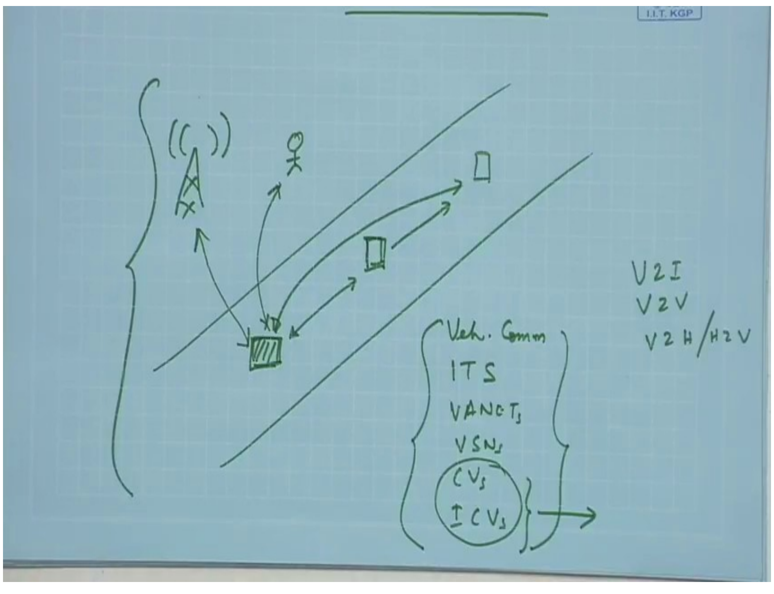
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 49
Connected Vehicles-I

Now, we start a new lecture which is on connected vehicles. So, connected vehicles has become very popular in the recent years. There is a lot of research that is going on building connected vehicles for good reasons, what are these different reasons? So, stand alone vehicles embedded with embedded with different sensors has been there since several years now if not decades. So, you know these standalone different vehicles you know we all are using different vehicles and these have different embedded sensors embedded systems and so on.

But in connected vehicles actually we are talking about how we can make communication between different vehicles possible. So, what kind of communications? Communication between a vehicle one vehicle with another vehicle. Communication between a vehicle and a pedestrian user or another user who is not there in the vehicle, and the roadside infrastructure or the existing infrastructure in a city. So, all of these different possibilities are there in a connected vehicle.

(Refer Slide Time: 01:37)

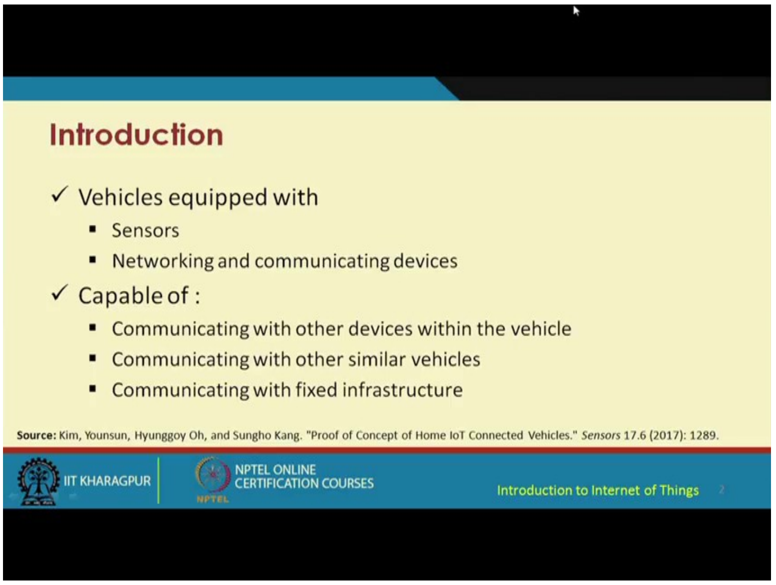


So, let us look at this particular example. So, let us say that we have. So, we are talking about a scenario to motivate why connected vehicle connected vehicles are required. So, let us say that we have these different vehicles on the road. So, in a every vehicle has it is own different sensors and it can even be feeded with more sensors more communication equipment and so on even further it can be done. So, if we talk about a single vehicle in a connected vehicle scenario these vehicle could be talking to the immediate next vehicle the neighbor vehicle. This vehicle could be talking to this one may be with the either directly or with the help of some intermediate vehicle which is there in it is neighborhood this vehicle could be talking to a roadside person you know.

So, this connection flow you know this communication flow might be possible or there could be these different existing communication infrastructure with which this information exchange may also happen. So, you can have V2I, V2V vehicle to infrastructure vehicle to vehicle communication, vehicle to human or even human to vehicle. And when we are talking about human we are talking about the humans who are not in the vehicle who are on the road side. So, all these things are made possible in the connected vehicles. And there is lot of; you know, if we look at the history there has been lot of you know, at least a decade or decade and a half there has been lot of research on vehicular communication and intelligent transportation systems, vehicular ad hoc networks, VANOTs vehicular sensor networks.

Then came this connected vehicles, then came the; you know intelligent connected vehicles. All of these you know in different forms have been around, but the different services this different service improvements that can be made possible in people are talking about in the context of connected vehicles and you know, and this intelligent connected vehicles.

(Refer Slide Time: 04:30)



So, let us look at some of this basics which will help in building this connected vehicles. So, in connected vehicles we have the vehicles that are equipped with different sensors, networking and communication infrastructure different devices, or by you know intra vehicle communication. So, so remember 1 thing couple of things you know. So, what is going to happen is in a connected vehicles scenario number 1, it would be possible to communicate with the different devices inside a single vehicle number 1, number 2 is between different vehicles from a vehicle to the roadside infrastructure or a fixed infrastructure; that means, a non mobile infrastructure.

(Refer Slide Time: 05:17)

So, all these different types of communication are going to happen in a connected vehicles scenario. So, issues such as security privacies, scalability, reliability, quality of service and on top the lack of any singular global standard for connectivity, are some of the challenges that are facing the building of connected vehicles. So, if you are interested you know. So, this particular paper that is reference over here prove a concept of home IoT connected vehicles this paper you can go through this basically gives a good account of the different issues surrounding building of connected vehicles at present.

So, this is a recent paper that was published in 2017 in the sensors journal. So, the different challenges for example, security. Security is very important because you know. So, you are opening up with the help of wireless and with the help of these different vehicles plying all around in the city, yes you are opening up to lot of vulnerabilities at their your opening up you adding to the vulnerabilities and additionally privacy is also very important, because the vehicular data plying all across different people can get you know access to that data.

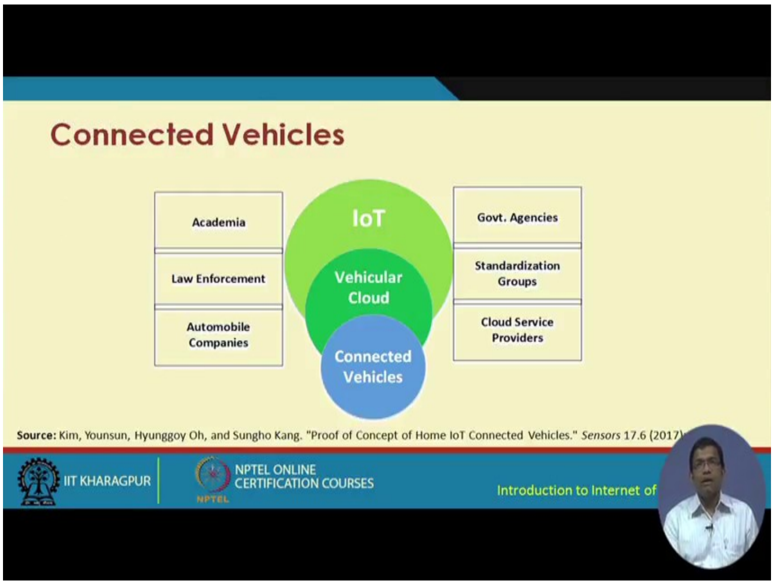
So, privacy of the data from different vehicles is very important, you know why privacy is important let us say, that if the data is leaked for one reason or another let us say that there is someone. So, I am driving and I am in a connected vehicle kind of environment, and from my vehicle the data is sent to another vehicle which is a trusted one by me. But in between the data is leaked and that data is made accessible to somebody else. So, in that case what is going to happen is the the intruder or the malicious person or the entity which gets access to this data which was not intended for it.

So, if that entity gets access to the data they will know that where I am going to for a for example, where this vehicle is going to, and that could be risky that could be even a security threat a safety threat. Because you know not only safety threat or security threat to the vehicle itself, but also to the people who are inside like for example, if I am the user of the car if I am the driver of the car, and if somebody gets access to this kind of information even my safety my security is also at risk.

Scalability is a huge challenge, you are talking about an environment where there is lot of mobility, large number of devices coming in going out of the cities and you have to have some kind of a registry about, who are the home users home vehicles who are which vehicles are the foreign vehicles, and some kind of pricings some kind of keeping track of all these mobility etcetera, etcetera, yes. These are going to be there and at any time anybody from outside can be coming into the cities people can we know the vehicles can be going out of the city and you know it is a highly challenging scenario. So, lot of issues of scalability you know more vehicles being added large number of vehicles being added at in peak hours it will large number of vehicles could be added.

So, scalability issues are there upscale even downscaling also. You know if you think it will be deep you will be able to understand that downscaling issues are also there. Then you have the reliability issues with respect to the reliable communication being possible in this kind of environment quality of service lack of global standards.

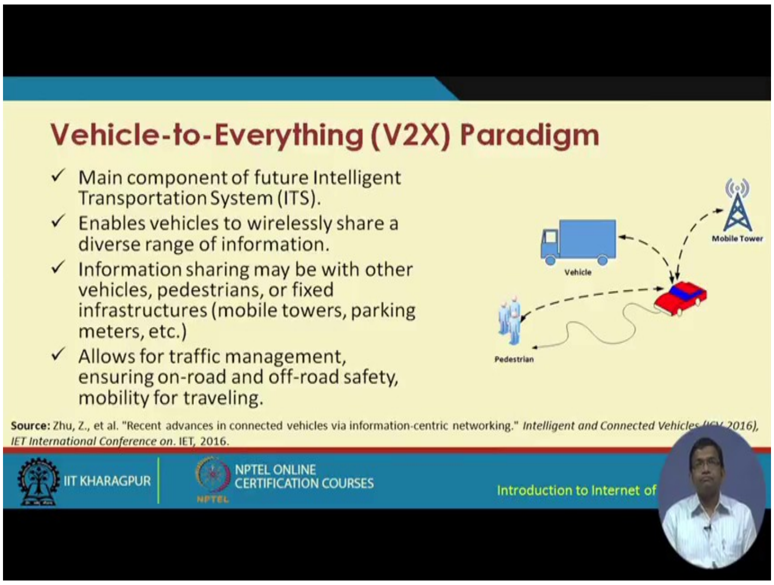
(Refer Slide Time: 08:57)



So, in a connected vehicle connected vehicles are very good as we have seen there are lot of different interesting use cases usefulness of connected vehicles then we have the vehicular cloud. In a vehicular cloud what is going to happen is these connected vehicles are going to send all these data these data are going to go to the cloud, from the cloud lot of you know analytics are going to be performed are you know the data the analytics data are going to made available to the respective stake holders and so on.

So, all these connected vehicles is part you can conceptualize connected vehicles in a as part of the vehicular cloud and vehicular cloud, and connected vehicles as part of the IoT. So, these are like enablers of internet of things. So, the different users and the stake holders of connected vehicles include academia, law enforcement bodies like police you know judiciary etcetera law enforcement bodies, automobile companies, government agencies standardization groups cloud service providers. So, these are the different stakeholder's different actors of connected vehicles.

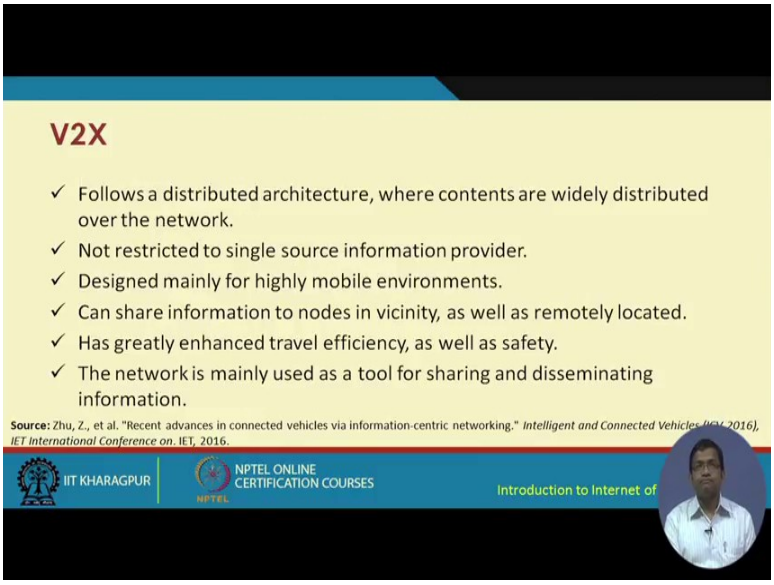
(Refer Slide Time: 10:08)



So, typically in a connected vehicle the most popular concept is the concept of vehicle to everything paradigm. So, V2X vehicle to everything V2X. So, V2X is basically part of the future it is intelligent transportation system, which enables vehicles to wirelessly share a diverse range of information, and the information sharing may be with other vehicles pedestrians or fixed infrastructures, such as mobile towers parking meters and so on. So, this is what at the very outset of this particular lecture I was also telling you that, this vehicle can communicate with the pedestrians on the way with the other vehicles on the road or with fixed infrastructures such as mobile towers or parking meters and so on.

So, this basically allows for graphic management ensuring on road and off road safety mobility for traveling and so on.

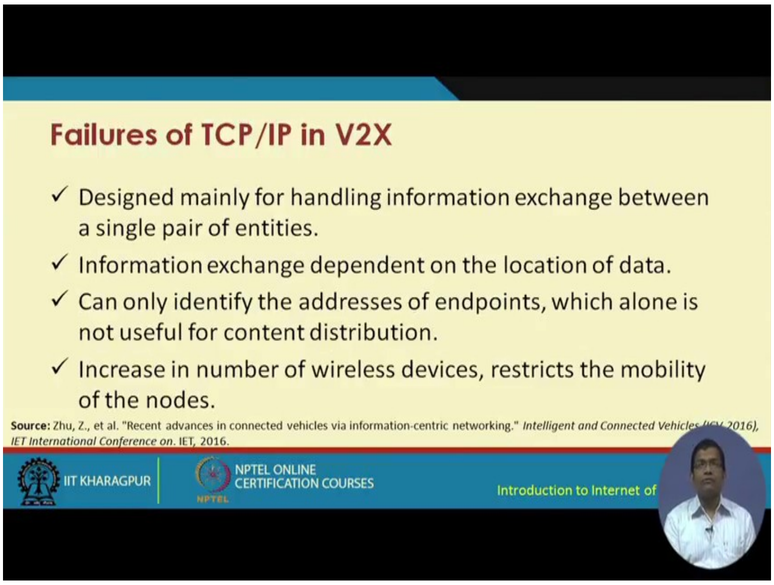
(Refer Slide Time: 11:20)



So, I do not need to elaborate on these, but this is quite evident and understandable the you know how this V2X is going to be useful. V2X basically follows a distributed architecture where the contents are widely distributed over the network. So, content based communication So, I will talk about that it is a content centric V2X basically uses content centric and not really the TCP/IP kind of you know information dissemination approach. It is not restricted to single source information provider it is designed mainly for highly mobile environments and vehicular environments are highly mobile environments. It is designed mainly for such kind of environments. The vehicles can share information to notes in the vicinity, as well as to remotely located notes.

So, here you know V2X has greatly enhanced the travel efficiency, the safety, security and so on. The network in V2X is mainly used as a tool for sharing and dissemination of information. And that is not something very new because ultimately, what is going to happen is after this information is collected from these different sensors. If the dissemination has to happen with some communication medium and typically it is a wireless communication medium, where there is a network and the network basically helps in the dissemination of information.

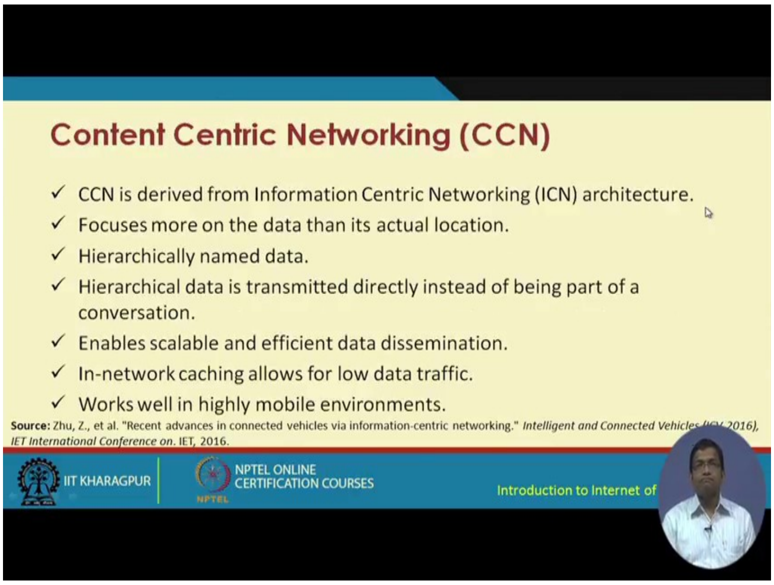
(Refer Slide Time: 12:30)



Now, what do we already have in terms of implementation of V2X. We already have our internet runs on TCP/IP. So, you know if we try to implement V2X on top of TCP/IP this is what is going to happen. So, you know it is going to fail, why? So, TCP/IP is designed mainly for handling information between single pair of entities. There is a source there is a destination you know and between these source and destination whether they are you know in direct range of each other or they are far apart, TCP/IP will have different solutions by which to send the data from one point to another.

So, the location the information exchange in TCP/IP is dependent on the location of data. So, you know there is a specific data base located at some place. So, from that point the data has to be fetched. So, from this particular data base in a particular server the data has to be fetched. So, this is like dependent on the location of the data can only identify TCP/IP can only identify the address of the endpoints which alone is not useful for content distribution, and that that content distribution is what is required in the cases of connected vehicles in V2X. And there is increase in the number of wireless devices which basically restricts the mobility of the different nodes.

(Refer Slide Time: 14:01)

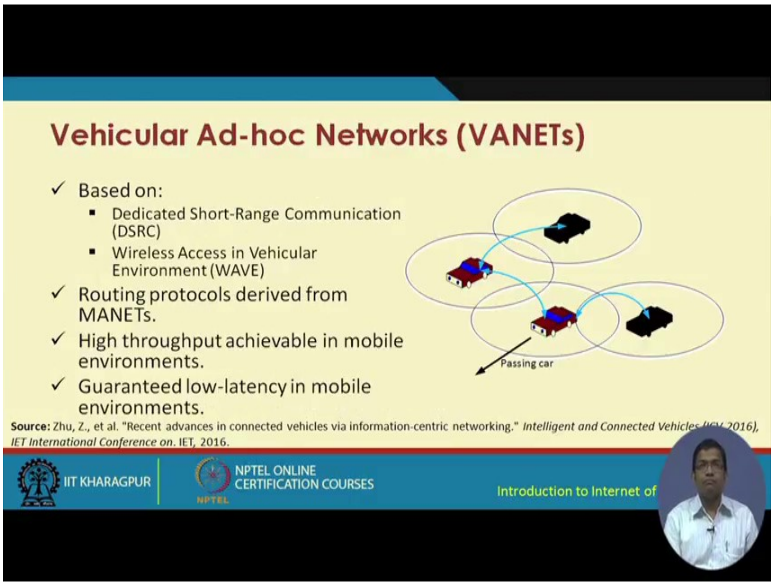


In content centric networking, you know it is basically conceptually has similarities to the popular information centric networking which focuses on the data than the actual location of the data. So, I need some data, I do not have to say that you know I have to get it from this particular database or this particular source, in content centric networking what is going to happen is, if I need access to a particular data I will be doing some kind of a broadcasting some kind of broadcasting of that particular requirement that query, and whoever has that data is going to send me the data. So, this is how the content centric networking contrast to TCP/IP functions.

So, we have hierarchically name data in content centric network. Hierarchically named data is something like x dot y dot z, you know this kind of hierarchy is followed. Something like you know my data would be something like mister dot sudeep dot age dot something. So, it is hierarchically named you know very similar I am giving you just an analogous example not the exact one. So, hierarchical data is transmitted directly instead of being part of the conversation. So, the conversation would be like the entire thing this dot this dot this dot this that becomes the entire conversation.

So, this is the how the hierarchical data is organized. So, I do not need to really if I need to get access to a particular part of that hierarchical data, I do not need to access the entire conversation. I can simply pick up from that particular part. So, it enables scalable and efficient data dissemination in network caching allows for low data traffic, it works well in highly mobile environments. So, in highly mobile environments you do not really need to keep track of the source the destination and the intermediate hops in between and how the data is going to float all around. So, you have a highly ad hoc kind of scenario and content centric networking, I basically the following this kind of philosophy that I just explained is very much useful.

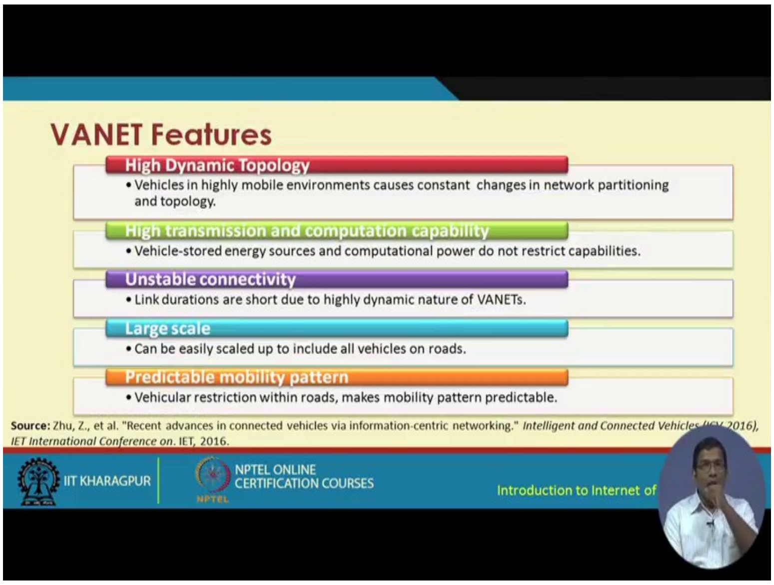
(Refer Slide Time: 16:17)



So, we are talking about vehicular ad hoc networks which is based on dedicated short range communication DSRC. And the wave protocol which is wireless access in vehicular environments the wave protocol.

So, these are the 2 you know very well known protocols that are used in vehicular ad hoc network, the DSRC protocol and the wave protocol. So, routing protocols are derived from the MANETs and, but here actually you have different types of characteristics than MANETs you know it is a derivation all these routing protocols for MANETs are basically derivations over from MANETs, but again they are different by taking the typical features of vehicular networks how the vehicles fly ply on the road on highways and so on are taking in account and how they communicate with the roadside infrastructure these are actually taken into account.

(Refer Slide Time: 17:24)

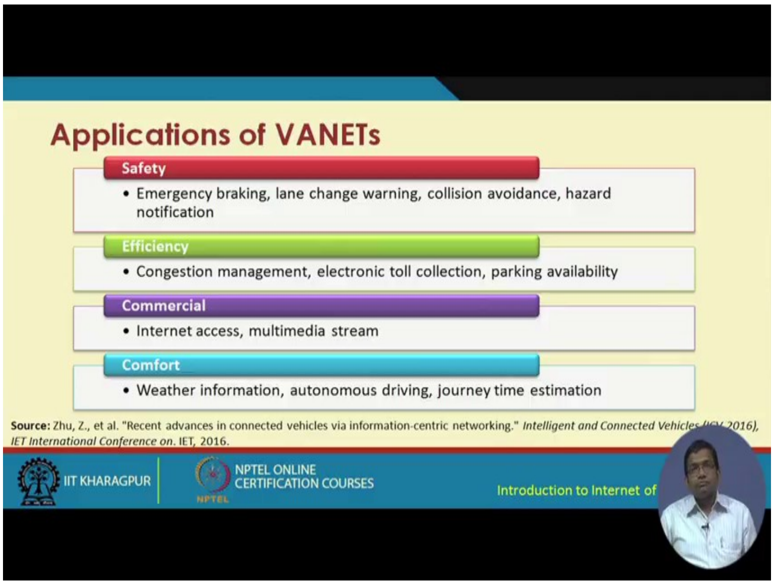


So, high through put is achievable in mobile environments using VANETs. And also low latency can be guaranteed in mobile environments in VANETs. VANET basically has different features. It has a highly dynamic topology, where the vehicle vehicles are highly mobile and they are changing their position. And the network topologies come continuously the brake and they make continuously. So, you have a highly dynamic breaking making kind of topology which is done continuously.

So, high transmission and computation capability the vehicles store energy sources sorry, the vehicles stored energy sources and the computational sources are used to draw power. And that basically is much higher compared to the stand alone IoT devices. And that is why there is no not much restriction there is not much of you know restriction on the energy source energy use and computational power and so on, because the vehicular you know energy sources and the computational energy sources in the vehicles these are quite high.

Unstable connectivity in VANETs link durations are short due to high dynamic feature of the these networks. These networks can be scaled up very easily to include different other vehicles on the road they can join these particular network without effecting the throughput in a very significant manner. The predictable mobility patterns can be can be achieved in these kind of networks because the vehicles are restricted within the roads you know how the road structure is and that basically restricts the mobility pattern also and these mobility patterns are predictable in these kind of networks. In contrary in MANETs basically in mobile ad hoc networks the mobility is a big issue you do not know.

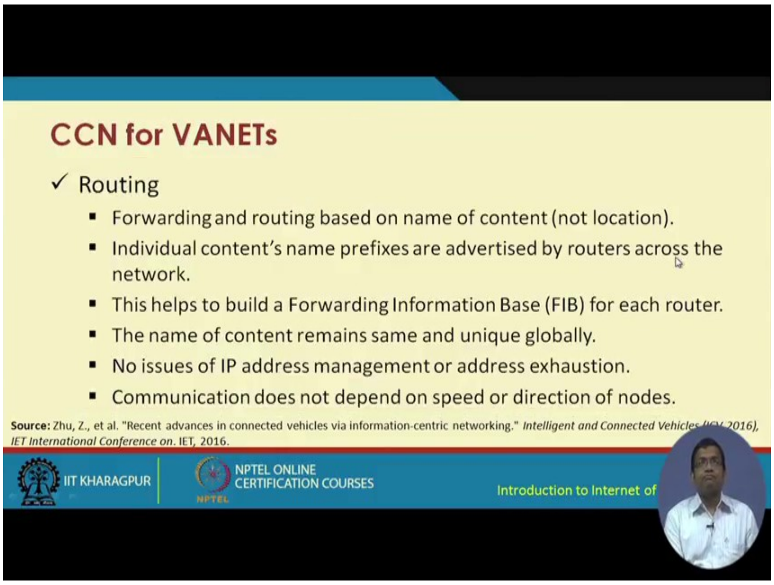
(Refer Slide Time: 19:17)



You know how the vehicles are going to move it is hard to predict the mobility of these different vehicles. Safety issues are there emergency breaking lenge sorry, lane change warning you know collision avoidance hazard notification these are the different safety applications of VANETs. Efficiency with respect to congestion management electronic toll collection parking availability these are again different attractive applications of VANETs.

Third type of applications are commercial applications for example, making a having internet access multimedia streaming all these possible on the road when you are on the road in the car in the vehicle. So, these are possible in VANETs, then different other comfort comforts with respect to getting whether information autonomous driving journey time estimation these are all made possible with the help of implementation of VANETs.

(Refer Slide Time: 20:05)

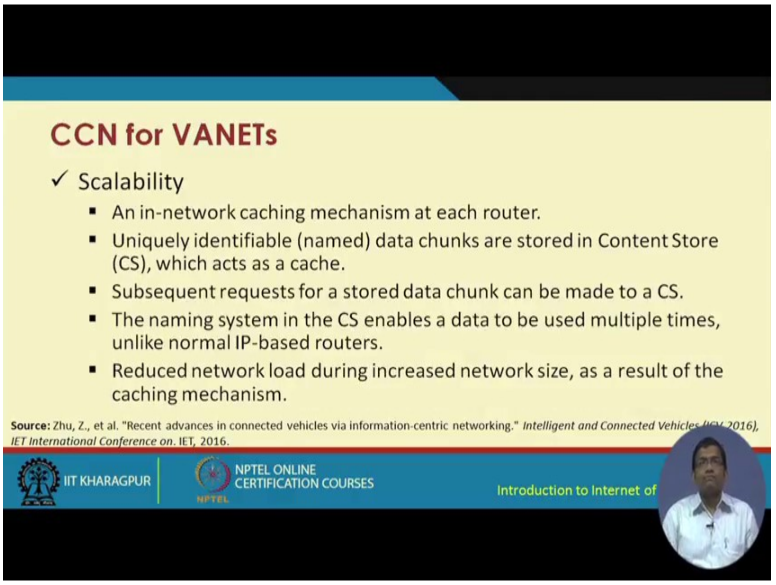


Then CCN the content centric networking that was telling you before, how it is implemented in VANETs?

So, some sort of routing is done, but this kind of routing is bit different. So, forwarding and routing is best here on name of the content not the location of the content. The name of the content is used for routing. The individual contents name prefixes are advertised by the routers across the network these helps to build a forwarding information base for each router. The name of the content remains the same and unique globally, and there is no issue of IP address management or address exhaustion. The communication does not depend on the speed or direction of the different nodes.

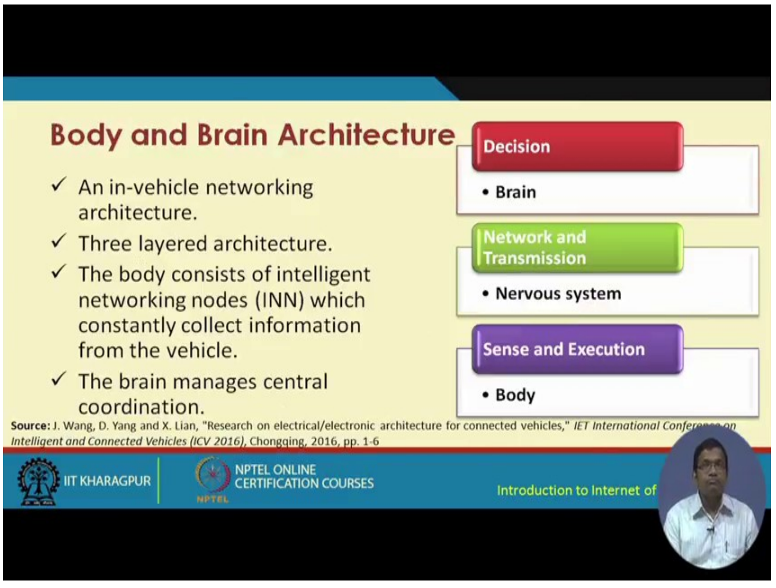
So, these are the different issues. So, the main thing that he have to has to be remembered is there is indeed the same way as we have routing tables in the case of TCP/IP based routing. Here we also have a very similar kind of thing which we have the forwarding information base at each of these different routers. But here the routing is done not on the basis of the location of the content, but on the basis of the name of the contents. So, where this and that name has to be unique. So, this is very important. If the name is not unique then this kind of routing cannot be done. So, in content centric routing the name also has to be unique in the network.

(Refer Slide Time: 21:25)



Scalability and in networking caching mechanism at each outer is implemented, which uniquely identifies the named data chunks. And these data chunks are stored in something known as the content store which acts as a cash. Subsequent requests for a stored data chuck can be made to a content store. The naming system in the content store enables a data to be used multiple times unlike in the case of normal IP based routers as we discuss before. And the there is reduced network load during the increase network size as a result of the caching mechanism.

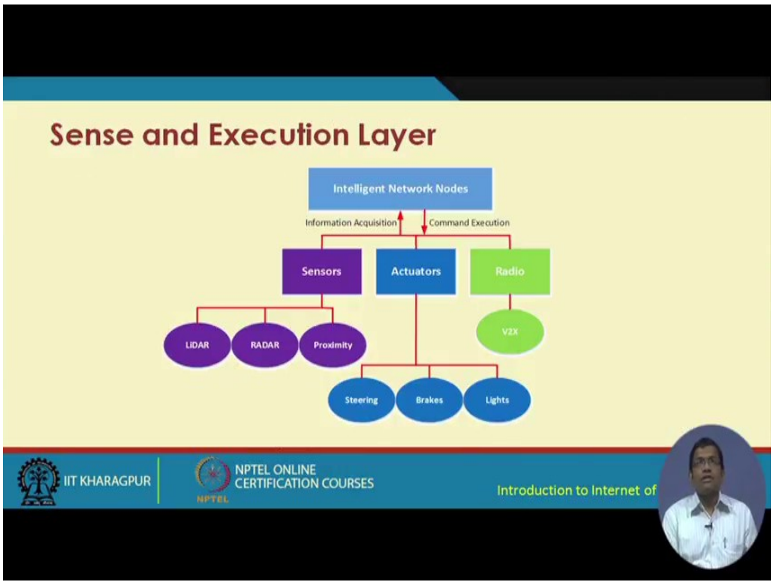
(Refer Slide Time: 22:00)



Now, will talk about a very interesting architecture which is called the body and brain architecture that has been proposed for the connected vehicles. So, it is an in vehicle networking architecture, which has very similar kind of you know architecture as the human body. As in the human body we have the body the code body having the skeleton the muscles the you know tissues the organs and this you know. So, that kind of structure, but on top you we also have the nervous system the brain etcetera and you know similar kind of thing is done in this case as well.

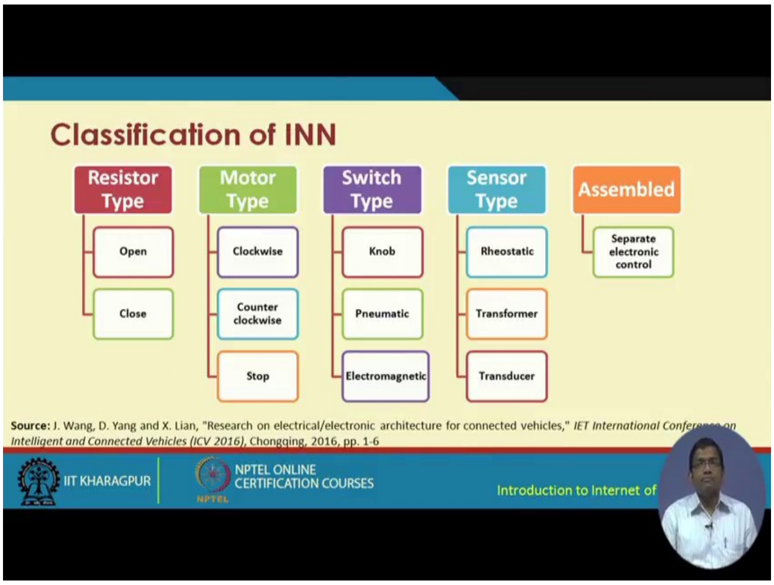
So, here we have a 3 layered architecture, there is that sense and execution layer then we have the network and transmission layer, and then we have the decision layer. So, the sense and execution layer is very similar to the body of a human body, the network and transmission layer is very similar to the nervous system of the human body. And the decision layer is very, very similar to the brain of the human body. So, there are 3 layers the body consists of intelligent networking nodes, which constantly collect information from the vehicle and the then the brain basically manages the central coordination.

(Refer Slide Time: 23:13)



So, let us first look at the sense and execution layer. In the sense and execution layer we have these intelligent nodes. With the help of sensors actuators different radios the information is acquired with the help of different other devices like, LDAR, RADAR proximity sensors and different other sensors plus actuators such as steering brakes lights etcetera the information is acquired. And the commands are executed through the through the actuators or through the different radio mechanisms. These are made available and this is how the sense and execution layer looks like in a connected vehicle scenario.

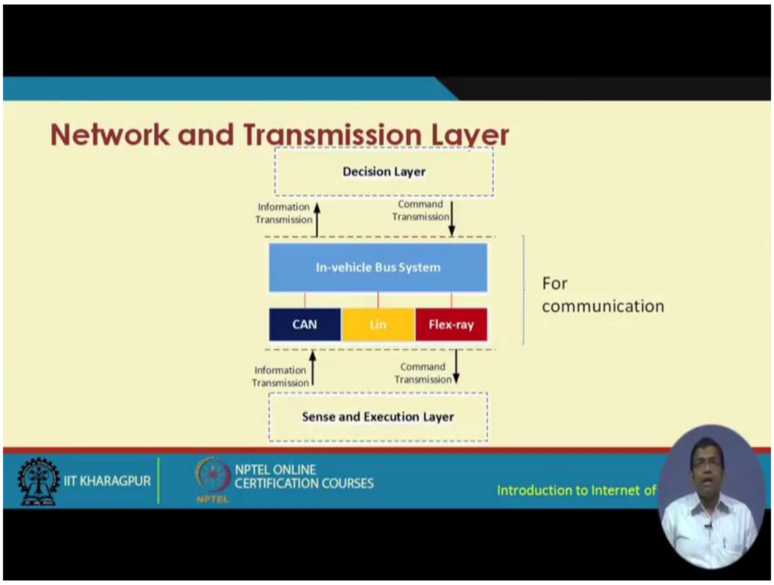
(Refer Slide Time: 23:54)



The intelligent networking nodes which has intelligence with implemented with the help of software you know different software. There are there are different types of nodes, one is the registered type nodes which can be opened or closed. There is a motor type nodes which basically are you know the motors can be moving clock wise counter clockwise or the motor can be stopped.

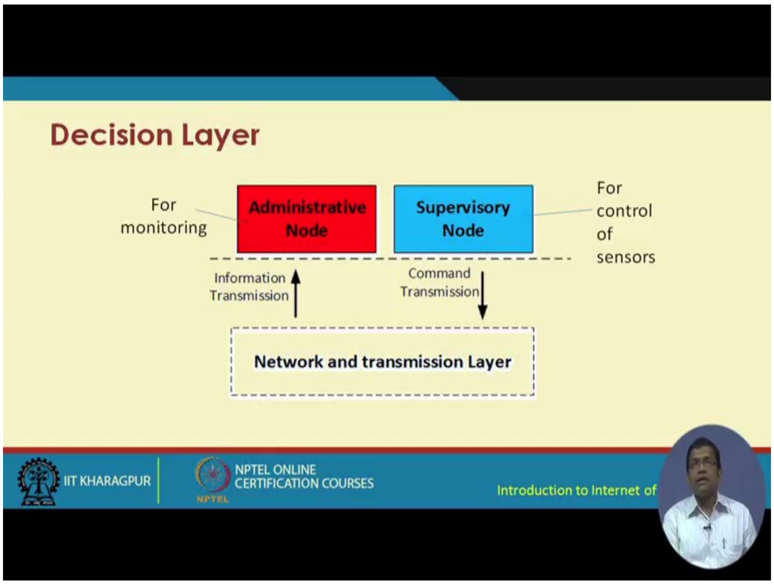
Switch type nodes switches can be of different types in a intelligent net node in a intelligent vehicle, a it could be the switches could be a nob. A pneumatic switch or an electromagnetic switch the sensors could be rheostatic switch rheostatic sensors rheostats we already know what a rheostat is. So, rheostatic sensors or transformers or transducers or they could be assembled nodes comprising of different separate electronic controls.

(Refer Slide Time: 24:45)



The network and transmission layer looks like this. So, you know this is basically you know this network and transmission layer, and as this name suggest we have for communication this is used primarily for communication. The sense and execution layer on the very bottom and on the top we have the decision layer and in between we have this communication in communication layer. Where there is a in vehicle bus system bus means that it is a collection of ware. So, we have the in bus in vehicle you know bus system and there are different you know proprietary and to open source components for communications. So, all these together will comprise the network and transmission layer which is used for communication. And that basically sit is in between the sensing and execution layer and the decision layer that we talk about now.

(Refer Slide Time: 25:31)



In the decision layer which sit is on top of the network and transmission layer. The information is transmitted for monitoring to the administrative node and for control of the sensor nodes the supervisory node basically sends the command to the network and the transmission layer, for further sending to the actuators underneath. So, with this we come to an end of this particular lecture of connected vehicles. We have talked about the first part of the connected vehicles the different issues with connected vehicles why connected vehicles are very important, and the different associated terminologies for example, vehicular communication we also spoke about different other allied terms such as vehicular ad hoc networks vehicular sensor networks.

Then intelligent vehicular systems then internet sorry, connected vehicles and intelligent connected vehicles ICVs; so, these are the different things that we spoke about in the next lecture we will talk about few other different issues with connected vehicles, and how those issues can be resolved.

Thank you.

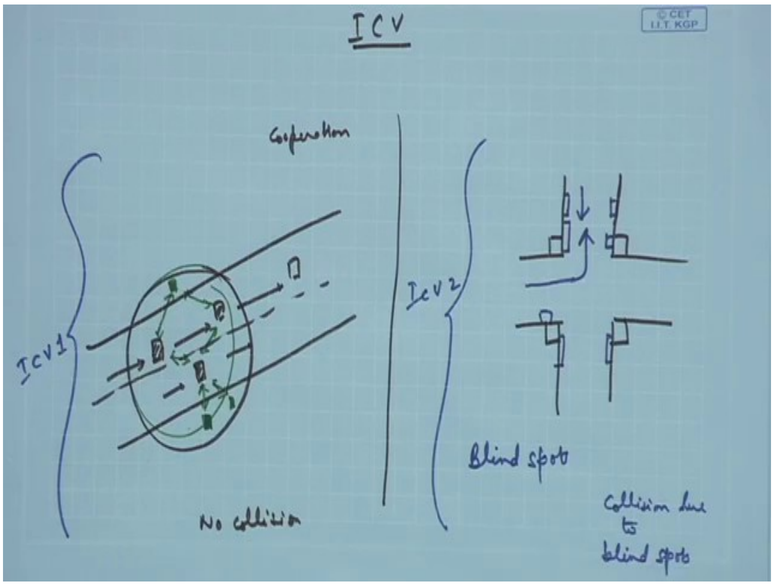
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 50
Connected Vehicles – II

So, now we are going to continue with our discussion about connected vehicles in the second part of the lecture on connected vehicles we are going to talk about the intelligent connected vehicles. So, intelligence means that it comes with lot of implementation of different types of software different things can be performed intelligently different inferences predictions etcetera, etcetera based on the data that is obtained either from the hardware; that is embedded or from the historical data that is collected from the from the site from the different vehicles on the site and what people have you know send the different vehicles have sent in the past.

So, based on that historical data, different types of inferences can be done so that intelligent decision making can be done. So, here basically you know when we are talking about intelligence of any kind we are talking about the use of software. So, intelligent software the software basically uses different types of analytics different types of machine learning methodologies and so, these that will be applicable on top of the data that is collected and the data that is collected is from the different sensors and these sensors the actuators and so on; get together are the down devices the base devices the physical devices which basically help in the procurement of this information.

(Refer Slide Time: 01:56)



So, let us consider a particular scenario like this for intelligent connected vehicles let us consider 2 scenarios in the first scenario we have a road on which there is a vehicle and all these different vehicles are also moving on the road and then there is a passerby. So, all these different vehicles and we are considering a very simple configuration like this. So, what happens is when this vehicle these vehicles are moving on the road and let us say that this is the lane and there is a vehicle which is trying to pass this particular vehicle. So, you know it might be possible to come up with a scheme through which cooperatively these vehicles will help each other. So, that there is no collision between them.

So, there has; these has to be made possible with the help of enforcement of or enforcement or implementation of some scheme which is based on cooperation between the different entities cooperation between the different entities. So, in this particular example we were talking about this vehicle this vehicle and this vehicle cooperating with each other in order to avoid collision and that would be made possible with the help of the data that is collected from the individual sensors in these different vehicles from the from the information that is obtained from the different roadside units from the different let me denote the road side units as solid blocks.

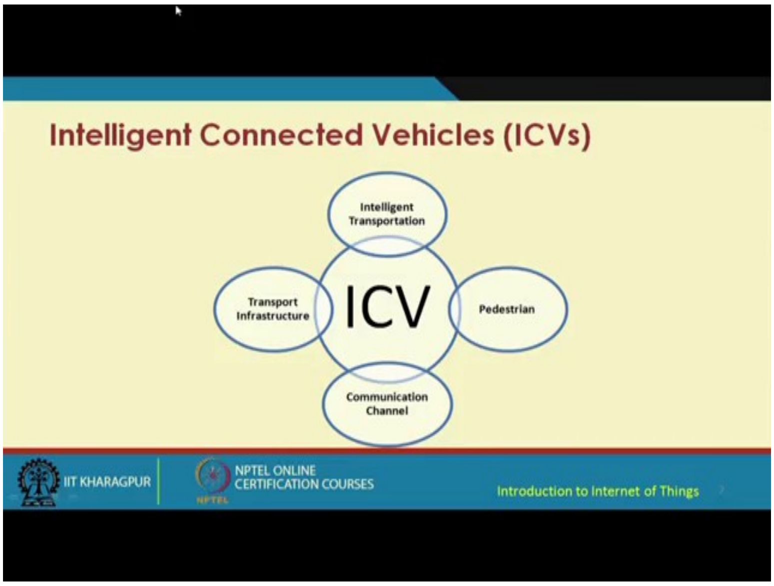
So, from this from this data from this data this data and also the data like this. So, all these information would be collected together there would be some kind of a cooperation enforcement scheme may be using cooperative game theoretic approaches or something like that 2 come up with schemes or to come up with decisions on driving. So, that these vehicles can keep safe distance from each other and they do not collide. So, this is one scenario.

Another one could be let us consider another example where we have let us say it is not a highway, but you know it is a city intersection like this and typically as you know that in the intersections you have different blind spots maybe due to different buildings in the corners or maybe there is a parked let us say that here we have you know these are the different buildings in the corners of an intersection or maybe there is some parked vehicle over here these are the different parked vehicles.

So, what might so happen is these vehicles these parked vehicles they often create blind spots blind spots and due to blind spots what might happen is a vehicle that is coming from this place and if they want to turn this way and another vehicle that is coming from this way they might collide because these vehicle cannot see this one this one cannot see these and they might collide. So, similar kind of other types of scenarios can also be you know thought of thought of involving blind spots and so how do we avoid this thing.

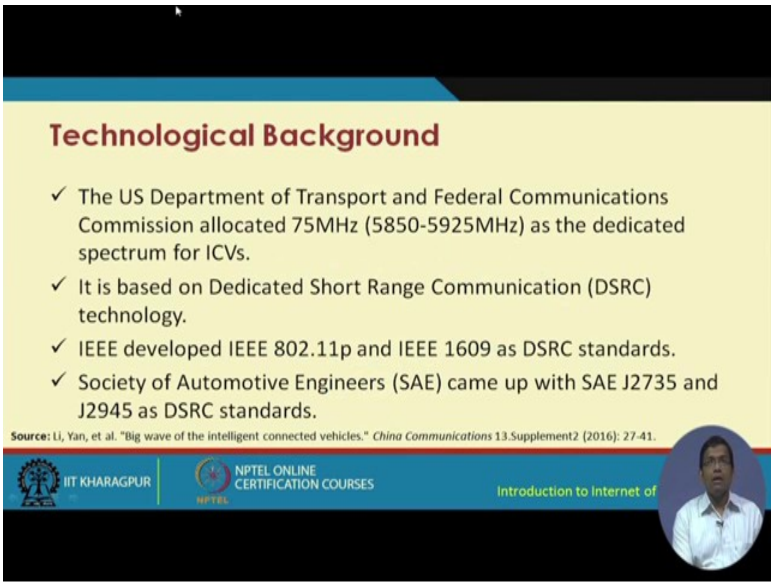
So, here also these might happen is again there is collision due to blind spots and intelligent connected vehicles can help in this scenario as well. So, these can cooperate. So, there other vehicles that are there and the sensors in them like in the case of this particular scenario they all can cooperate with one another in order to help these 2 vehicles. So, that they do not collide with each other. So, we have one scenario of ICV and the other scenario of ICV intelligent connected vehicles. So, let us look ahead and see what is there for us further.

(Refer Slide Time: 06:57)



So, when we talk about intelligent connected vehicles we are talking about intelligent transportation which we have already discussed the different transport infrastructure the communication channel pedestrians all coming together interconnecting them in an intelligent fashion to fulfill certain objectives the different use cases.

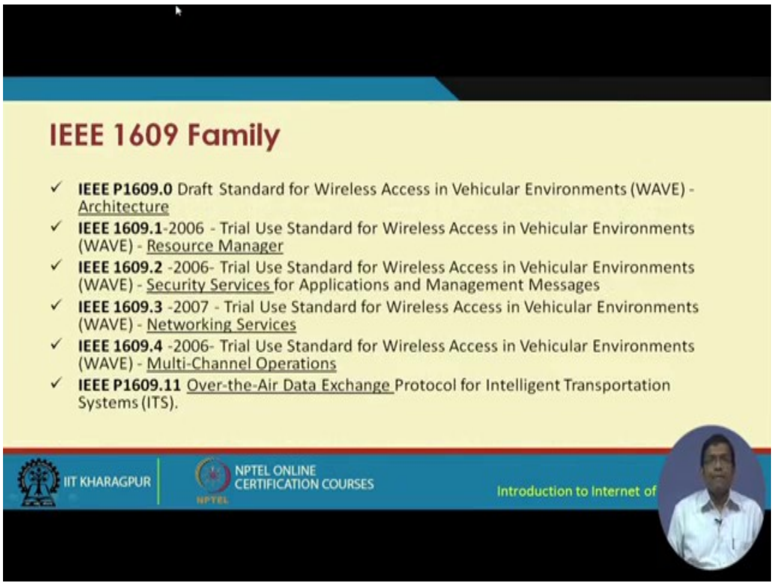
(Refer Slide Time: 07:22)



So, let us look at some technological background about ICV. So, the US department of transport and federal communications commission allocated 75 megahertz in the band 5850-5925 megahertz, so, this 75 megahertz band as the dedicated spectrum for internet intelligent connected vehicles. So, US has already done it. I for ICVs they have a separate allocated 75 megahertz band and these particular thing for ICVs, it is supported by the DSRC technology that we spoke about in the first part of intelligent of the connected vehicle's lecture.

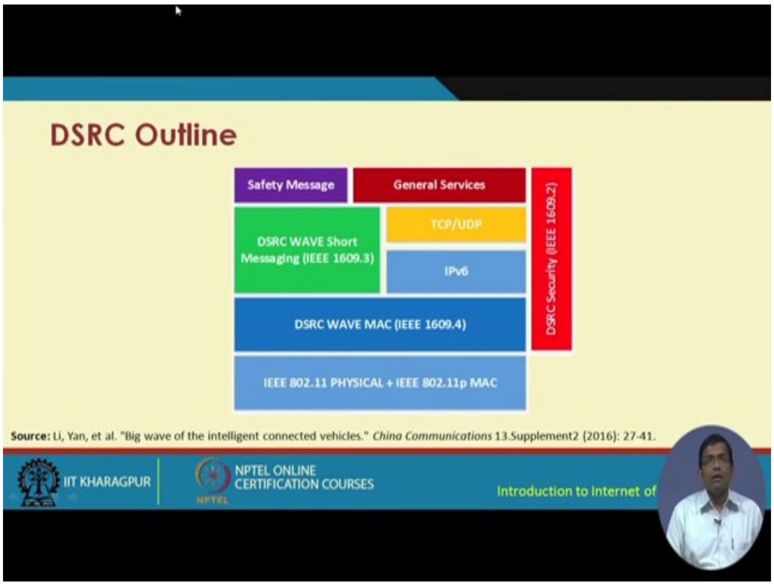
So, in the first part we talked about the 2 types; one is the DSRC communication technology the other one is the wave communication technology. So, basically for this part basically the 75 megahertz communication for ICVs there is that DSRC that is commonly used and IEEE concurrently has also come up with this protocol 802.11p and the IEEE; IEEE 1609 as 2 different standards for DSRC implementation. So, 2 different standards 1 is 802.11p not the simple not the standalone 802.11 protocol the standard. So, p the 11p and 16.0 sorry; 1609 IEEE standards are also used for ICV implementations and the society of automotive engineers came up with the SAE J 2735 and J 29452 different standards by this particular society.

(Refer Slide Time: 09:17)



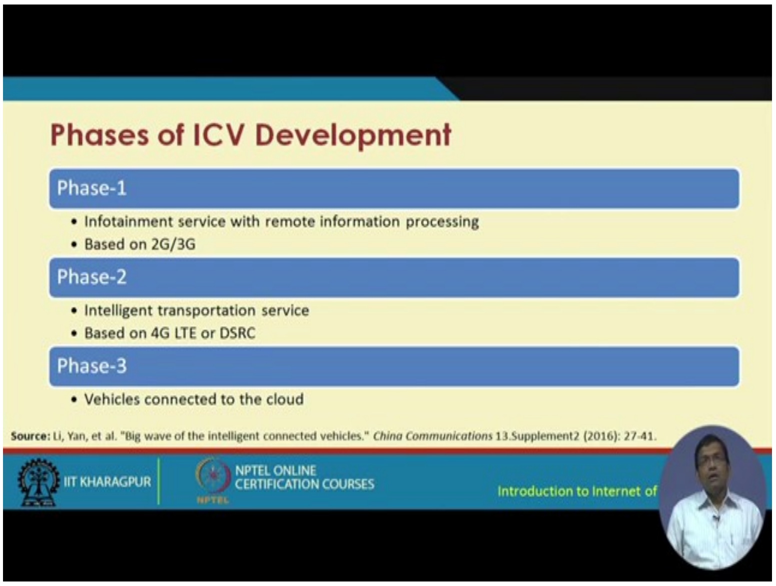
So, 1609 is for automotive connections automotive connections interconnected vehicles. So, these standard and the different drafts I am going to go through. So, P1609.0 this is a draft standard for wave architecture and this wave architecture I already told you before wave protocol. So, the wave architecture is basically drafted in this particular a in this particular document the P1609 draft then the 1609.1-2006; these basically takes about the trial use standard for wave from a resource manager point of view .2-2006 is the trial use standard for wave with security services for applications and management of messages .3-2007 is the trial use standard for wave consisting of different networking services .4-2006 is the trial use standard for wave with multichannel operations and P1609.11 is over the year data exchange protocol for standard transportation systems for intelligent transportation systems the ITS.

(Refer Slide Time: 10:45)



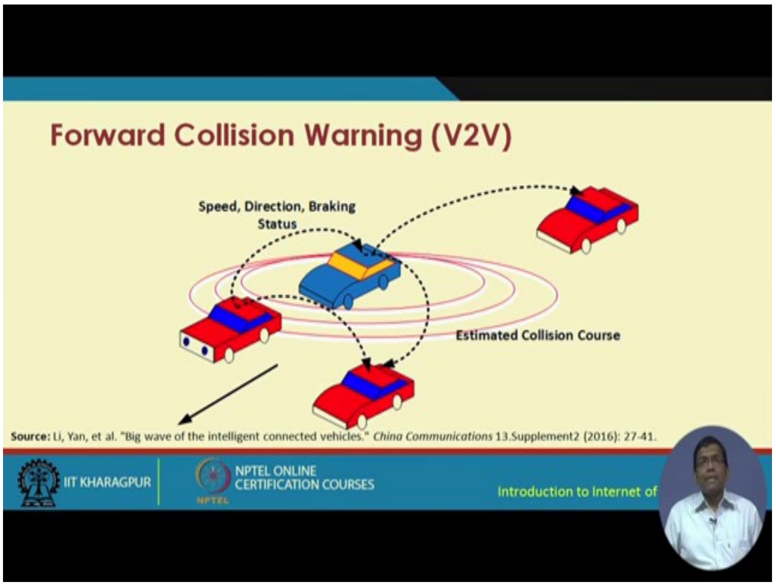
So, DSRC protocol if you look at it looks like this as shown in this particular figure we have at the very bottom the bottom layer is not just the physical. So, it includes the 802.11 physical and the MAC of 802.11p these 2 are at the very bottom then we have the 1609.4 which is the DSRC WAVE MAC and then on top we have the DSRC wave short range messaging protocol 1609.3 and also the regular IPV 6 and TCP IP; TCP UDP as the transport and the different applications such as safety messaging general services etcetera on the very top the security is something that cuts across vertically across all these different layers. So, security is drafted in point 2 IEEE 1609.2.

(Refer Slide Time: 11:53)



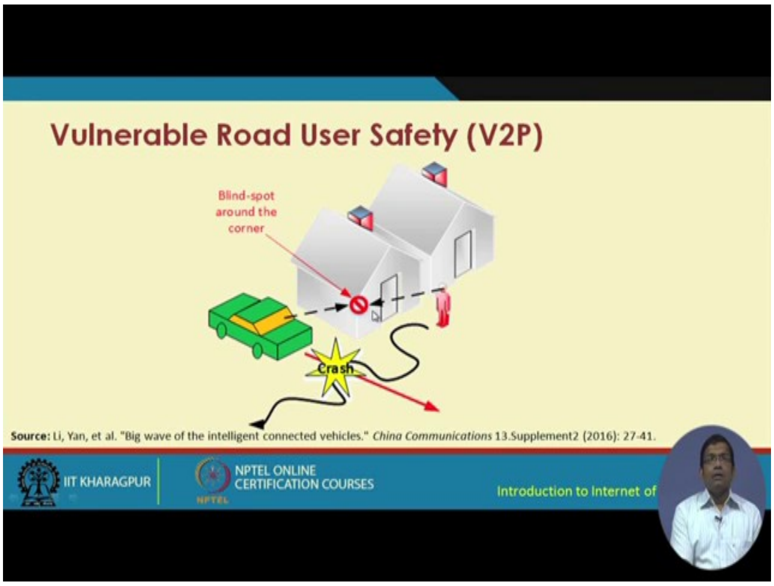
Now, the phases of internet sorry intelligent connected vehicle development in phase one it was considered to have you know facilities for infotainment service availability with remote information processing and that was based on the 2 G, 3 G technology phase 2 basically included 4 G LTE or DSRC and here the focus was on intelligent transportation service and phase 3 basically was to connect all these vehicles to the cloud that was the phase 3.

(Refer Slide Time: 12:34)



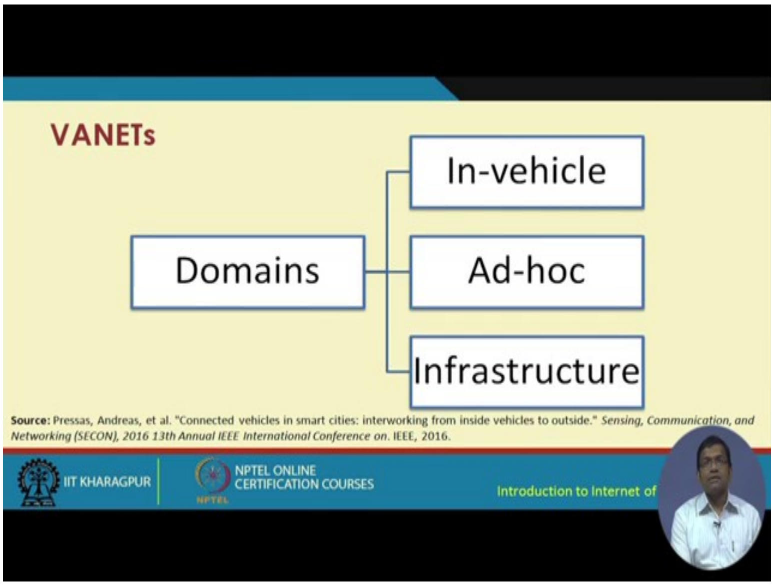
Now, let us look at some ICV scenarios forward collision warning scenario. So, we have these different vehicles which are running on the road we have this vehicle and these 3 different vehicles and this particular vehicle. So, they all would be you know having this information with respect to the speed the direction the breaking status and. So, on and based on these they can cooperatively estimate the collision course you know. So, that they do not collide with each other then this is an example of the existence of blind spot across you know blind spots on the road.

(Refer Slide Time: 13:06)



So, you know in particularly blind spots exist in the corner as I was telling you at the very outset for a different kind of scenario. So, it might. So, happen that a particular vehicle would be coming when there is a human who is trying to pass. So, this vehicle was supposed to come this way this human was supposed to walk on the pedestrian; you know on these pedestrian road. So, when they try to cross there could be a possibility of crash crash between the vehicle and the human who is trying to cross because and this was happening because they were not within line of sight of each other and because of the existence of this particular building on the house on the corner.

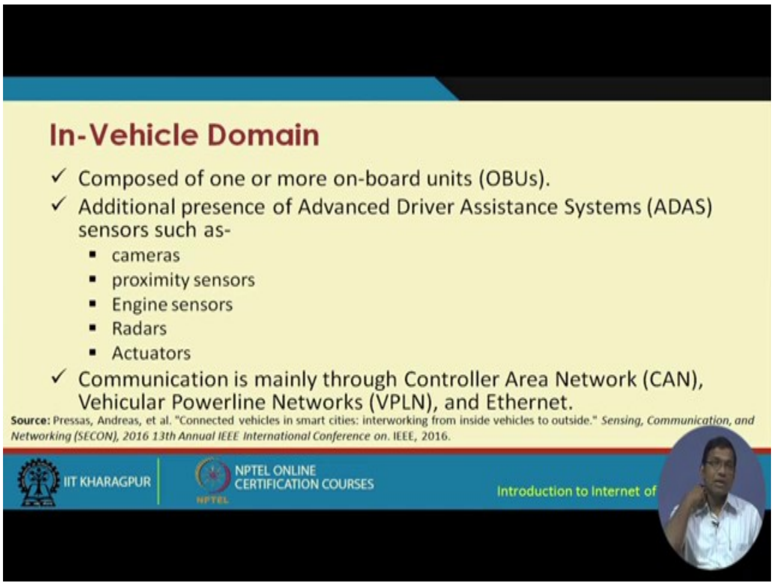
(Refer Slide Time: 14:09)



So, you know. So, taking care of this kind of scenarios these V2P scenarios vulnerable road user safety scenarios was something that was considered in the intelligent connected vehicles vehicular ad-hoc network is at the core of ICVs. So, when we talk about vehicular ad hoc networks we are talking about 3 different types of communications at least number one communication inside the vehicle inside every vehicle there are lot of sensors there are lot of actuators there are different types of other embedded devices there are these different transmitters receivers and so on.

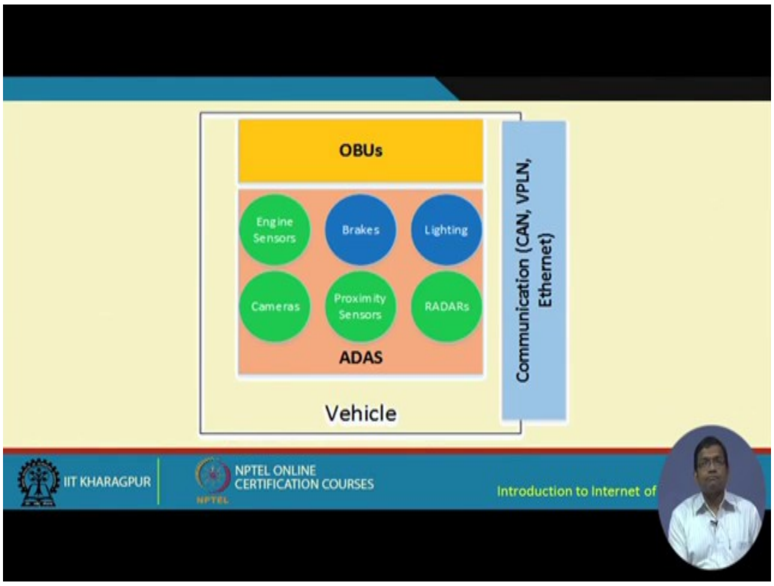
So, in vehicle communication is one, then comes the ad hoc communication ad hoc communication is with without the help of any infrastructure these vehicles would be able to communicate with one another. So, vehicle to vehicle communication may be directly or via some intermediate vehicle which will act as a relay of the messages. So, vehicle to vehicle communication either directly or through relays and the infrastructure based communication may be with the help of road side units or mobile towers and so on.

(Refer Slide Time: 15:18)



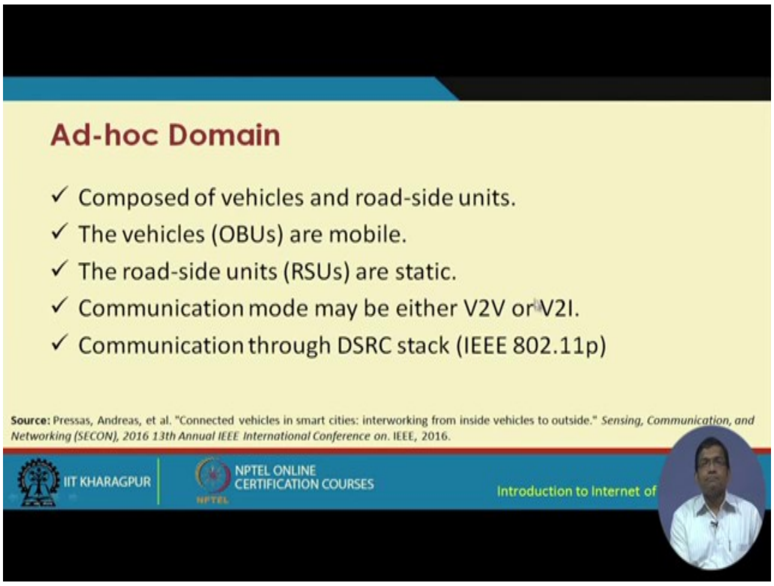
So, these are the 3 different domains of vehicular communication in-vehicle communication ad-hoc communication and infrastructure based communication. So, in vehicle communication for that there are different OBUs the on board units that are basically fixed on the vehicles. So, these vehicles they have each of these vehicles they have one or more OBUs the on-board units they also have something known as the ADAS unit advanced driver assistant system unit which has different sensors such as cameras proximity sensors engine sensors actuators radars and so on, the communication is mainly through controller area network vehicular power line network and the Ethernet. So, these are 3 typical typically used communication equipments communication facilities communication networks that are used.

(Refer Slide Time: 16:15)



So, what we have is something like this; this is the whole vehicle this is the whole vehicle and in the vehicle we have these OBUs the onboard units the ADAS comprising of different sensors engine sensors brakes lighting radars proximity sensors and cameras and these are all connected with each other with the help of different communication technologies like controller area network VPLN and Ethernet.

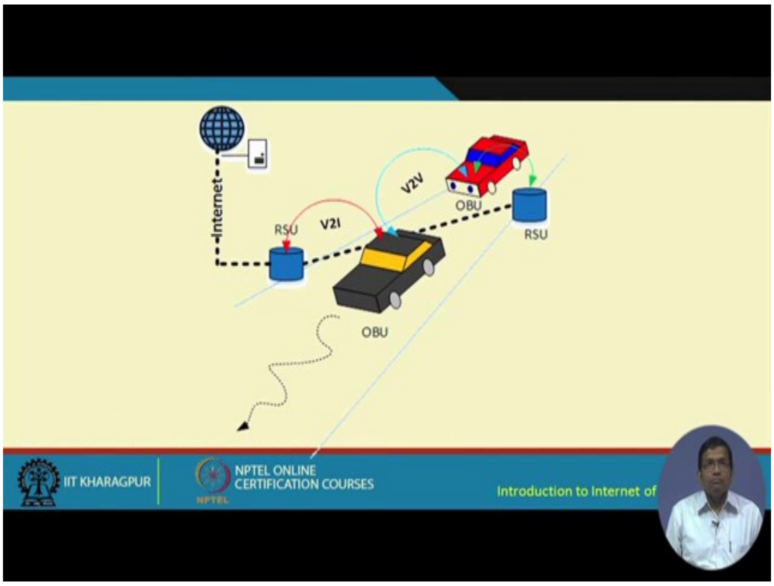
(Refer Slide Time: 16:47)



In the ad hoc domain again we have these OBUs, but we are considering OBUs which are mobile and these vehicles basically can talk to each other and also with the road side units the

RSUs, but these road side units are considered to be static in this particular architecture. So, the communication mode may be either V2V orV2I and the communication is done through the DSRC stack using the 802.11p IEEE standard.

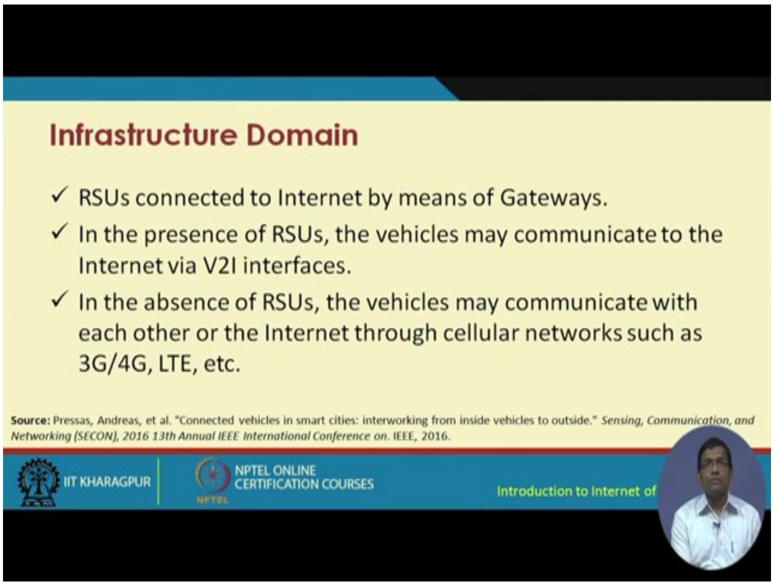
(Refer Slide Time: 17:19)



So, let us consider this particular scenario of these vehicles moving on the roads. So, each of these vehicles they have their own different OBU like this every vehicle has one or more OBUs and these RSUs road road side units and it is possible to have different types of communication either vehicle to vehicle communication like this or from vehicle to RSU communication vehicle to RSU communication. So, this is V2V and this is V2I vehicle to infrastructure because RSUs are fixed infrastructure on the road sides.

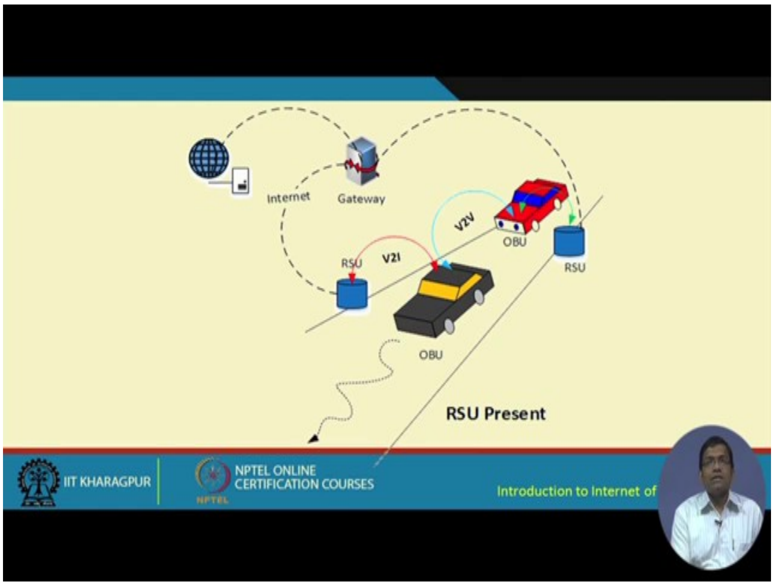
So, that is the reason this is known as V 2 I infrastructure and it is also considered in the case of VANETs in the case of intelligent connected vehicles is that these RSUs are connected to the internet RSUs the road side units are also connected to the internet. So, basically the RSUs have the internet connectivity.

(Refer Slide Time: 18:26)



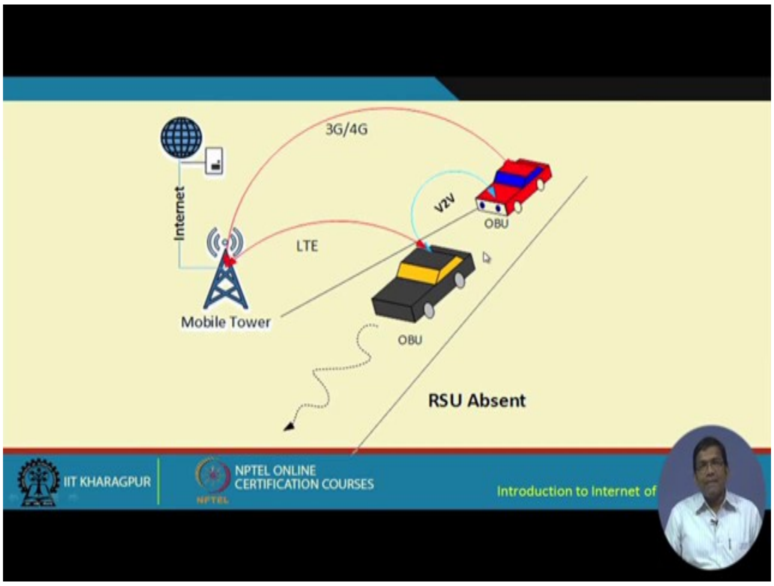
And this is how this internet connectivity is used is provided to these different vehicles on the road. In the infrastructure domain the RSUs basically are connected to internet by means of gate ways in the presence of the RSUs the vehicles may communicate to the internet viaV2I interfaces. So, when the RSUs are present it is going to be the vehicles are communicating to the internet via the V2I interfaces whereas, when the RSUs are not present the vehicles communicate with each other or the internet through cellular such as 3G, 4G LTE.

(Refer Slide Time: 18:55)



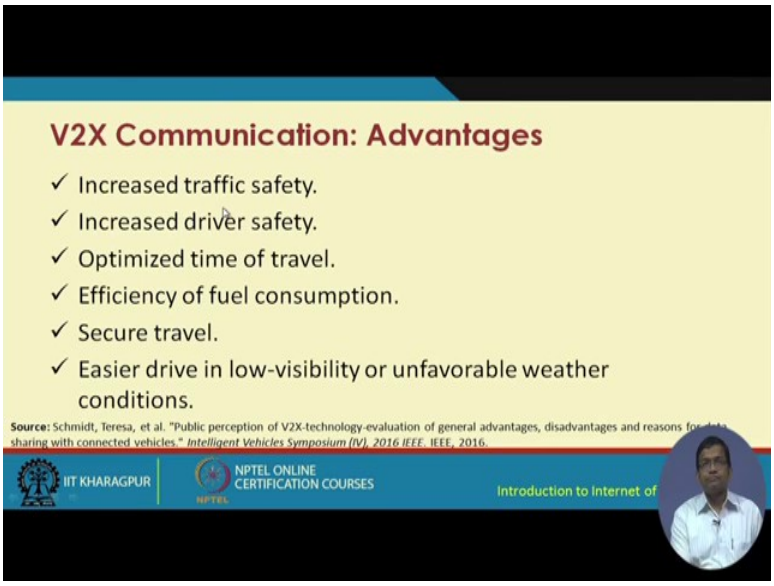
So, these are the 2 scenarios that are depicted over here that I just mentioned here is a scenario of the RSU being present and when the RSU is present you know. So, RSU has the internet connectivity via the gateway and that internet connectivity basically helps to have V2I and V2V communication.

(Refer Slide Time: 19:18)



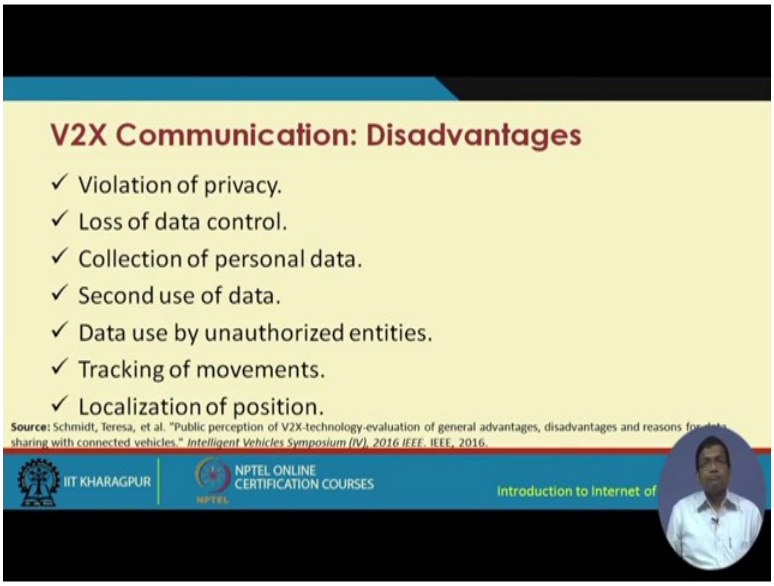
And this is the scenario of the RSU being absent and here basically you know if the RSU is absent what is suggested is to take help of the existing infrastructure of cellular communication like 3G, 4G etcetera and with the help of 3G, 4G LTE you know these vehicles they would be able to communicate with each other.

(Refer Slide Time: 19:35)



Now, what are the advantages of V2X communication? So, we remember in the last lecture previous lecture we spoke about the V2X; that means, vehicle to everything vehicle to anything basically communication what are the advantages it number one increases the traffic safety increases the driver safety optimizes the time of travel because you know if you if everything is connected together you can calculate your systems onboard systems can calculate that from 1 point to another; what is the optimized time of travel what are the different you know possibilities for different roots etcetera and how the travel can be made and the efficiency of fuel consumption and secure travel security secure you know. So, because you know it is all connected together and you know you can secure you know you know that; what is the way to travel from a point A to point B in a secured manner; fuel consumption likewise can be you know reduced. So, efficient fuel consumption easier drive in low visibility or unfavorable weather conditions.

(Refer Slide Time: 20:38)



The disadvantages include violation of privacy loss of data control collection of personal data secondary use of data secondary use of data is interesting secondary use of data means these data that is floating all across you know. So, what is going to happen to it who is going to use it you know, so, whether there would be a non intended use of the data. So, secondary use of the data data use by unauthorized entities very similar and tracking of movements of the vehicles is made possible.

So, you know it is possible that you know one can get all these different vehicles who are connected together through that if there is some kind of a security leak or something like that the positions and the movement patterns and futuristic predictions of about these vehicles can be made and these you know. So, that basically is not a very good thing if there are some vulnerabilities that are there tracking of the movements and localization of the positions of these different vehicles are the other disadvantages.

So, with this we come to an end of the second lecture on connected vehicles. In fact, we have spoken about connected vehicles in the first lecture and the second lecture as well we have seen the different different advantages and disadvantages of connected vehicles intelligent connected vehicles the different architectures the different standards that can be used and the only thing that is required is from understanding about one of these things and whatever we understood as part of the module one and module 2 as well implementing those and coming up with a platform to enable this kind of architecture.

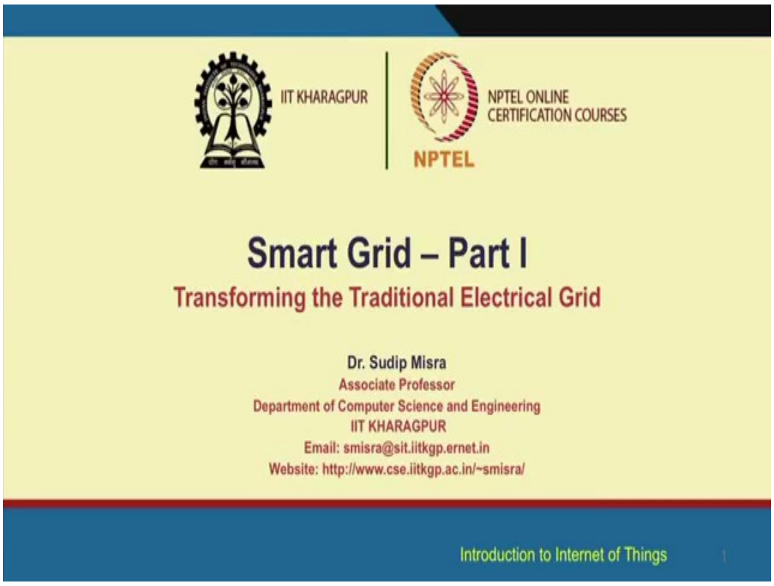
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 51
Smart Grid- Part – I

So, this lecture on internet of things focuses on the smart grid.

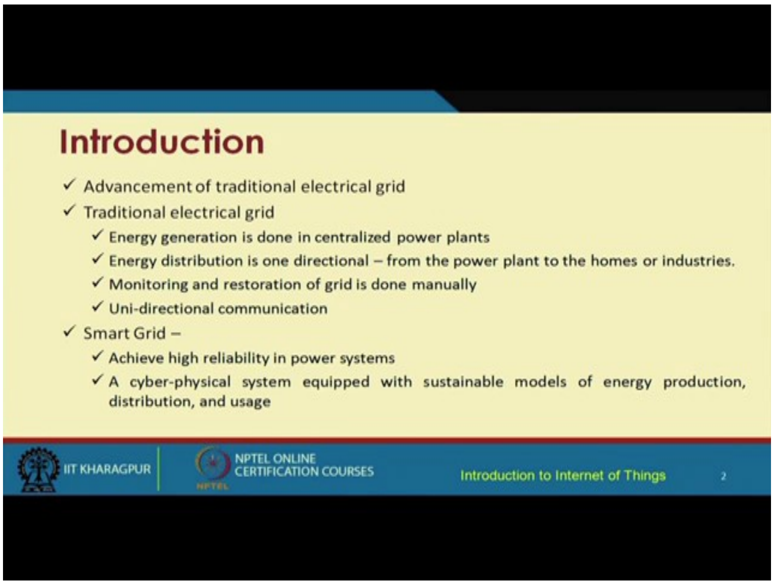
(Refer Slide Time: 00:26)



So, in the first part, we will be talking about the basics of smart grid, some of the motivations behind why smart grid is required and there after some of the more; you know a advanced concepts will be covered in the second part of the smart grid lecture. So, first part we are going to do is we are going to understand that what is smart grid, and what is its role in the overall building of internet of things, and what are different components of smart grid.

So, let us first look at what smart grid is all about.

(Refer Slide Time: 01:05)



We all are familiar with the traditional electrical grid; in the traditional electrical grid what happens is, you know what we have is we are consuming electricity that is generated by some generating station and is basically carried through different electrical you know electrical transmission devices and transmission lines to either homes or to offices. So, most of it most of it is all about the traditional electrical grid; is all about from the generation; that means the source of the energy being generated, renewable or nonrenewable depending on you know how the electricity generated.

So, from the source how it is going to be transmitted and then at intermediate points there are going to be different you know substations, which are going to relate the electricity to different parts of the city for further use, and also about the storage of electricity and so on and so forth. So, end to end from the generation through transmission to the final consumption at homes and offices the traditional electrical grid is all about. So, this is what the traditional power systems you know people who focus on power systems and electrical grid, this is this is what they study the; this is what they do they want to study how it can be done efficiently.

Now, as it happens with the internet of things as well, you know internet of things; when we talk about there are you know. So, its the advancement in terms of the use of different advanced information and communication technologies, to make everything smart and when we talk about that one of the important components is electricity distribution to homes and offices. So, that also has to be that has that also has to be made smart. So, that is where the smart grid comes into picture, the traditional electrical grid being made smart. And how will it be made smart? Through the use of the ICT tools different advanced information and communication tools, being used to make the traditional electrical grid smart is all about it is the concern of the field of smart grid.

Now, when we talk about smart grid, it concerns energy generation and energy generation is typically done in a centralized manner at the different power plants, and this generation can be as I said before this generation can be of two types either you know through nonrenewable sources like you know coal and so on and so forth nonrenewable sources electricity can be generated, or from the renewable sources like wind, solar power and so on.

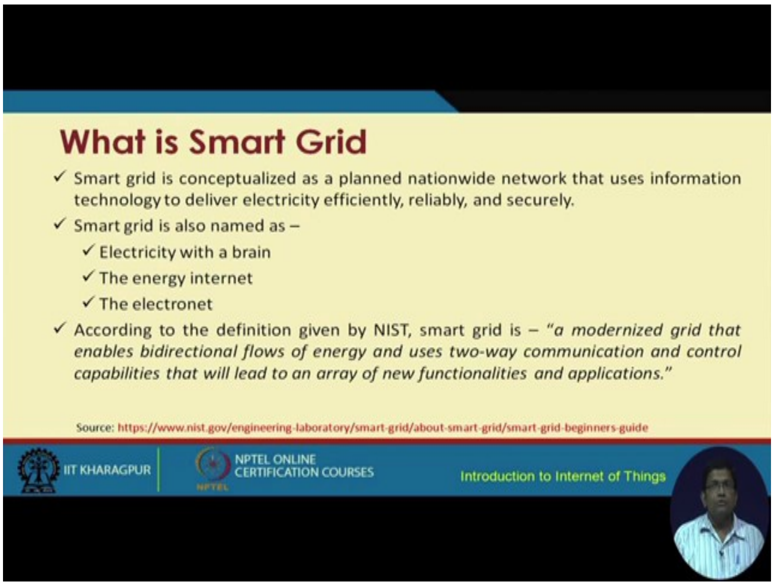
Now, this energy that is generated at the different power plants through the centralized mechanisms typically in the traditional field, that is then you know distributed in a typically traditionally in one direction. From the power plant to the homes or industries or offices and traditionally this particular flow of electricity is monitored and the restoration like if something goes wrong, the restoration of the grid is also done manually. So, what happens is what we have is unidirectional communication not that the energy flows unidirectionally, but also the communication is also unidirectional from the source to the end consumers.

Now, in a smart grid basically there is a divergence from this traditional concept of that means, that additional electrical grid concept, in the smart grid as I was telling before that you use the information and communication technologies the different variance of it the different types of it, to achieve higher reliability in power systems number one and overall making the system smart and what kind of system we have here? It is a cyber physical system. It is a cyber physical system that is equipped with sustainable models of energy production, distribution and final use by the consumers.

And what is a cyber physical system by the way in a nut shell its cyber physical system is an integral component of internet of things, in a nut shell what happens is in any cyber physical system smart grid being a good example of it in any cyber physical system, the cyber part; that means, the internet or the network part is intertwined very tightly with the physical system. So, physical system the cyber system cyber based system; that means, the internet based or the network based system being intertwined very tightly in order to make it smart. So, that it can do things much more efficiently than the traditionally you know exclusive physical system. So, this is a cyber physical system which is being used wide widely in the building of internet of things.

Now, let us move ahead.

(Refer Slide Time: 07:14)



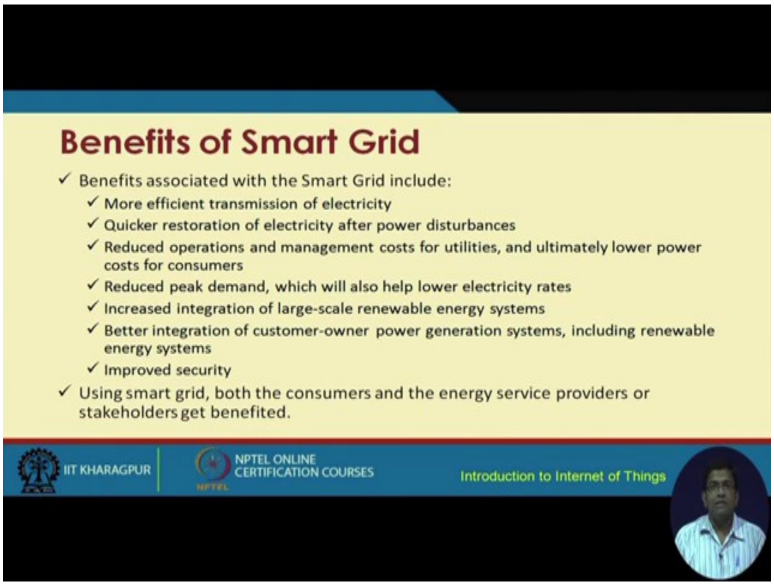
So, we have a smart grid which is conceptualized as a plant nationwide network, that uses information technology to deliver electricity efficiently reliably and securely this is very important you know. So, we have so many different problems with the traditional smart grid the sorry traditionally electric grid. So, what is you see we you in our country for example, I mean many countries you know with the distribution generation to distribution and use there are lot of problems. We have theft of electricity you know electricity being stored stolen while in transient, before it is actually being used by the legitimate consumer.

So, smart grid basically also tries to address this particular problem that how securely this electricity can be transmitted to the legitimate and the actual consumers the internet consumers. So, delivering the electricity efficiently, reliably reliable means if something goes wrong how things can be taken care of and if something it may be some subsystem goes down may be a substation for example, in the overall distribution system goes down. Then even if it goes down the smart grid is going to still function without any interruption and everything will be remain fine. So, that is not possible with the traditional electrical grid and which is possible with the smart grid.

So, you know smart grid as we are using computer based methodologies information technology, communication technology etcetera it becomes very interesting. So, some people prefer to call smart grid as electricity with brain, some people prefer to call it as the energy internet, some even prefer to call it as the electro net. So, NIST which is an organization based in US. They defined smart grid as a modernized grid that enables bi directional flow of energy and uses the two way communication and control capabilities that will lead to an array of new functionalities and applications the overall thing is service electricity is a service right. So, offering the electricity the end consumers are getting this service in their homes and their offices and in the industries and you know workshops and so on and so forth.

So, but what makes electricity smart grid smarter or interesting is that we have two way communication two way communication, not only from the source towards one direction is from the source towards the end users, and the other direction is from the end users to towards the source or in the interim the different substations micro grids and so on. So, these are some of these terminologies that will become more familiar as we proceed through, but you know so like this there are other functionalities as well and it is a mod modernized power grid that that is the core concept the heart of the smart grid.

(Refer Slide Time: 10:58)



There are different benefits of smart grid; one is that it is possible to more efficiently transmit electricity than the traditional one traditional electric grid, it is it has quicker restoration of electricity after power disturbances reduced operations and management costs for utilities and ultimately lower power costs for consumers, reduced peak demand which will also help lower electricity rates. So, what it means is basically you know there are certain peak times of electricity uses and during that basically you know what happens is during the peak time most of the users are connected and they consume lots of volumes of electricity, and with the smart grid it is possible to have reduced peak periods and overall distribution of electricity use is moderated over the entire length of the day.

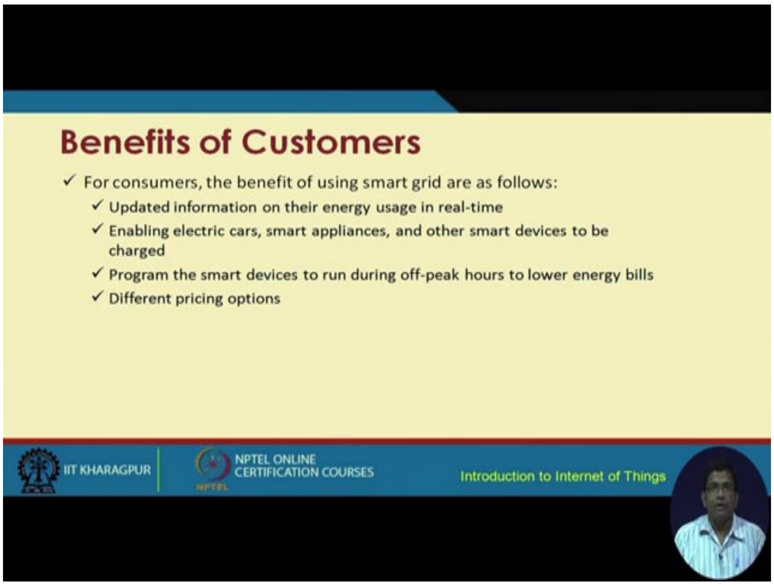
So, this is possible with the smart grid better integration of customer owner power generation systems including renewable renewable energy systems, now days as we have already experienced. So, not only we are using power from the main power distribution centers, but also many of us we have you know other you know we exploit the different other sources of energy the renewable sources of energy, we have many of us we use these the solar power panels right.

So, the solar panels are used to you know harness the solar energy similarly small wind turbines are also used wind sources of energy can be you know exploited can be used and they can not only be used locally by the by these different users, but if there is any surplus energy that is generated through these renewable means they can be even stored and can even be distributed and that surplus energy can be even fed back to the main grid. So, these are all possible with the smart grid which was not possible before with the electric traditional grid.

Then improved security is very interesting because you know power theft is one thing and the second thing is there are different other you know different attacks that is possible on the on these like it is a cyber physical system. Like any other cyber physical system or any other computer based system, you know smart grids are also vulnerable to different attacks and if it is a traditional electrical grid that attacks are even more you can you know it is possible to bring down a particular electrical grid due to different attacks. So, you know improved security is one such feature which tries to overcome these problems of the traditional grid.

So, using smart grid both the consumers and the energy service providers or stake holders can get benefited everybody gets benefited all kind of stake holders get benefited.

(Refer Slide Time: 14:06)



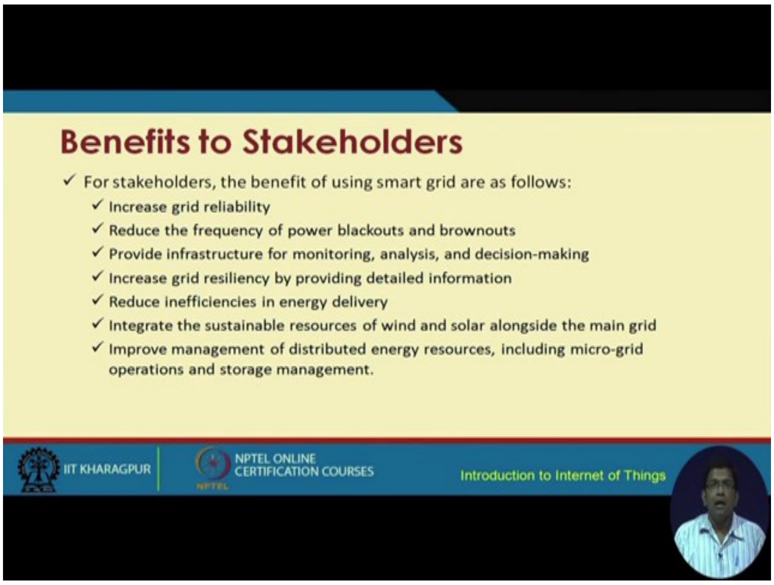
So, let us look at the different benefits for the customers let us first look at it, everybody gets benefited what are specific benefits to the customers. For customers or the consumers the benefit of using smart grid are that they can get updated information of their energy usage, in real time at any time basically whenever they want you know customers basically you know they can get an update about how much energy they are using. In fact, not only that cast you know customers they can also not only that they can monitor their inner energy usage, but they can also program that in ok. So, this during this time of the day you know I will be using this much energy I planned to use this much of energy during the other times I will be using you know this much of energy, some other amount of energy and so on.

So, all these different planning everything can be programmed by the customers of the smart grid customers in the smart grid; another thing is electric cars there you know. So, now, days we are taking about plug in electrical vehicles hybrid electric vehicles and so on. PVs, PHEVs and so on; these are possible in to be used by the customers in the smart grid smart appliances. So, appliances which can like you know we have smart air conditioners, smart refrigerators and so on and different other smart devices everything is possible in the whole world of smart grid. It is possible to program the smart devices to run during the off peak hours to lower energy bills. So, you know so there is some at certain times of the day there is peak the it is a it becomes a peak hour, peak hour means that during that time basically you know everybody is trying to you know have different appliances connected and use consume electricity much more than few other times of the day.

So, those are the off peak hours. So, during the off peak hours you know if one customer wants they can run certain appliances during the off peak hours and the other the bare basic necessities those appliances can be run during the peak hours and so on. So, it can be distributed and all of these things can be done by the customer himself or herself and that is all possible in the in the world of smart grid. And the different pricing options are also possible. So, in the traditional electrical grid as it happens you know. So, there is a single rate you know. So, at one particular rate that applies to all customers at all times of the day the week the month and so on.

So, in the smart grid it is possible to have the customers can enjoy different pricing levels different costs at different times of the day, week month and so on. So, all these things are possible and the customer gets benefited by using smart grid in different ways.

(Refer Slide Time: 17:25)



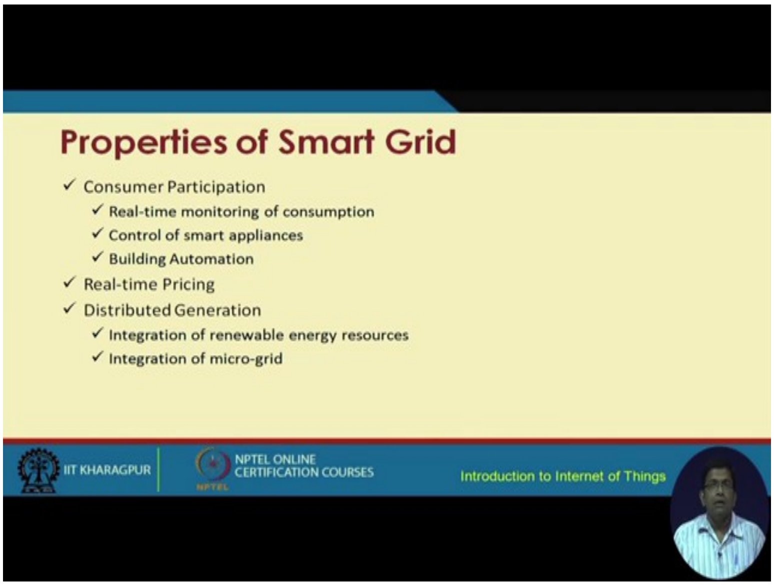
Other stake holders can also benefit from this smart grid as follows; for example, you know overall by the introduction of the smart grid the grid becomes more reliable as I already said before. The possibilities of blackouts and brownouts; so, black out means that that you know power consumption is no longer possible. So, there is a complete you know power is completely cut off for longer durations of time.

So, that is a power blackout what is burn out brown out sorry what is brown out? Brown out is basically that for few hours there is going to be reduced levels of voltage for example, you know that we often experience that at certain times of the day at certain times not always, that some are particularly you know if we are using the bulbs the incandescent bulbs. We see that the bulbs are glowing at lower strength and like this you know so that is because the overall electricity load in the line in the grid is lower.

So, brown outs can happen when we have you know intentionally, typically intentionally it can be unintentional also that for few hours the electricity load in the grid is lower. It is not a complete black out, but with reduced load so that is the brown out. So, the stake holders the other stake holders they can basically make it possible to have black outs or burn brown outs sorry to reduce the possibilities of black outs and brown outs. Providing infrastructure for monitoring analysis and decision making is possible, increasing grid resiliency by providing detailed information.

Reducing the inefficacies in energy delivery you know if there a certain points, where there is some energy leakage or something. So, those things those inefficiencies can be you know more efficiently addressed by the smart grid and that is very important particularly for the stake holder the service providers and so on. And there are other important features also it is possible to you know supplement these traditional power grid with the renewable sources as I said before for the customers as well and same thing is possible for the stake holders and the stake holders get benefited as well because you know they can supplement the main source of energy with wind sonar and other renewable sources through the use of micro grids. And overall the; you know over all the management of these distributed sources of energy, their storage from the generation to the storage and use everything can be done everything can be managed in a much more improved fashion.

(Refer Slide Time: 20:39)



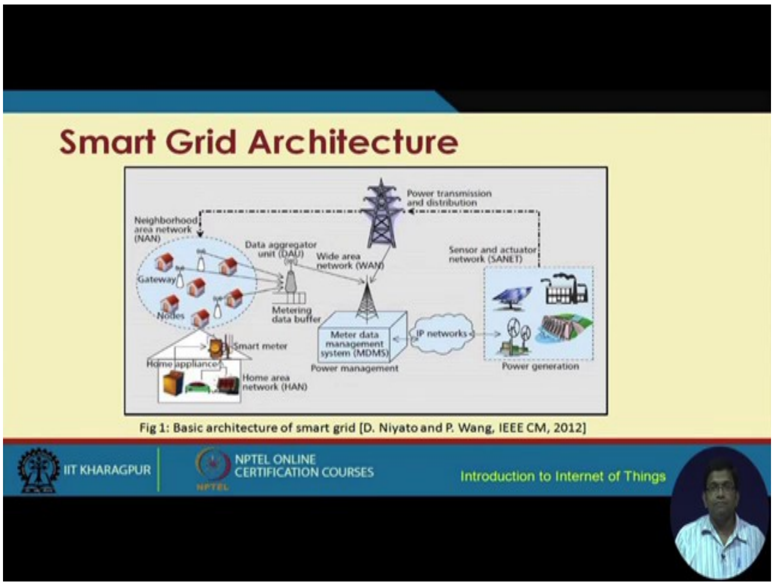
There are different properties of the smart grid consumer participation with respect to that, we have real time monitoring of consumption control of smart appliances, building automation. So, all these things are possible with the help of smart grid, and I have already mentioned about real time pricing you know at different times of the day, different whenever there is a requirement whenever there is necessity you know prices can be changed by the stake holders, and can be enjoyed by the consumers of course, there has to be certain policies and those policies have to agreed upon by a between these end consumers and the service providers.

So, that is a completely different issue, but this is made possible by this technology real time pricing is possible with the help of smart grid distributed generation integration of renewable energy sources and integration of micro grid. Other properties include a power system efficiency. So, including power monitoring it is possible to monitor the power in real time at all times asset management and optimal utilization is possible in a smart grid context distributed automation and protection.

So, everything is possible in the case of smart grid and making the overall power system efficient. In terms of power quality self healing behavior is exhibited by smart grid, self healing means if something goes wrong the system will be able to heal up on its own a some component may be has broken down, some subsystem a transformer has grown out, still the system can continue you know it will heal up on its own and it will continue to function as usual without much interaps interruption.

Frequency monitoring and control load forecasting that is possible and I do not think I need to elaborate that the overall electrical load can be forecasted in the smart grid and accordingly the power distribution can be made possible and reducing the overall black out and burn times sorry brown out times is possible with the help of load forecasting. And anticipation of any any type of disturbance any type of interruption is possible with the help of smart grid.

(Refer Slide Time: 23:01)

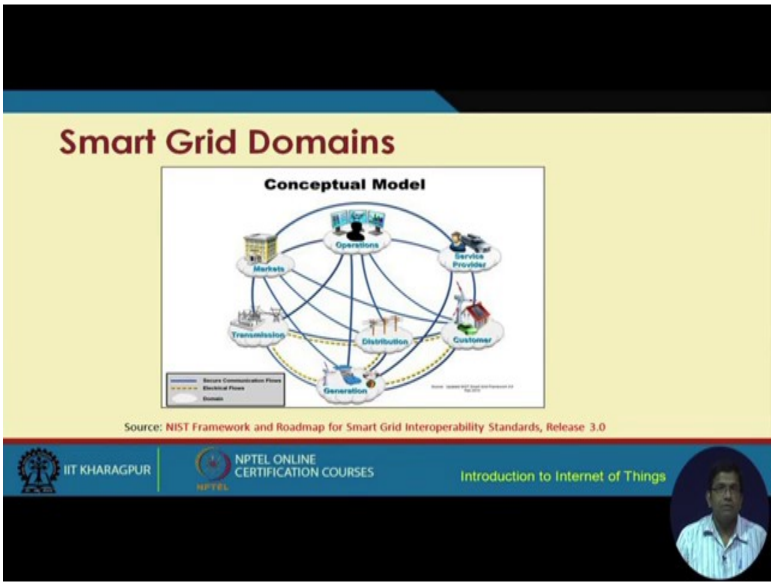


So, here is the smart grid architecture if we look at you know. So, what we have is we have the source of power generation. And from the source of power generation which can be from the renewable as well as the nonrenewable sources this energy is as you can see through the different transmission lines and distribution systems these energy is fed to different offices and homes, and these form something known as the neighborhood area network and then each of these homes have different appliances smart appliances including a smart meter the; you know it is a smart meter not a traditional regular kind of meter, but it is a smart meter which can be programmed as well. So and different smart appliances and the homes smart meters you know. So, these can be made possible.

Now, what is what is interesting is that. So, this is this is the traditional basically this is more of like a traditional flow of energy, but alongside what we also have is that connectivity to different networks. We have the sensors and different actuators being used a in this source you know in the power generation sources, then IP networks can be connected to the something known as the MDMS the meter data management system, and these can impact the MDMS can be connected by when or even the other internet connectivity to the power distribution systems, then we have the data aggregator unit which is basically sort of like from each of these homes, this information they can be aggregated at the data aggregated unit and this data aggregated unit has a metering data buffer which basically stores and buffers the data and so on.

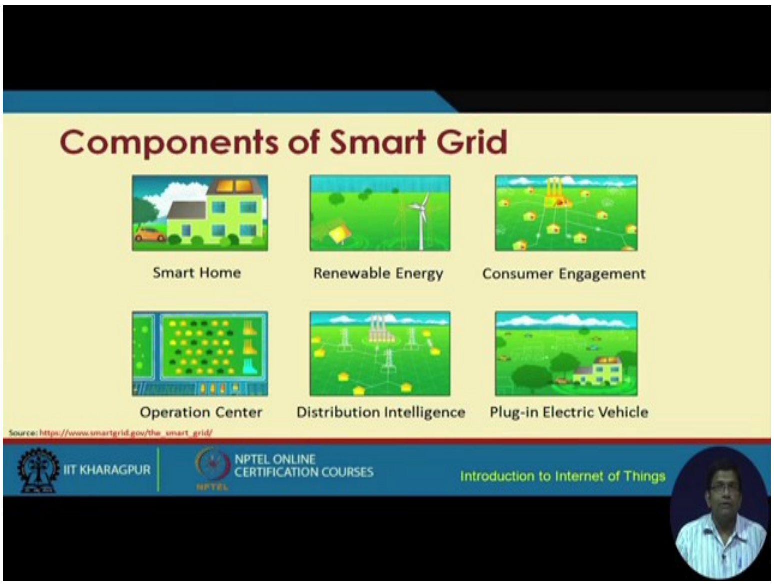
So, as we can see that we have basically and handshaking with or handshaking between the traditional power distribution and the information flow. So, we have you know in a smart grid we have both the flows energy flows and a energy flow and also the information flow together.

(Refer Slide Time: 25:25)



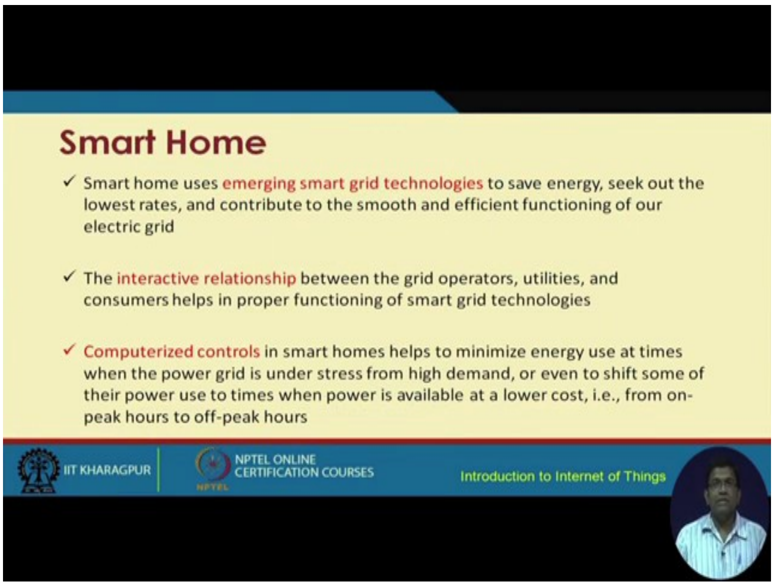
So, here is the conceptual model of the smart grid, we have different components as we can see over here, we have the customers, we have the service providers, we have the operation centers, we have markets transmission systems distribution systems and of course, the generation system. So, this is specifically showing these different you know flow of energy as well as the communication flows these dotted lines over here are showing the communication flow. Sorry the this is this is the sorry this is the electric electrical flow these dotted lines are the electrical flows between the customer the distribution system transmission system generation system and so on and these blue colored ones are basically the it they are showing the it is a depicting basically the flow of communication and it is a secure flow of communication in the case of smart grid.

(Refer Slide Time: 26:30)



So, there are different components of the smart grid; we have the smart home, then we have the renewable energy, consumer engagement, operation center, distribution intelligence, and plug in electric vehicles. So, we are going to take up each one of these one by one and we are going to discuss them in more depth.

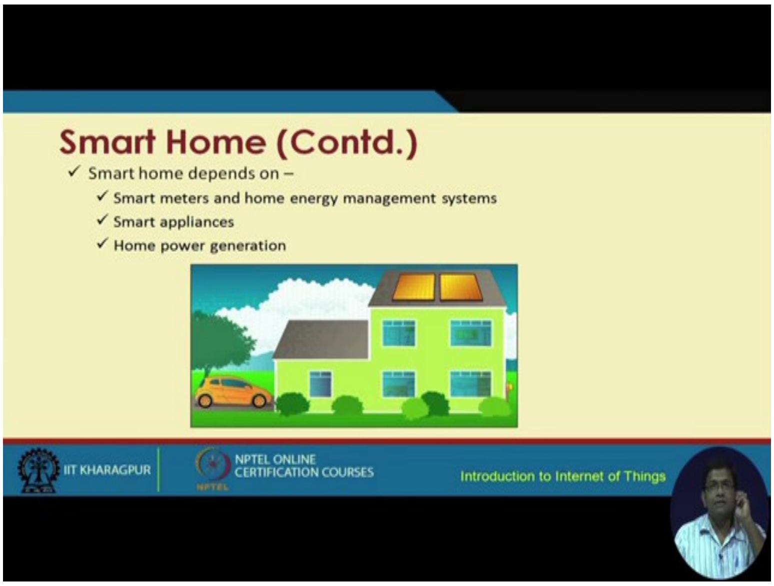
(Refer Slide Time: 26:51)



So, we will start with the smart home. So, in a smart home what we have our smart appliances and they use these different emerging smart grid technologies to save energy. And at lower I mean different rates you know prices different rates and the different prices can be used and these contribute to the smooth and efficient functioning of the electric grid.

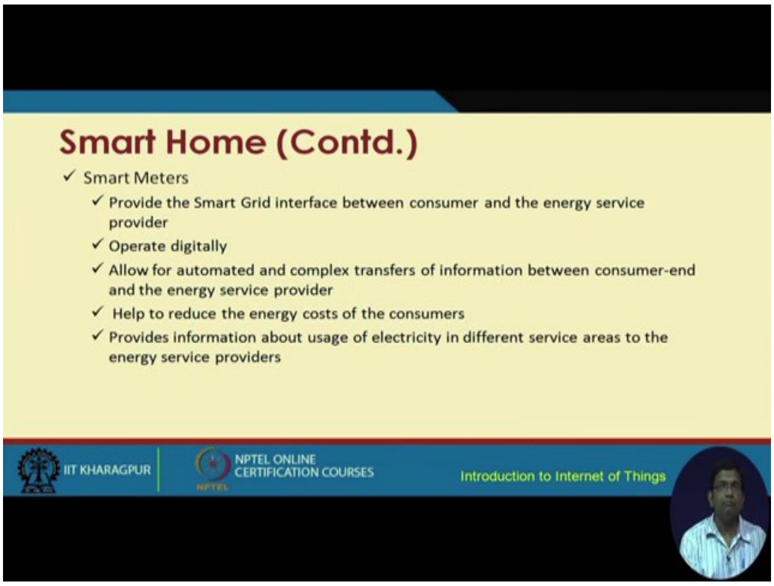
The interactive relationship between the grid operators utilities and consumers help in proper functioning of the smart grid technologies and there are different in a smart home, there are different computerized controls that help to minimize the energy use at different times of the day from the power grid and if the power grid is under stress; that means, there is high demand etcetera then this power load can also be shifted in the in a smart home. And so that basically you know what can happen is power can be distributed between the on peak hours and the off peak hours, and that way the power distribution in a smart home can be rationalized so that the users are benefited by you know. So, they can be having different appliances that can be connected at different times of the day depending on whether it is a peak hour or it is an off peak hour.

(Refer Slide Time: 28:18)



So, in a smart home what we have is something like this. So, we have smart meters smart appliances and there is a home power generation system as well. So, you know on the roof tops there can be these power panels the solar panels and the solar panels can additionally generate some electricity to supplement the electricity that is that is supplied to the home.

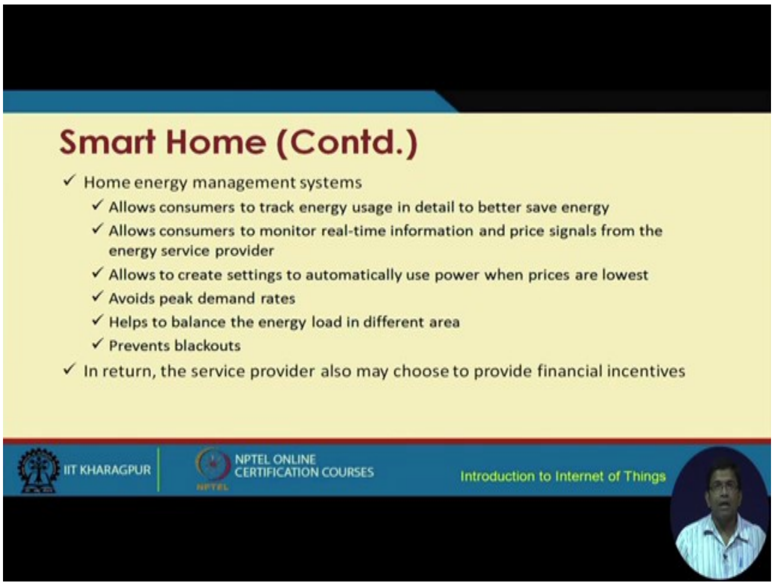
(Refer Slide Time: 28:42)



In a smart home the one of the important components is the smart meter and this is a programmable meter, and this meter can be programmed in such a way that at different times of the day, the different appliances can be enjoying the different you know loads of electricity at different rates.

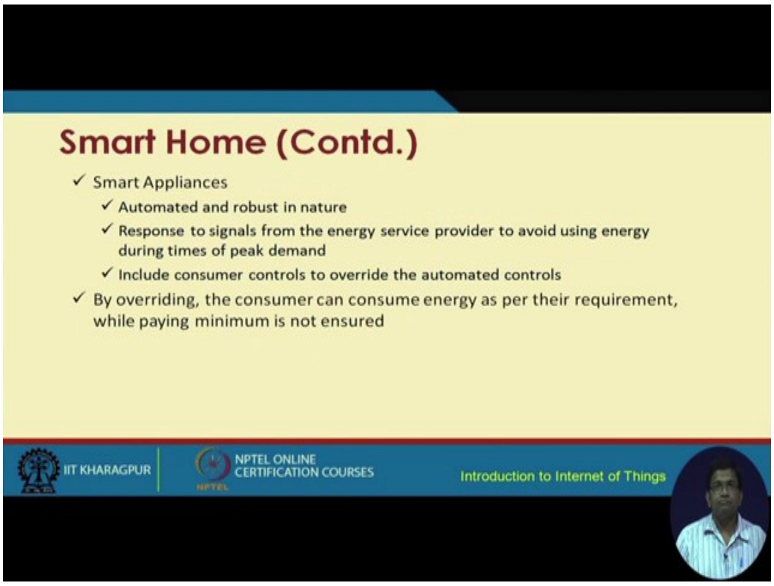
So, the smart meters basically they provide the smart grid interface between the consumer and the energy service provider and they operate digitally; that means, computerized you know. So, they have small computers embedded in them, and they allow for automated and complex transfer of information between the consumer and the energy service provider and that way the consumers can enjoy reduced energy cost.

(Refer Slide Time: 29:33)



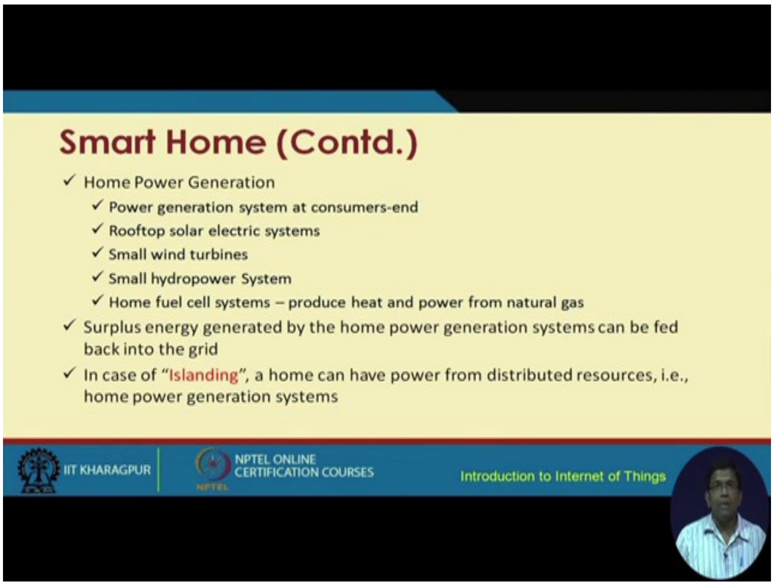
So, in a smart home the you know smart home basically allows the consumers to trace sorry to track the energy use in detail to save energy in a better way. So, basically you know what happens is you have something called the home energy management systems. So, these home energy management systems basically allows these particular thing to be done, these home energy management system also allows consumers to monitor a real time information and price signals from the energy service provider, it also allows to create settings to automatically use power when prices are lowest, it helps in avoiding big demand rates prevents black outs and brown outs, in return the service provider may also choose to provide financial incentives.

(Refer Slide Time: 30:29)



Smart appliances in addition to this smart meters smart appliances will be there, which can be automated and they can be robust in nature. They respond to signals from the energy service provider to avoid using energy during peak times, these smart appliances also include consumer controls to override the automated controls and by overriding the consumer can consume energy as per their requirement, while paying minimum that is not ensured.

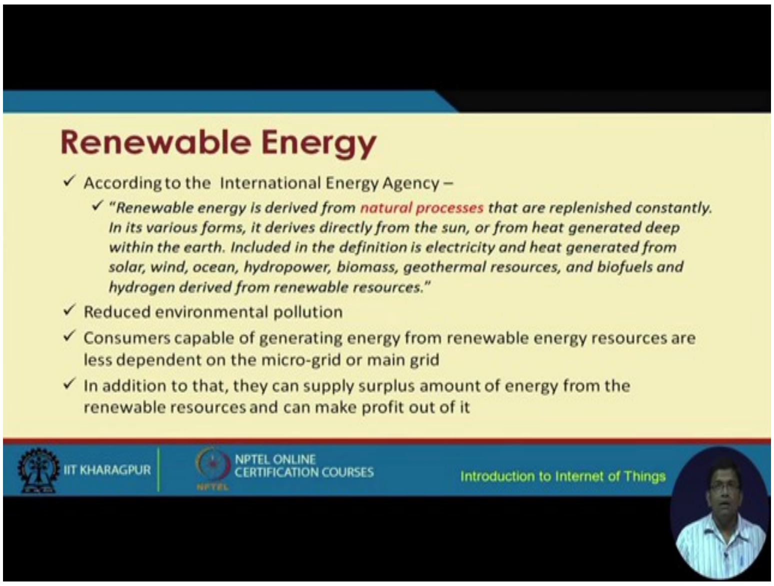
(Refer Slide Time: 31:03)



In every home these homes are also equipped with home power generation systems on the roof top there can be these wind turbines which can be fitted, or solar panels can be fitted to supplement these regular flow of energy.

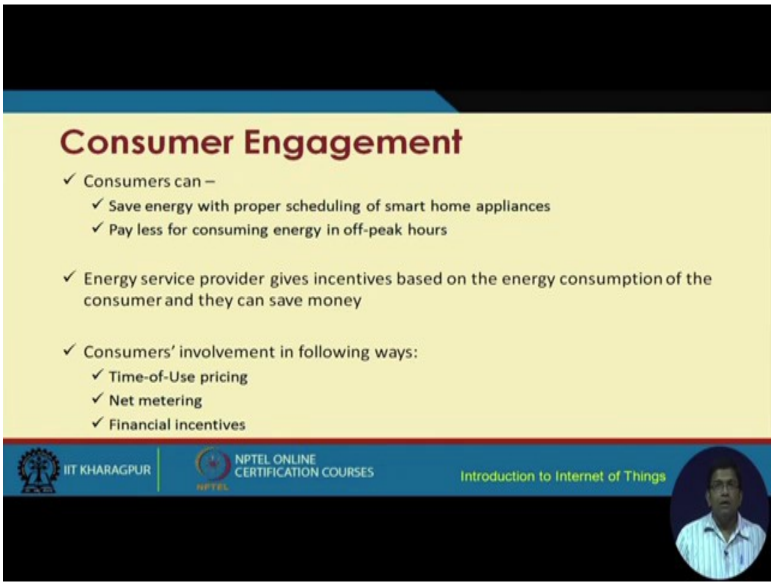
Surplus energy that is generated by the home power management systems can be fed back into the grid additionally, and these consumers can in fact, act as service you know the energy generators and they can in fact, on some additional money through this particular process and in case of islanding a home can have power from distributed sources that is they can have power home power generation systems.

(Refer Slide Time: 31:53)



Renewable sources are an important component of smart grid, I am not going to talk about what is an renewable source the definition is given for you, but there are as we all know from our basic knowledge that wind solar and different other forms. These sources of energy they are they have lot of advantages in order to reduce environmental pollution. So, and these are very attractive and renewable sources of energy are important components of a smart grid.

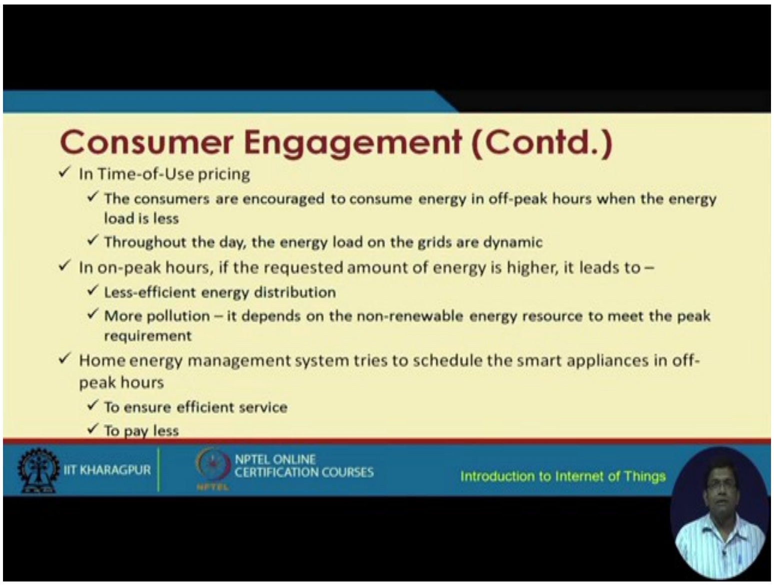
(Refer Slide Time: 32:28)



Now, let us talk about the consumer engagement in a smart grid, as I was mentioning briefly before it is possible for the consumers can also to get engaged in the overall process and the system in the functioning of the system, that way the consumers can save energy with proper scheduling of smart home appliances paying less for consuming energy in off peak hours these become advantages to the consumers. So, consumers get engaged in the process and they get advantaged through these means.

Consumer involvement comes in different ways, timer pricing is one net metering is another and financial incentives we are going to talk about each of these in brief.

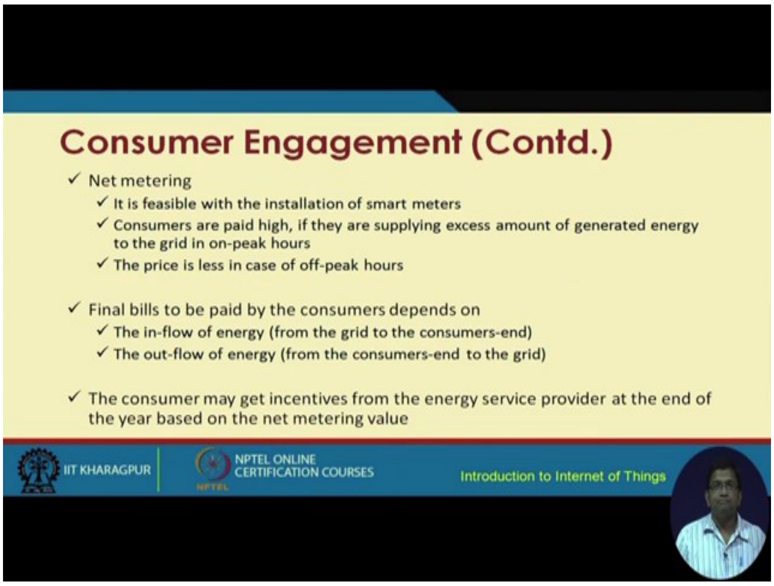
(Refer Slide Time: 33:14)



In time of use pricing basically what happens the consumers are encouraged to consume energy in the off peak hours when the energy load is less. So, it benefits both the service provider as well as the consumers. Consumers get you know during if their enjoying the power during the off peak hours that way you know. So, they have lower rates of electricity they are paying at lower rates and it also benefits the overall grid the different other stake holders like the service provider because that way they can manage the overall load in the city or you know where ever the electricity is being provided they can manage it better. And throughout the day the energy load on the grid becomes dynamic.

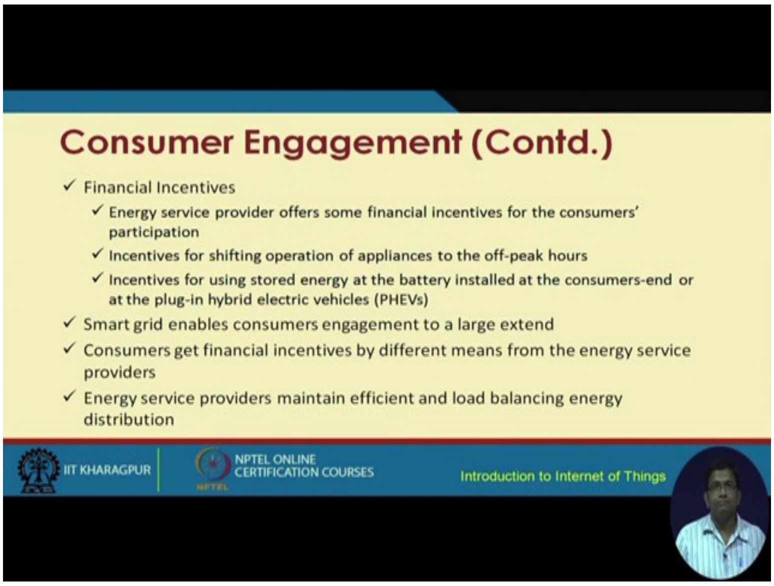
So, dynamically you know it can be made possible to use the different consumers they can use the grid the energy load in different times of the day in a dynamic fashion. In the on peak hours if the requested amount of energy is higher it leads to less efficient energy distribution more pollution, and home energy management system basically tries to schedule the smart appliances in the off peak hours to ensure efficient service and to pay less.

(Refer Slide Time: 34:42)



Net metering it is one feature through which it is feasible with the installation of it is feasible net metering can be done with the help of installation of smart meters. The consumers are paid high if they are supplying excess amount of generated energy to the grid in the on peak hours, and the price is less in case of off peak hours. The final bills to be paid by the consumers depend on the inflow of energy from the grid to the consumer end and the outflow of energy from the consumer end to the grid. The consumer may get incentives from the energy service provider at the end of the year based on the net metering value.

(Refer Slide Time: 35:26)



There are financial incentives as well through consumer engagement, energy service provider offers some financial incentives to the consumers participation incentives can be there for shifting operation of appliances to the off peak hours, incentives can also be provided for using stored energy at the battery installed at the consumer send and at the plug in hybrid electrical vehicles or the plug in electrical vehicles as such. Smart grid enables consumers engagement to a large extent, consumers get financial incentives by different means from the energy service provider through this particular process.

With this we come to an end of the first part of the smart grid as we have already seen that vision of smart grid is very attractive. So, it basically tries to transform the traditional power grid to a new system new cyber physical system, where ICT tools are used in a big way and these traditional smart grids can be made much more efficient, much more secure, and much more useful to the consumers and so what we are going to do is we will continue with our discussions. We have already seen some of the components of the smart grid we have seen the smart home and the consumer engagement and there are few other facets of the smart grid and that is what we are going to discuss in the second part of the smart grid.

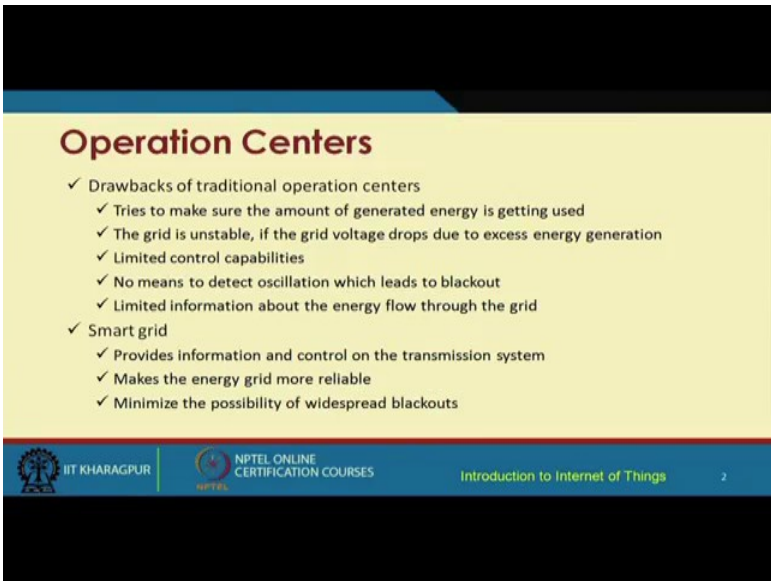
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 52
Smart Grid- Part– II

We have discussed in the first part of lecture on smart grid. We have already seen the different advantages of smart grid over the regular traditional electrical grid. We have also seen that this smart grid has different components; different facets, we have already discussed about 2 such facets of smart grid one is the smart home the other one is the consumer engagement when are going to continue and look at the other four facets of smart grid.

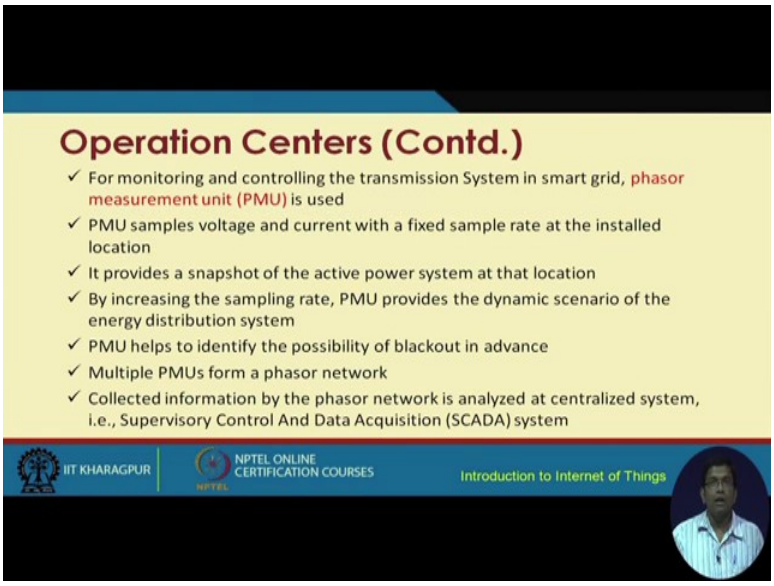
(Refer Slide Time: 00:59)



So, we will start with the operation center.

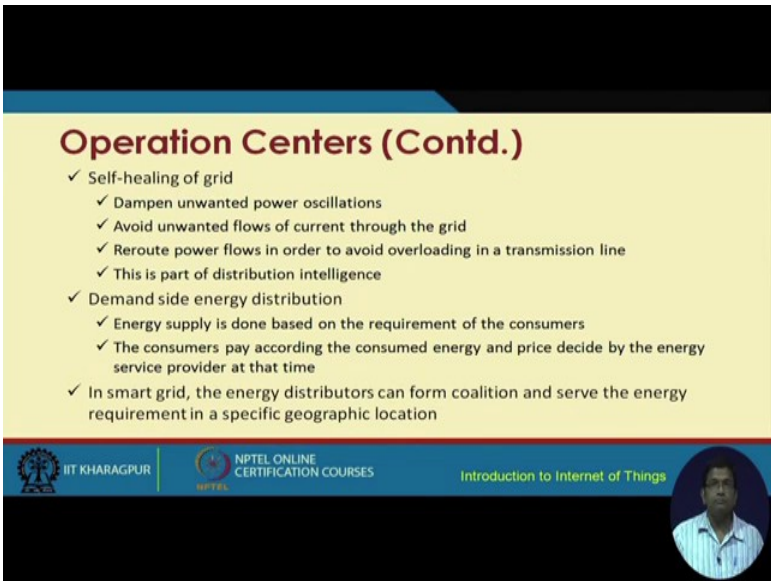
So, we have different draw backs of the traditional operation center for example, traditionally these operation centers they try to make sure that the amount of generated energy is getting used the grid is unstable if the grid voltage drops due to excess energy generation there is limited control capabilities and there is no means to detect oscillation which leads to blackout and there is limited information about the energy flow through the grid. In a smart grid, it is possible the smart grid basically overcomes some of these different difficulties with respect to the operation center by providing information and control on the transmission system making the energy grid more reliable and minimizing the possibility of wide spread blackouts.

(Refer Slide Time: 02:03)



For monitoring and controlling the transmission system in the smart grid something known as the phasor management units or the PMUs are used. These PMUs what they do is the sample the voltage and the current with the fixed sample rate at the installed location and then provide a snapshot of the active power system at that particular location and this way it increases the by by increasing the sampling rate. The PMU provides the dynamic scenario of the energy distribution system. The PMU helps to identify the possibility of blackout in advance and these multiple PMUs can be connected together can be networked together to form something called the phasor network and this connected information of the phasor network can then be fed to the SCADA system may be there could be a server or something some centralized system with some data acquisition and analytics and analysis ability it can fed and further analytics can be performed for better use of that particular information.

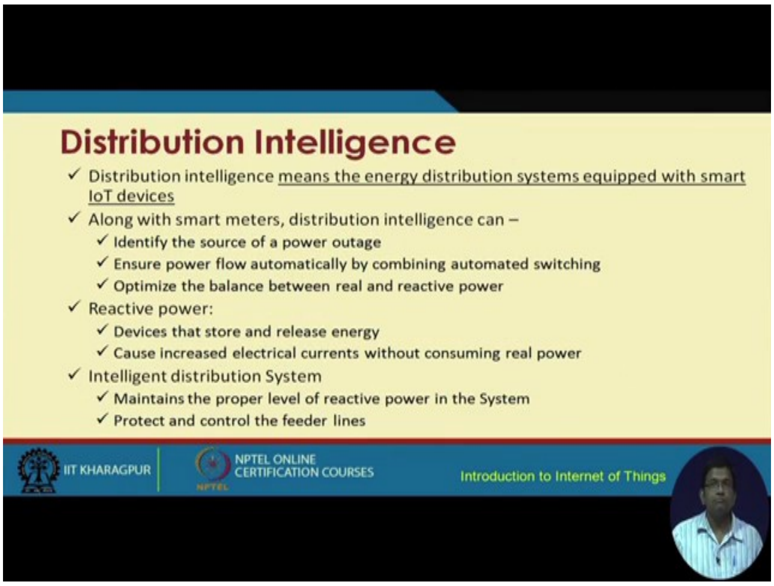
(Refer Slide Time: 03:18)



So, these operation systems operation centers they have the self healing capability. So, these self healing by the self healing mechanisms it is possible to dampen unwanted power oscillations; that means, that you know power oscillations power voltage fluctuations etcetera, etcetera they can be dampened and then avoiding unwanted flows of current through the grid rerouting power flows in order to avoid over loading in a particular transmission line and this is possible through the distribution intelligence or distributed intelligence incorporation of it in to the system. Demand side energy distribution is also possible energy supply is done based on the requirements of the consumers the consumers pay according to the consumed energy and price decided by the energy service provider at that particular time and as I told before that this energy.

Now the price can vary at different times of the day and the consumers they can connect their different appliances. They can schedule their different appliances to function at different times of the day depend on the on peak or off peak hours and everything you know each of these is possible through the help of advanced computational methods. So, in smart grid the energy distribution can form coalition and serve the energy requirement in a specific geographic location.

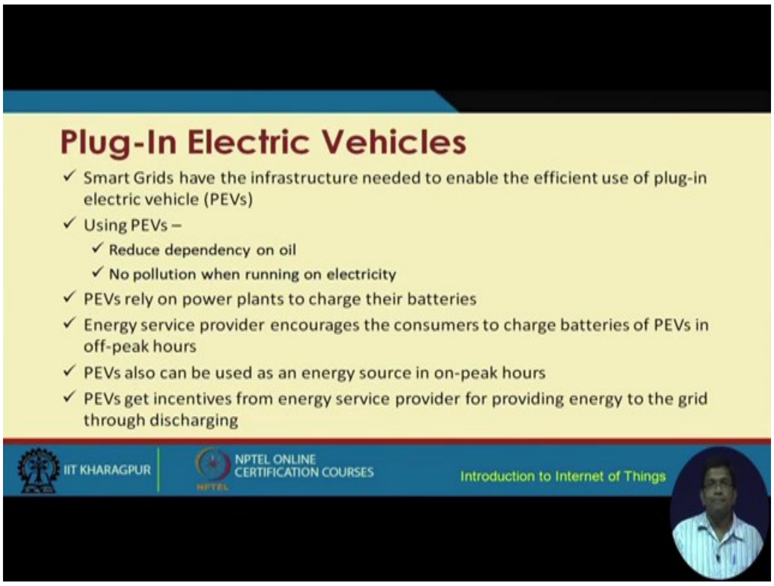
(Refer Slide Time: 04:57)



So, this distributed intelligence or the distribution intelligence implies that the energy distribution system is equipped with smart devices, sensor based devices, smart IoT devices, internet of things devices and this is where smart grid becomes very attractive to the consumers. So, along with the smart meters distribution intelligence can help to identify the source of power outage there are different sensors that are used. So, from the sensors and their different data that are equipped through from each of the locations of the sensors.

It is possible to find out automatically in a very intelligent way that where things are going wrong what is the source of the power outage ensure power flow automatically by combing automated switching optimizing the balance between the real and reactive power. In the case of reactive power the devices that store and release energy and devices can store and release energy and cause increased electrical currents without consuming real power the intelligent distribution systems can maintain the proper level of reactive power in the system and protect and control the feeder lines in the transmission system.

(Refer Slide Time: 06:26)



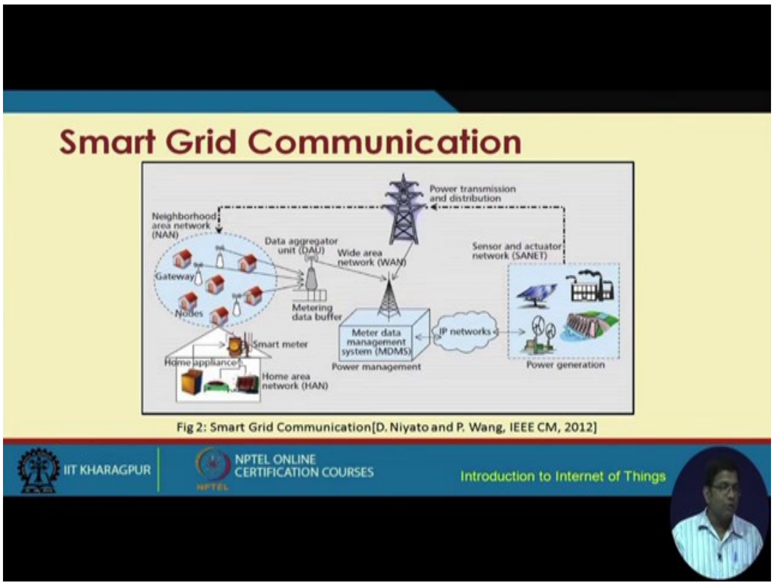
Now, let us look at the other component on the facet as I was calling it of the smart grid which is called the plug in electrical vehicles PEVs or if it is a hybrid electrical vehicle plug in hybrid electrical vehicles or PHEVs smart grids have the the infrastructure that is needed to enable the efficient use of plug in electrical vehicles and what happens to these PEVs is in the same way as we have these gas stations, in the gas stations what happened is these vehicles go and they you know they basically connect to the petrol pump and the petrol gets petrol or the diesel, the fuel basically is injected into the fuel tank of the car or the vehicle and then according to the bill that is generated the basically the consumer or the user he or she pays for that that much of the petrol or the diesel the fuel that he has purchased.

A similar sort of thing happens in the case of PEVs as well. So, there are charging stations as we have petrol pumps or the gas stations the here there are charging substations in the city. So, these electric vehicles they are going to go and they are going to connect to these different points where it can charged the vehicle can be charged and depending on you know how much charge has been has been received by the vehicle the owner of the vehicle basically the owner or you know driver basically pays for a that that much unit of charge that has been consumed that has been used that has been transferred to the vehicle.

A very similar sort of analogous situation happens in the PEVs. So, these are very interesting and plug in electric vehicles PHEVs basically you know what happens; it is hybrid vehicle; it is a hybrid electric vehicle. So, you here you have not only electric source of energy that drives the system, but also the traditional you know gasoline or you know traditional diesel gasoline and so on. So, we have hybrid sources of energy driving the vehicles. So, sometimes it will be running on diesel a bus can be running on diesel the hybrid bus, hybrid electrical vehicle sometimes it can be running on the electricity. So, we have both the sources of transmissions of power.

PEVs basically help in reducing the dependency on oil and these are clean and clean sources you know because electricity is a clean source. So, there is no pollution when running on electricity PEVs rely on power plants to charge their batteries and energy service provider encourages the consumers to charge the batteries of PEVs in off peak hours PEVs also can be used as a energy source in on peak hours.

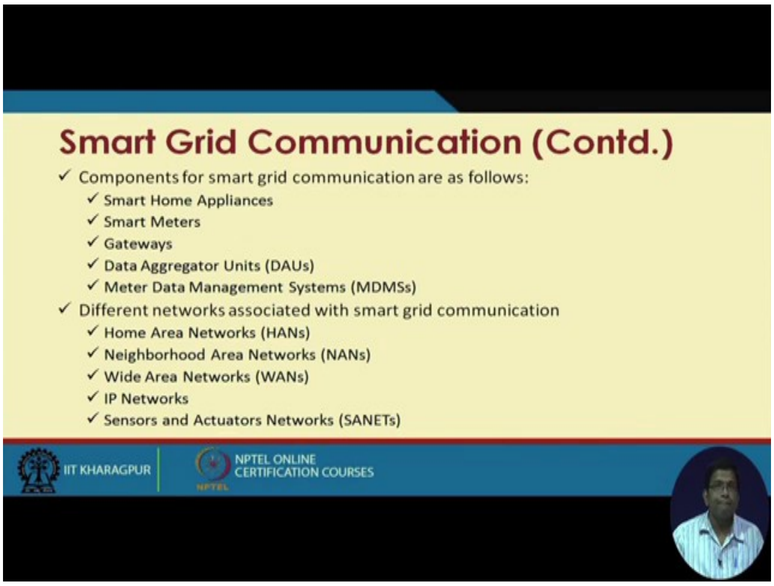
(Refer Slide Time: 09:51)



So, let us look at this particular figure. So, what we have as we can see is here we have the power generation system and this is the figure that we have seen earlier as well, but here we are going to look at it from a different perspective. So, we are going to look at it from the communication perspective here as we have seen that we have 2 types of flows of information sorry of 2 types of flows one is the flow of energy the other is the flow of information. So, we have the traditional flow of power the energy the electricity and we have the additional information flow.

So, this has to be you know. So, and why it is required it is required because sometimes it might be required to for the consumers for example, to operate upon some of their appliances or can feed some information to this to the to the power center to the service provider service provider can be receiving some information their intermediate systems can be receiving some of these information through a from the consumer through their smart meters and so on.

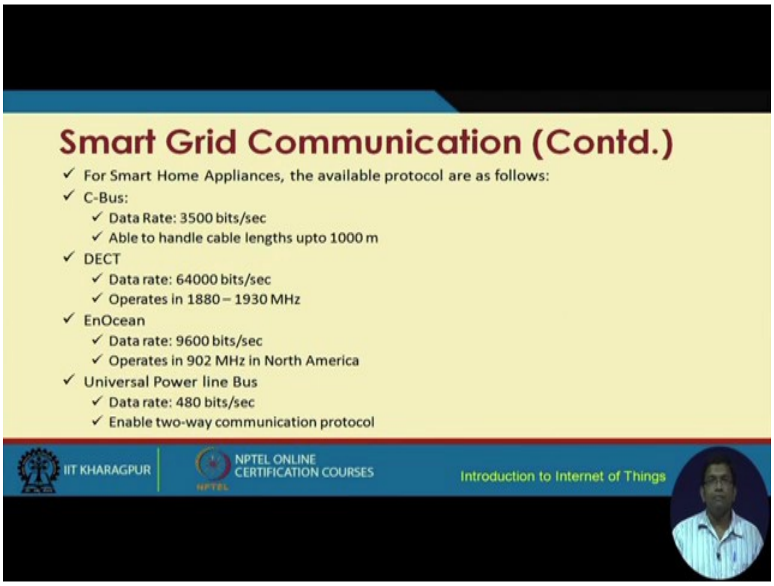
(Refer Slide Time: 11:20)



So, you see that what we have is not only the flow of energy, but also the flow of information. So, communication is very important smart grid one of the important components is the communication component and here we have the smart appliances smart meters and gateways these are communication gateways the network gateways and we have the data aggregator units. The DAUs the data aggregator units basically aggregates data from these different appliances at different homes from each of these homes each of these homes and their corresponding smart meters are connected to the DAUs and then we have the meter data management system the MDMS.

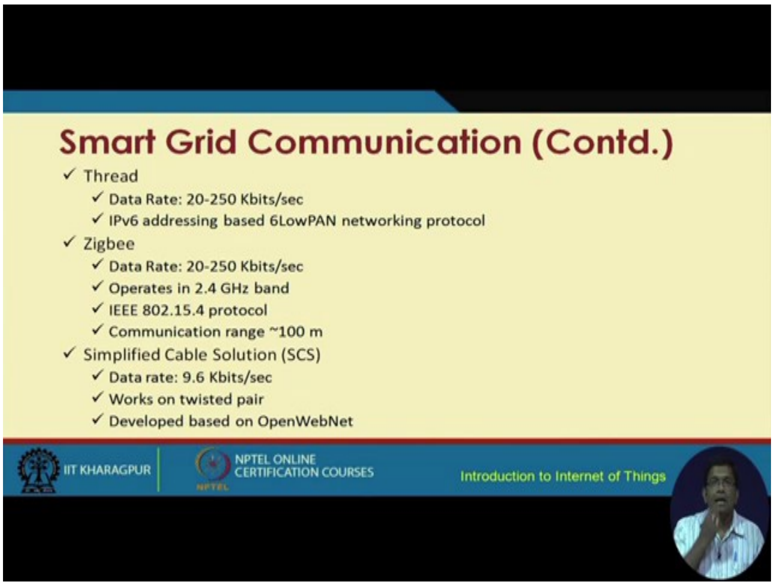
So, these are the different components of the communication aspect of smart grid. So, as you can see that each of these components they can form different nodes of the traditional networks that we are familiar with as we discussed in a previous lecture. So, different networks are associated with the smart grid communication we have in the case of smart grid we have different terminologies like neighborhood area network, wide area network, IP network and sensor and actuator networks. So, we have different types of network.

(Refer Slide Time: 12:32)



So, for smart grid appliances the available protocol that are used are C-Bus, DECT, the EnOcean and the Universal power line bus and I am not going to go through, but the corresponding data rate.

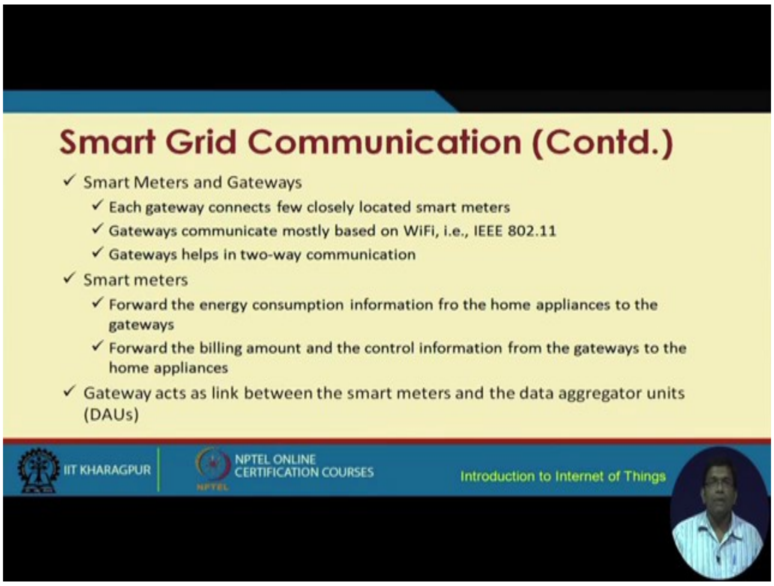
(Refer Slide Time: 12:59)



And the main feature are given in the slide in front of you similarly what we also have other thread the Zigbee and simple cable solution SCS with the corresponding data rate and their corresponding features are given over here some of some of these like Zigbee is something that we have already discussed in a previous lecture and this is not very you know Zigbee;

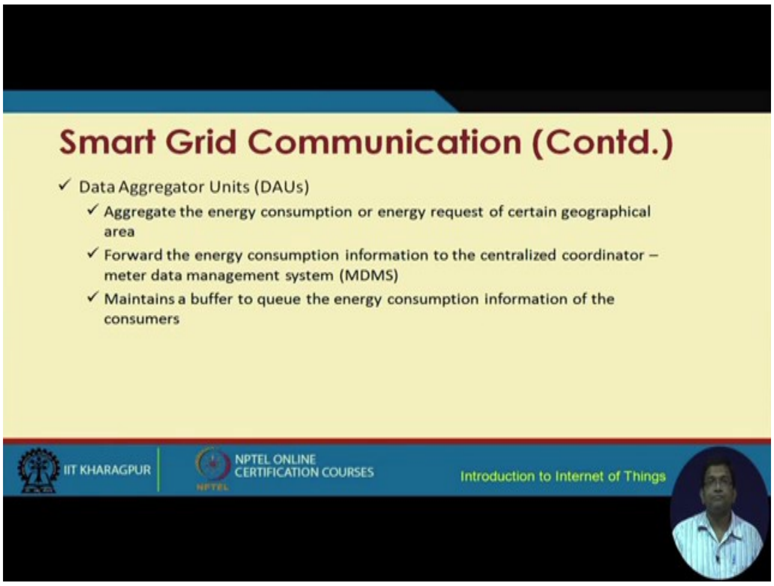
Zigbee is very attractive to have you know low data rate small short range communication established between different nodes in the network for example, different sensors it is possible sensors in the smart grid is possible to have Zigbee communication between between them.

(Refer Slide Time: 13:39)



We also have different other components like the smart meters and the gateways where each gateway connects very closely to the smart meters the gateways communicate mostly based on Wi-Fi which is 802.11 the gateway helps in the 2 way communication and the smart meters forward the energy consumption information from the home appliances to the gateways and forward the billing amount and the control information from the gateways to the home appliances these gateways act as link between the smart meters and the data aggregation units.

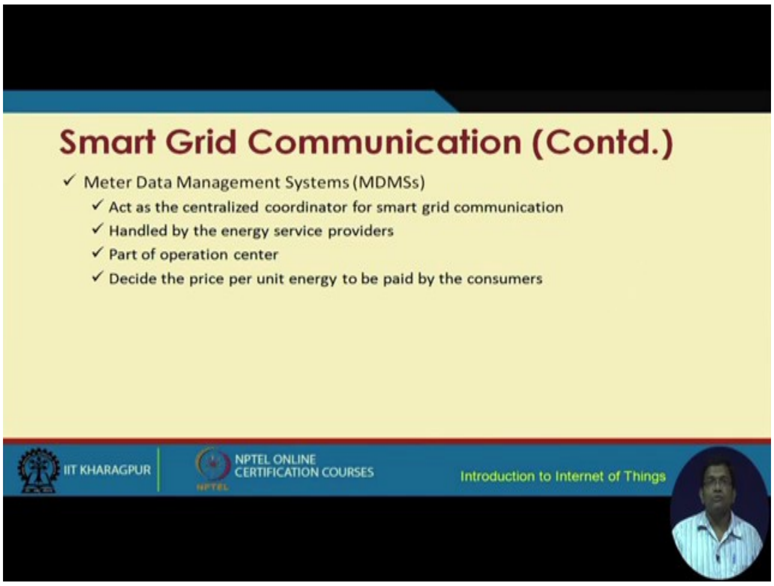
(Refer Slide Time: 14:17)



The data aggregation units aggregates the energy consumption or energy request of certain geographical area this is very important and this is very much required. So, what we have is we have a very complex problem and this complex distributed problem can be solved with the help of the traditional you know grouping or clustering based mechanisms. So, use of DAUs is very similar to clustering approach. So, what we are trying to do is for every few entities in a particular area we are going have this DAUs this DAUs are going to be the aggregators of the information and the energy consumption etcetera and then this DAUs after aggregation they are going to forward the energy consumption information to the centralized coordinator through the MDMS.

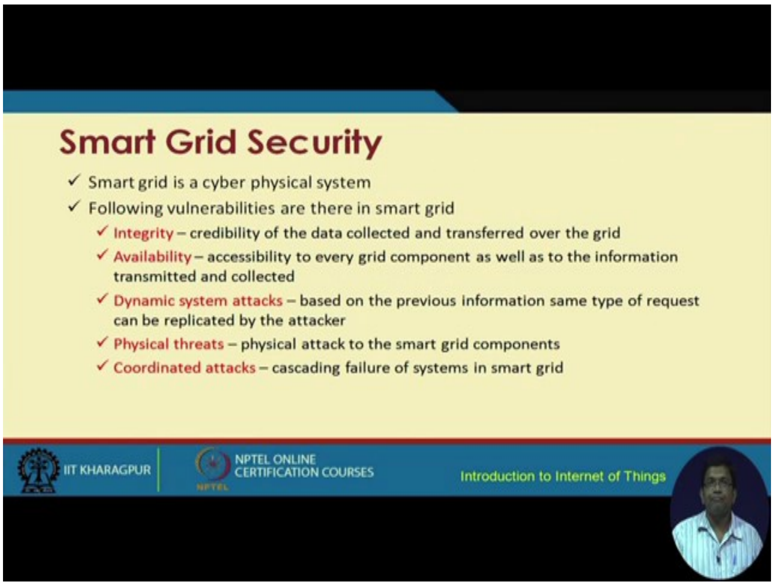
So, the MDMS basically you know helps in connecting to the centralized back end and it maintains a buffer to queue.

(Refer Slide Time: 15:27)



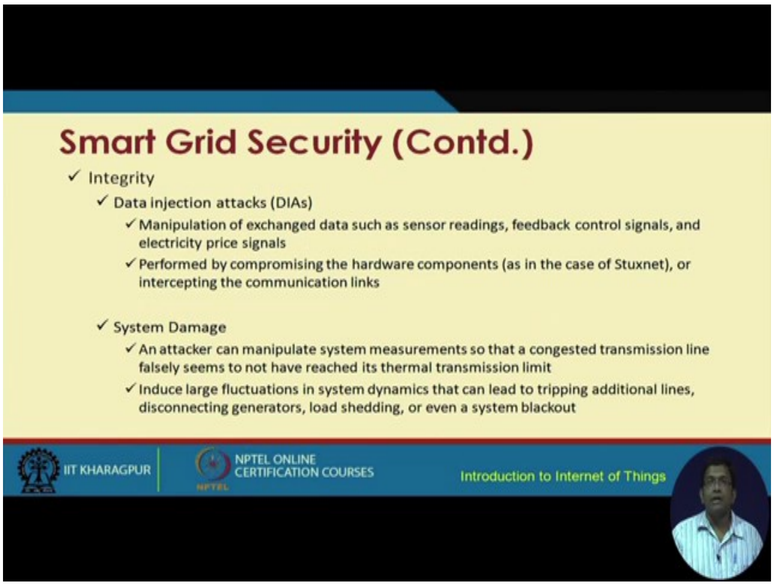
The DAUs basically they maintain a buffer to queue the energy consumption information of the consumers the MDMS acts as a centralized coordinator for smart grid communication it handles it is handled by the service providers and it is part of the operation center. The MDMS decides the price per unit energy to be paid by the consumers. So, it plays the MDMS plays a very important very crucial role in the functioning of the smart grid. So, we need to understand this thing very well the DAUs basically send the data to the MDMS which is located which is you know which is located in the smart grid back end at the service provider end and it is a centralized coordinator for the entire smart grid and it is part of that operation center and decides the price per unit energy this is very important, it decides the MDMS decides the price per unit energy to be paid by the consumers at different times.

(Refer Slide Time: 16:25)



The next part is very crucial in this smart grid communication which is the security aspect and it is very very crucial because we are dealing with not a traditional power system, but a cyber physical system and in as it happens in any cyber based system and any cyber physical system security is very important there are different types of vulnerabilities in a smart grid we have issues with integrity availability dynamic system attacks are possible different types of attacks are possible different types of physical threats on the different components of the smart grid are possible different types of other complex and coordinated attacks can be launched on a smart grid.

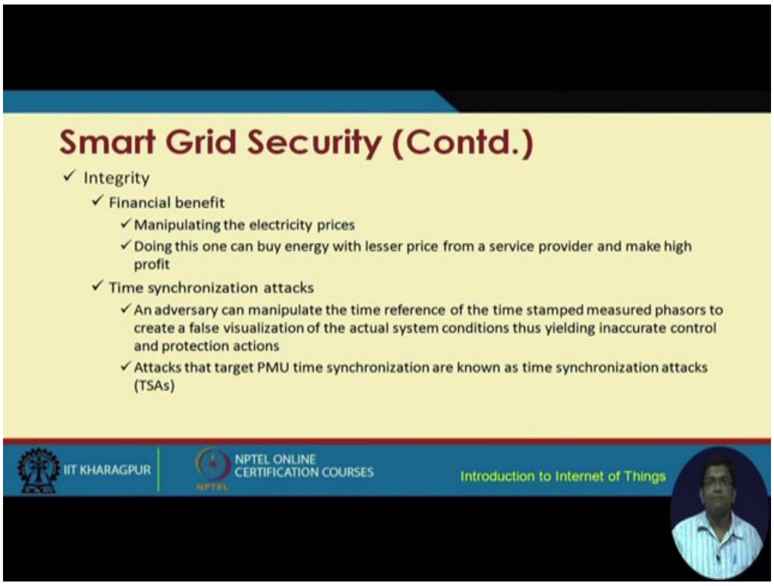
(Refer Slide Time: 17:23)



So, these are very important to be looked into when we are trying to build a smart grid integrity is very important you know because you know it is all about use of data different types of data are fed in to the system.

You know different types of attacks can be performed consequently for example, the data injection attack, DIA attack can be performed on a smart grid and there by effecting the overall integrity of the functioning of the smart grid. System can be damaged very easily an attacker can manipulate the system measurements. So, that the congested transmission of the falsely of the all the of the false data seems to not have reached to the to the thermal transmission limit. This induces large fluctuations in the system dynamics that can lead to tripping additional lines disconnecting generators load sharing or even a system blackout. So, as we can see that overall system can be damaged if this is not taken care of. So, this is a very important security concept.

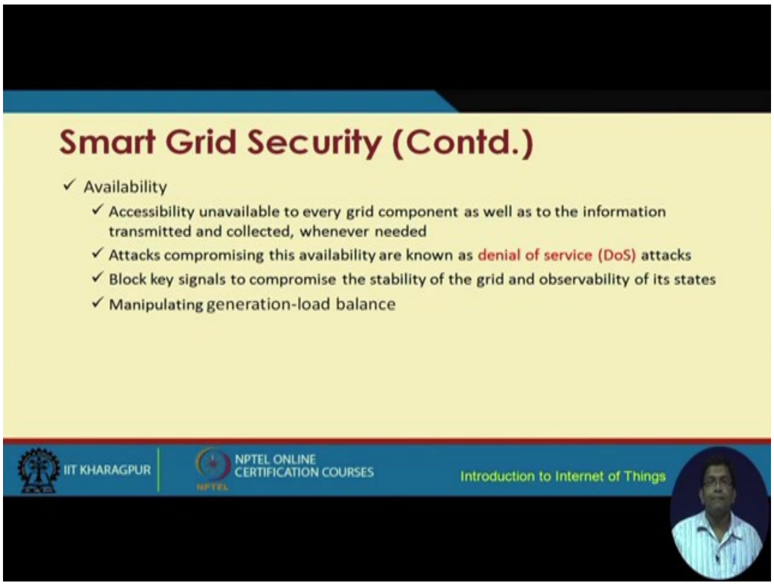
(Refer Slide Time: 18:34)



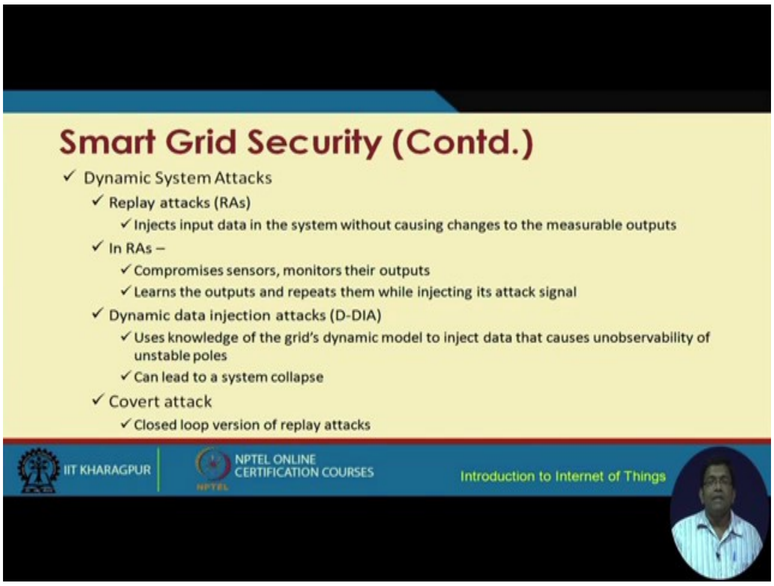
Financial benefits can be there to hurting the integrity of the system for example, you know the attacker can manipulate the electricity prices by doing this one can buy energy with lesser price from a service provider and make high profits and as you as you can understand that it is very easy to do because the cyber system basically connects to the physical system and through the cyber system attacks can be launched on the physical system and it is possible to basically indirectly steal the electricity at lower prices or even at low prices without paying it without paying any price electricity can be stolen.

Different time synchronization attacks can be launched where an adversary can manipulate the time reference of the time stamped measured phasors to create a false virtualize a visualization of the actual system conditions there by yielding inaccurate control and protection actions.

(Refer Slide Time: 19:45)

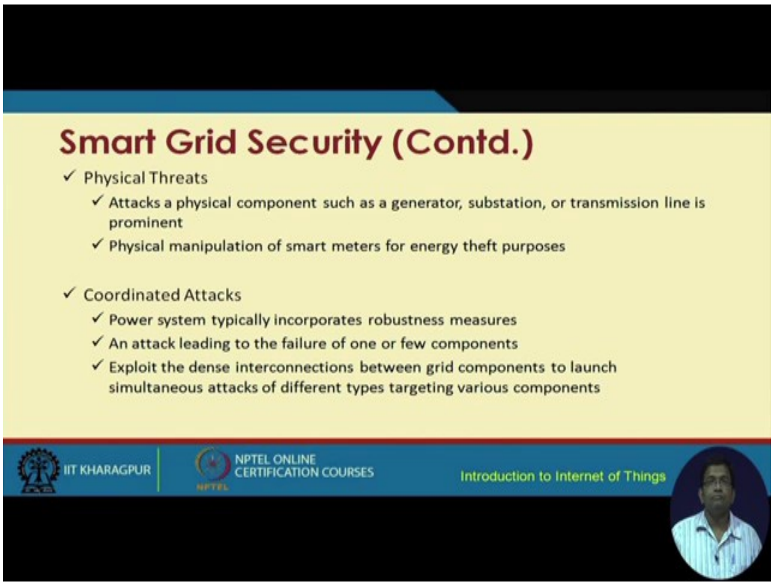


(Refer Slide Time: 19:54)



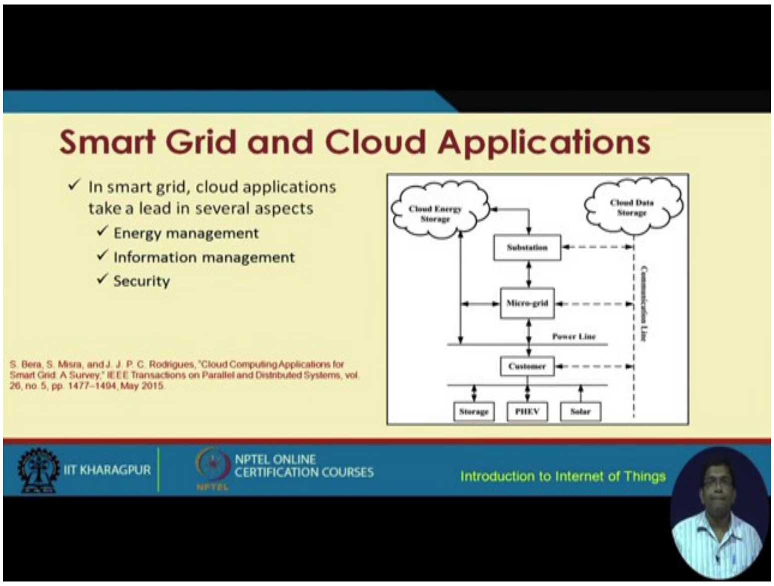
Availability is a very important issue in the case of security of smart grid different types of denial of service attacks, different types of replay attacks can be launched. In a replay attack basically what happens if the attacker injects the input data into the system without causing changes to the measurable outputs different types of other distributed data injection attacks can be dynamic data injection attacks can be performed where in the attacker uses the knowledge of the grids dynamic model to inject data into data that causes of unobservability of unstable poles.

(Refer Slide Time: 20:36)



Physical threats can be launched attacker basically physically damages some of the components for example, the generator can be damaged the substation or the transmission lines can be damaged and different other types of coordinated attacks can also be launched.

(Refer Slide Time: 20:53)

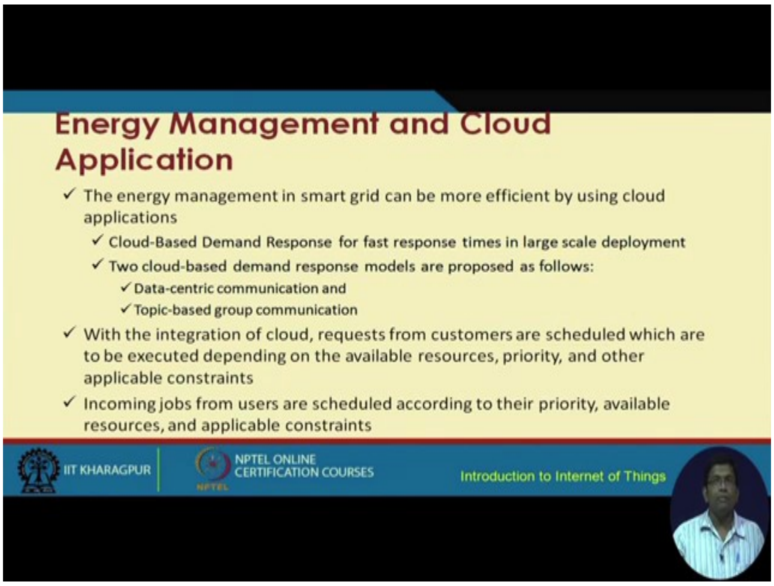


Now, one very important issue is that the smart grid can exploit the use of the cloud technology as well because this smart grid as we have seen is a source of generation of lot of information that information can be stored at the cloud and therefore, there are the very important things that can be done with the help of augmenting with the cloud technology.

So, cloud applications can take a lead in different several aspects for example, with respect to energy management, information management and security management. So, I am going to briefly talks about each of these highlighting their use, but this is available in the paper in the research paper that for the reference of which is given on the slide. So, this paper has been published in the IEEE transactions on parallel and distributed systems in the year 2015 and this particular paper basically serves as an important reference about how smart grid and cloud technologies can integrated together to harness the benefits of each of these and making the power system much more attractive.

So, as we can see in this particular figure what we have is we have the substation micro grid customers the traditional power lines and then we also have the communication link and this communication link basically feeding this data to the cloud data storage and here on the other hand on the other side as we can see over here we have another type of cloud which is the energy storage. So, we have the cloud energy storage which basically stores the electricity over here and on the other hand this information can be stored in the cloud data storage. So, bringing the energy storage and the data storage together 2 different types of in a cloud conceptually we are talking about is made possible with the help of these cloud integrated smart grids.

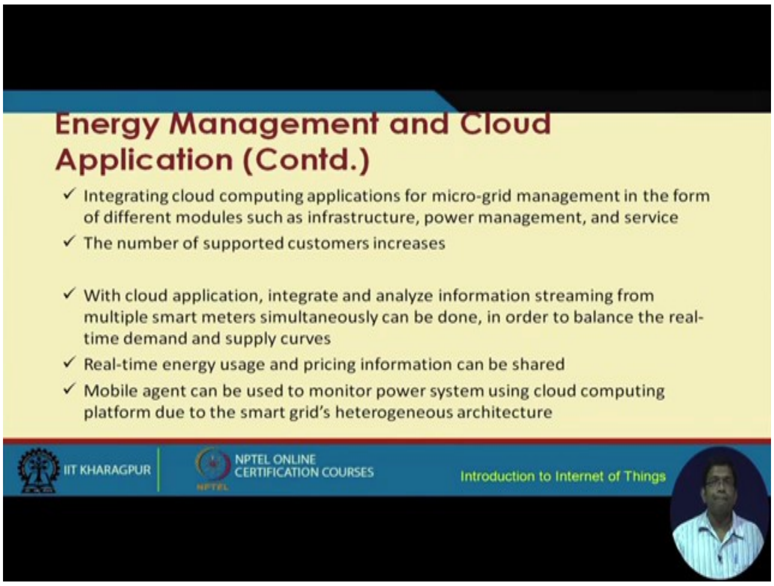
(Refer Slide Time: 23:11)



So, energy management and cloud applications are very interesting the energy management in smart grid can be more efficient by using cloud applications with the integration of cloud requests from the customers are scheduled which are to be executed depending on the available resources priority and other application constraints.

So, this is very interesting because you know. So, on the cloud side there are different models of cloud which can be utilized over here by the smart grid for energy management for example, we have this platform as a service we have the software as a service we have the infrastructure as a service. So, not only that we will you know will be using the cloud for storing the information, but different algorithms different you know different systems different you know software can be executed at the cloud end and that basically you know helps the smart grid to harness the benefits of the cloud technology.

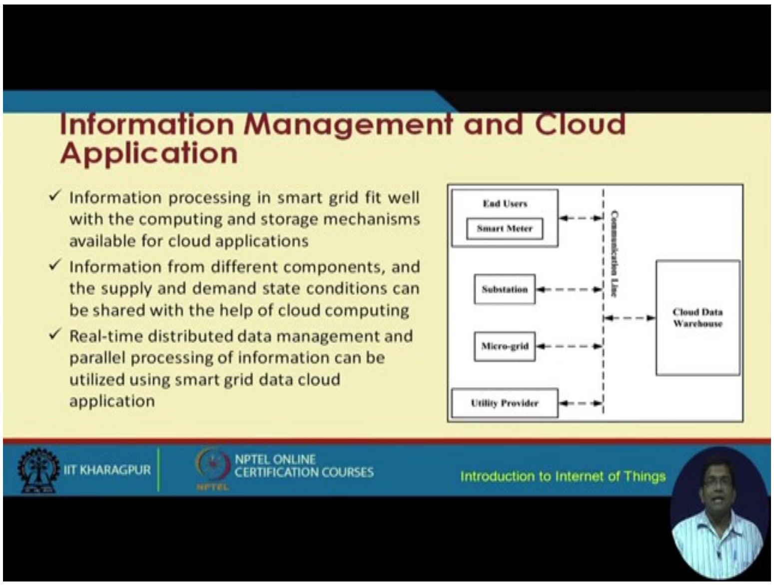
(Refer Slide Time: 24:20)



Integrating cloud computing applications for micro grid management in the form of attractive in the form of different module such as infrastructure power management and service. The number of supported customers basically increase that way and with the cloud applications it is possible to integrate and analyze the information that streams from multiple smart meters simultaneously in order to balance the real time demand and energy curves.

So, as we can see over here lot of dynamic aspects you know can be managed efficiently dynamic because you know when we are talking about energy management in the smart grid, things are very dynamic not only the pricing is dynamic everything is dynamic energy generation, energy distribution, energy use, pricing each and every thing is dynamic and all of these requests smart algorithms and software to help in you know in achieving all of these particular features these specific features and the cloud can help in achieving this particular objective. Then another advantage is real time energy usage and pricing information can be shared because you know. So, in the cloud we have these; the communication backend the network everything is network together. So, this information about the energy usage pricing information they can be shared with that potential customers and not only customers, but also the other stake holders.

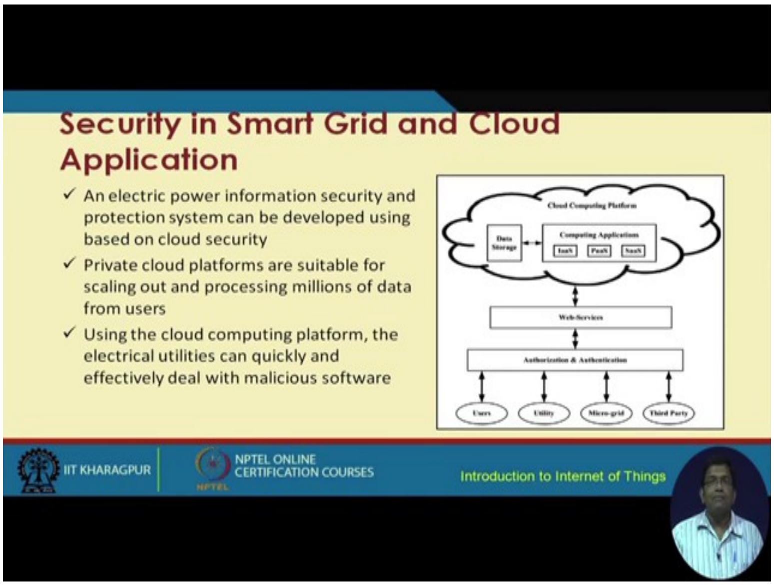
(Refer Slide Time: 25:51)



So, that was the energy management then we have the information management. So, information processing in smart grid fits well with the computing and storage mechanisms available for cloud applications information from different components and the supply and demand state conditions can be shared with the help of cloud computing real time distribution data management and parallel processing of information can be utilized using smart grid data cloud application. So, if you can look over here in this particular figure what we have are end users substations micro grids utility providers communicating bidirectionally with the cloud data ware house.

So, cloud data ware house basically has all the data. So, all these data can be stored in the cloud data ware house. Also from this particular end it is bidirectional because the data can flow also from this end to these different components. So, we have this information flow in both the directions and this information flow has to be managed properly.

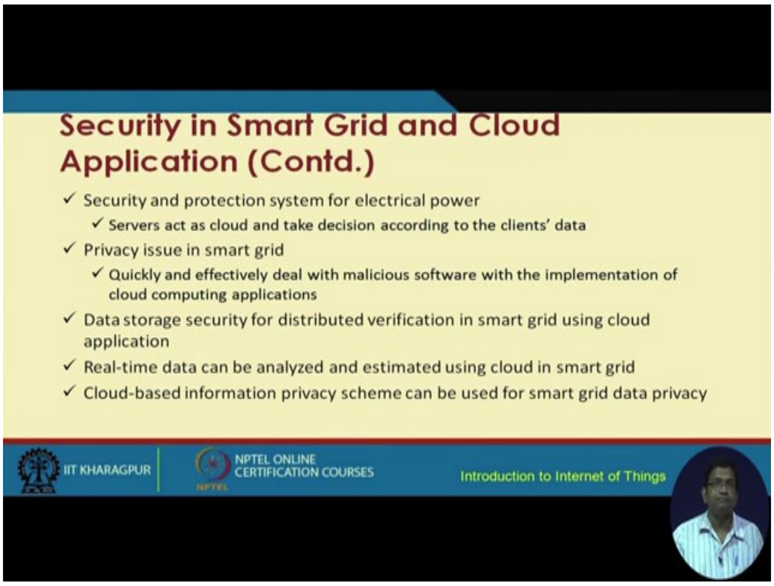
(Refer Slide Time: 27:01)



So, then comes the security aspects some of which I have already mentioned before. So, security in the smart grid is very important and electrical power system an electric power information security information security and protection system can be developed using the cloud security mechanisms private cloud platforms are suitable for scaling out and processing millions of data from the users and using the cloud computing platforms the electrical utilities can quickly and efficiently deal with malicious software.

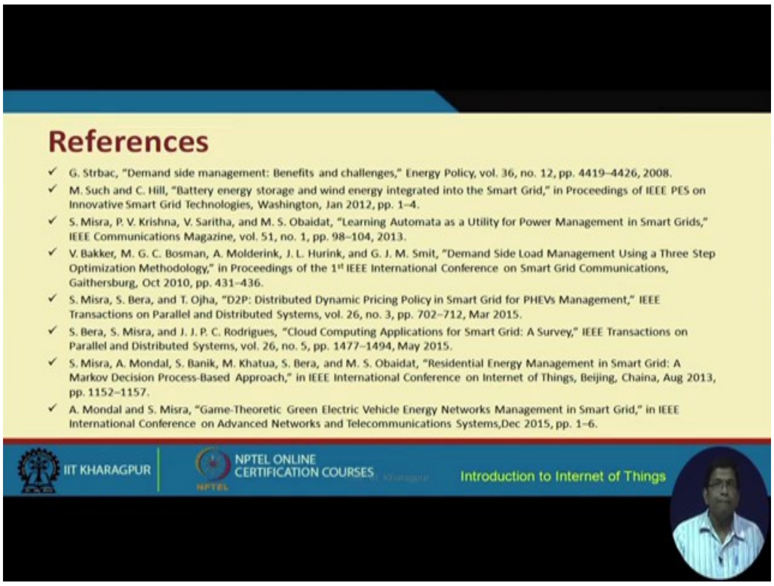
So, here you know this particular figure is very interesting to look at we have at the very bottom the users, the utility micro grid third party and through different authentication and authorization mechanisms these and in the interim we have this web services you know. So, these basically can feed in the data from these different devices authorized data in a secured data can be fed in you know and can be stored at the cloud end and the other direction also the same way because we have these different models of the cloud IaaS, PaaS and SaaS and these data can be basically you know shared bidirectional between these devices and the cloud models and that way these components the intermediate components and the layers can be made much more efficient and secure there by making the system much more secure than the traditional smart grid. So, cloud basically helps in this particular in the security process cloud basically helps in a big way.

(Refer Slide Time: 28:46)



So, security and protection system for cloud here we have the servers that act as the cloud and take decision according to the clients data their privacy issues in the smart grid that also can be can be used can be can be solved can be addressed by the help of the cloud in a much more better fashion, but again cloud security as cloud security and privacy particularly is also a very a important concern and so we have the privacy concerns in the case of cloud which are inherent to the cloud plus we have the privacy concerns in the case of the smart grid the traditional smart grid and how these 2 privacy concerns can be further addressed in an integrated way is something that different people different researches are looking into.

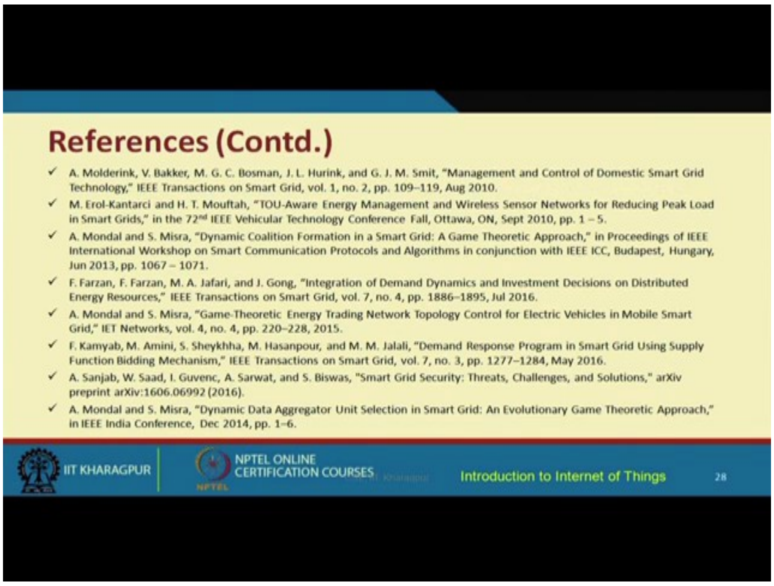
(Refer Slide Time: 29:40)



So, with this we come to an end here are some of the references for you to go through. So, this particular paper you know it is authored by me it is published by IEEE communications magazine and there are few other papers I was already mentioning about plug in electrical vehicles and plug in hybrid electrical vehicles this particular paper you can have a look at to understand how in the smart grid and PEV or PHEV context how dynamics pricing can be made possible this is one such solution which talks about it integration of cloud to smart grid this particular paper which is been published in the IEEE transactions on parallel and distributed systems.

This is a important this is a very interesting source I can say and this is one of the kind and you know. So, by going through this particular paper one can understand the different aspects of or the different challenges that are going to be phased by integration of cloud with the smart grid and different aspects like the how residential energy management can be done in the smart grid you know there is one such paper given over here and in vehicular energy networks you know how energy can be managed this is given in this particular paper at the end.

(Refer Slide Time: 31:06)



So, these are different papers that talk about different aspects the few other papers are also given over here very important papers are listed. So, one can you know if you if you are interested further interested to learn about smart grid you know these are the important rich sources of information about smart grid. So, what you must have noticed is you know. So, what I tried to do in this particular lecture is to you know keep our discussions at the level of motivating and trying to understand how smart grid is important, but we try to abstain ourselves from deeper discussions about how to build a smart grid. So, that is you know the; here basically you know our focus is not on how to build a smart grid, but what are the different aspects of smart grids.

Smart grids if somebody is interested you know particularly somebody from power systems background if they are interested to build a smart grid what are the different issues that have to be taken care of and so, these are the this is this is the focus of this particular lecture and how smart grid plays an important role in the IoT context because our course is on IoT; internet of things we do not want to really really understand deep into each of these technologies, but we want to get introduced about the different aspects smart grid is one such technology or one such aspect we wanted to understand. And so, this is the reason you know we try to keep ourselves at this higher level of understanding about smart grid and not deeper into how a smart grid can actually be built.

So, this basically requires you know building of a smart grid is a different semester course that can be you know that if somebody is interested with electrical engineering background they can attend, but this particular you know course because we are focusing on IoT we you know it is important to understand the different important subtleties that are involved in the building of the smart grid and why smart grid is required and what is the what is the motivation behind building smart grid in the IoT context. So, with this we come to an end of discussions on smart grid in the case in the context of internet of things.

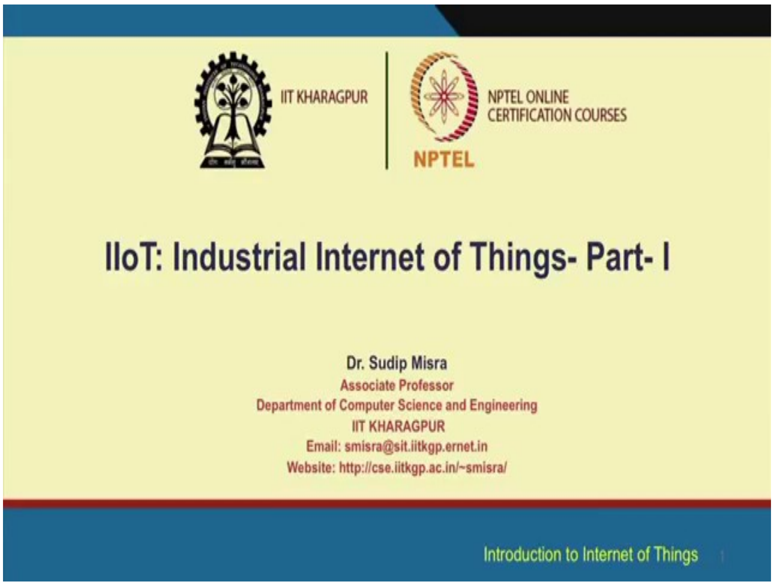
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 53
Industrial Internet of Things – Part – I

This lecture is on industrial internet of things which is popularly known as IIoT.

(Refer Slide Time: 00:23)



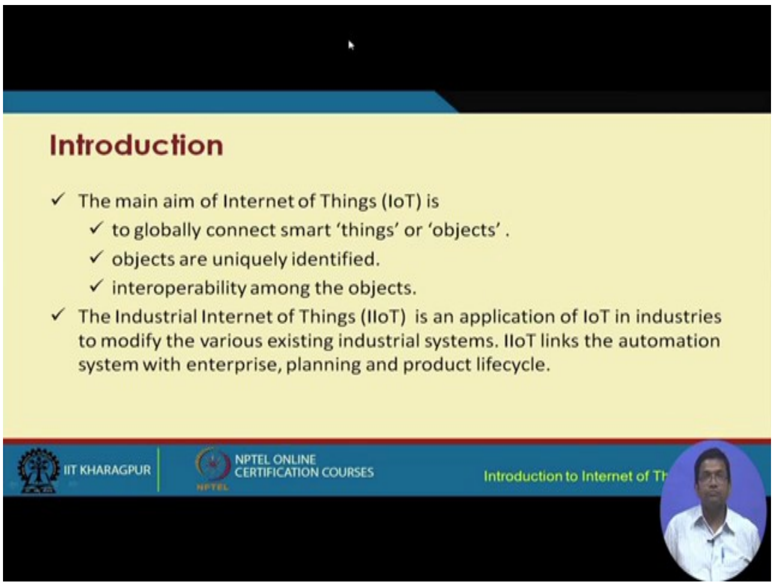
So, IIoT has differences with the existing IoT the popular IoT internet of things. So, industrial internet of things has a different scope and there are some specificities that are there in IIoT. So, we are going to understand in this particular lecture, what IIoT is how it differs from the regular IoT and how IIoT solutions are useful to real life industrial problems.

So, it is in two parts this particular lecture is in two parts the first part we are going to talk about some of the basics of IIoT.

(Refer Slide Time: 01:08)

So, we start with the quote by Paul Howarth and what he has said is that IoT as a concept has crossed the chasm from slideware to reality with many industries implementing IoT solutions. So, basically you know what it means is that IoT is no longer confined to theory and you know a height based a notion it is no longer like that you know. So, it is being used in reality in industries different IoT solutions are being implemented in the industry for solving different industrial problems to make industrial processes, manufacturing processes much more efficient then the way it is at present.

(Refer Slide Time: 02:01)

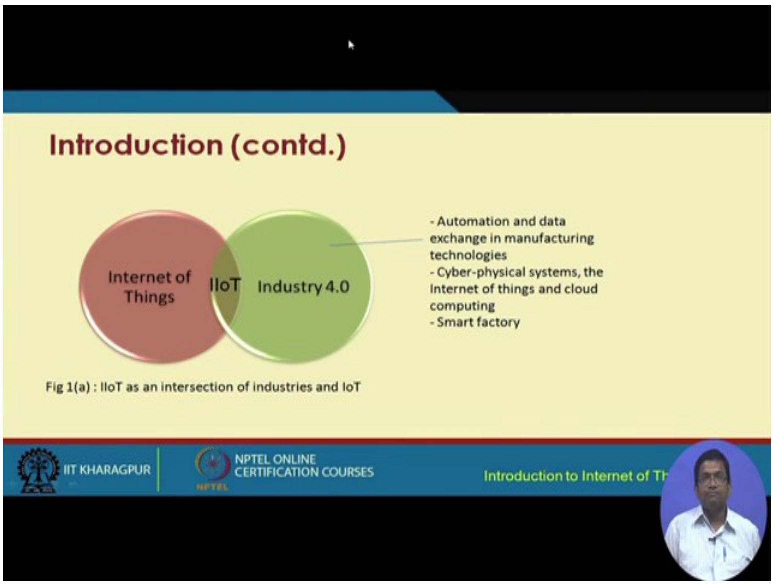


So, let us try to understand IIoT vis a vis IoT, as we have already understood through the previous lectures that the main aim of IoT is to interconnect different things and these things are different objects on the smart objects. So, what is required is to globally connect these smart object or the things so that the objects are uniquely identified and they are able to interoperate between themselves.

So, it is you know in an IoT in an IoT solution we what we have are different objects which are smart objects, where there is intelligence that are embedded in the different things. So, there are embedded systems that are attached to the different things the worldly things and these things they which have their abstraction as smart objects they are able to interconnect with each other they are able to internetwork with each other and so on.

So, in the contrast in industrial internet of things, we are focusing on industries particularly focusing on industrial systems, industrial automation enterprise, systems enterprise, planning product life cycle and so on. And while we do it we basically digress from the core requirements of IoT and there are some specific requirements which concern industrial processes that come into picture. So, we are going to understand what these are in this particular lecture.

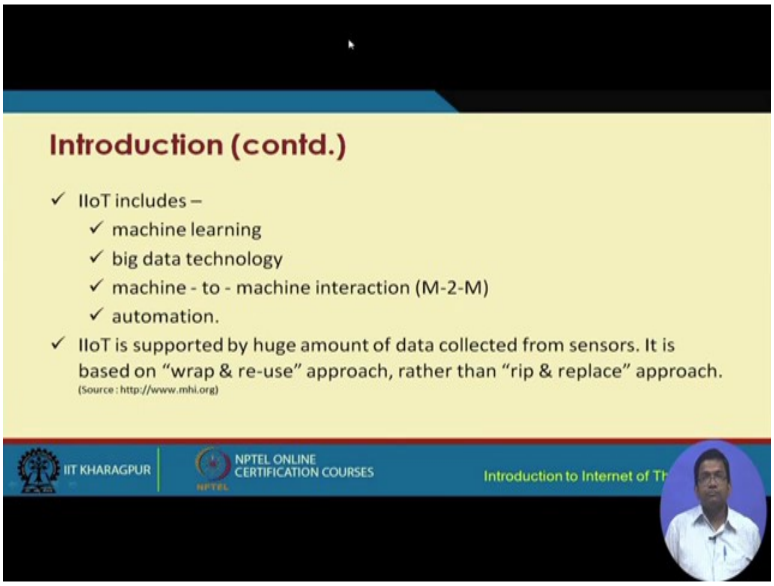
(Refer Slide Time: 03:47)



So, before that in terms of the scope of IIoT basically it borrows some of the features of the existing internet of things IoT, plus it borrows some features from the vision of industry 4.0. So, industry 4.0 basically gives a frame work for automation and data exchange in manufacturing technologies. So, it is a vision it is a way forward that has been proposed. So, industry 4.0 basically tries to improve the automation and data exchange in manufacturing technologies, it tries to incorporate concepts from cyber physical systems IoT cloud computing and so on. So, what we have essentially is what is well known as the smart factory.

So, IIoT basically takes some features from the regular IoT the conventional IoT, some from industry 4.0 and try tries to have a separate vision separate technology for itself. So, what we have we have already understood that whereas, IIoT combines features from IoT and industry 4.0, it is not IoT as such we have to understand this thing. There are certain features that have been borrowed from IoT, but it is not the IoT. IIoT and IoT are not the one and the same they are not where as IoT focuses on consumer level services consumer level products and so on. IIoT basically has the focus on the enterprise. So, the scope for IoT is consumer level where as the scope for IIoT is enterprise level.

(Refer Slide Time: 06:07)



So, things such as concepts technologies methodologies, such as machine learning big data technology M-2-M machine to machine communication, automation these are some of the integral components for building IIoT. So, machine learning I think we all understand machine learning is very very popular it is a part of artificial intelligence it is a kind of artificial intelligence. So, which basically now learns you know. So, learning form the past and there are different things you know. So, there are different aspects of machine learning.

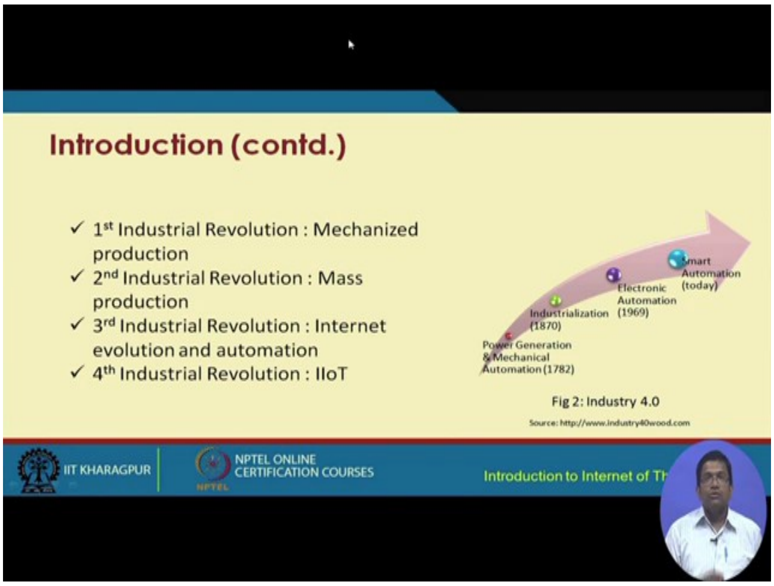
So, learning from the data; the existing data and trying to make things predictive and trying to have things which are better in the future; so, machine learning techniques and technologies are used big data, we are going to talk about big data later on. So, in another lecture we are going to talk about big data how to handle big data what are the tools that are available. So, we will talk about that when we talk about data handling and data analytics.

Then machine to machine interaction machine to machine communication is about two machines directly talking to each other, directly communicating with each other getting a particular work or a task accomplished without any human intervention without any human intervention. So, for example, a robotic arm opening the door of a refrigerator and then performing certain other tasks in the refrigerator that is an example of machine to machine. So, may be the robotic arm goes and opens the door of the refrigerator checks whether there is sufficient milk in the milk pot of the refrigerator or not if there is no if there is no sufficient milk, then the system as a whole will send or the milk pot or the refrigerator will send an SMS to the milk person.

So, what is happening in the entire processes there is no human intervention. So, we have machine communicating with machine, another machine communicating with another machine and so on we have machine to machine communication M-2-M without any human intervention. So, going back we have machine to machine communication and automation. So, these are the different features different aspects of IIoT. So, IIoT is supported by huge amount of data collected from sensors, it is based on wrap and reuse approach rather than rip and replace approach.

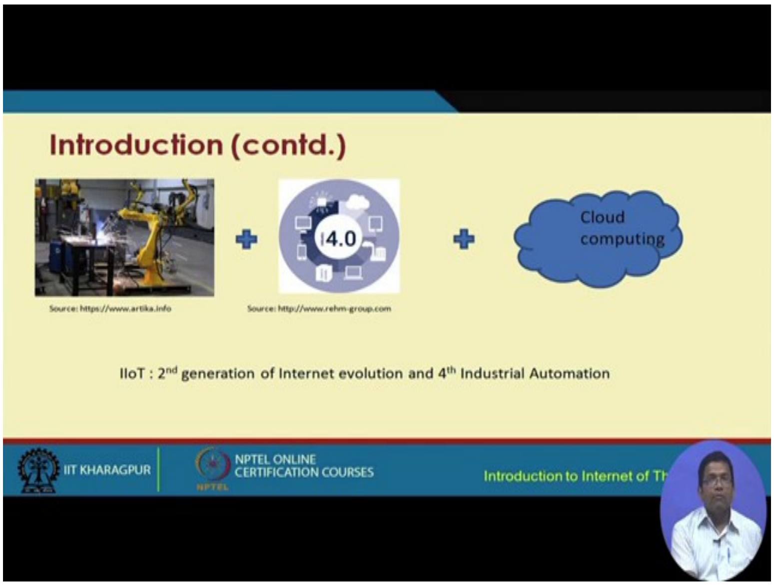
So, what is meant by these terms is when we talk about IIoT, we are not talking about building a new system from scratch, we are talking about using the existing manufacturing systems, existing industrial systems you know rap them with sensors actuators and so on and make things efficient. We are trying to reengineer the existing systems and the processes and we are not building anything brand new from scratch. So, this is what we have to remember when we discuss IIoT.

(Refer Slide Time: 10:01)



So, let us try to understand the revolution of IIoT. So, the first industrial revoluation happened with mechanized production, then came mass production which is the second industrial revolution in the third industrial revolution internet and automation was featured in manufacturing and at present what we have is the fourth industrial revolution which incorporates IIoT. So, IIoT is featured as part of the fourth industrial revolution. So, if we look at this particular figure what we have starting from 1700 when there was power generation and mechanical automation, then came the 1800s industrialization, in 1900s we had this electronic automation and at present we have smart automation and this is what this is how the industry 4.0 evolved today. So, in industry 4.0 we have smart factories and so on in the industrial sector.

(Refer Slide Time: 11:21)

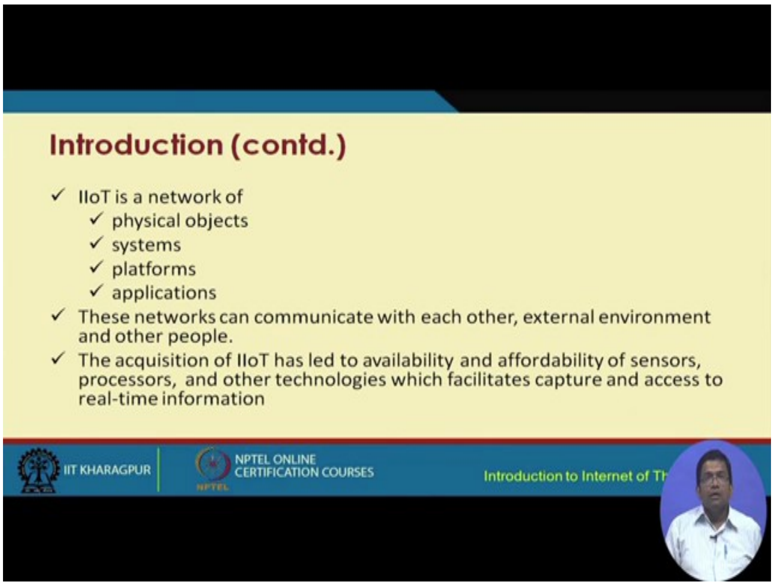


So, when we talk about IIoT it is about fourth generation of industrial automation; that means, industry four 4.0 clubbed with the second generation of internet evolution. So, internet at present; so, the first generation of internet is the internet that we all use the regular internet with connects different computers throughout the world this is the first generation of the internet. Second generation of the internet is about connecting different things, connecting different machines and so on.

So, IIoT basically combines the second generation of internet, fourth generation of industrial automation and cloud computing. So, cloud has become very popular technology since about more than half a decade or so, cloud has become very popular it is being used in the industrial sector as well. So, what happens is cloud basically offers computational environments, computational infrastructure, computational platforms, computational software in addition to regular storage. So, cloud is like a huge data storage, which can store lot of data. And all these things huge data storage coupled with you know infrastructure, software, platform, hardware and so on and so forth. Everything one can get access to in an industry without basically having to purchase these of their own right.

So, cloud computing is very popularly used not only in others spheres of everyday life, but also in the industry.

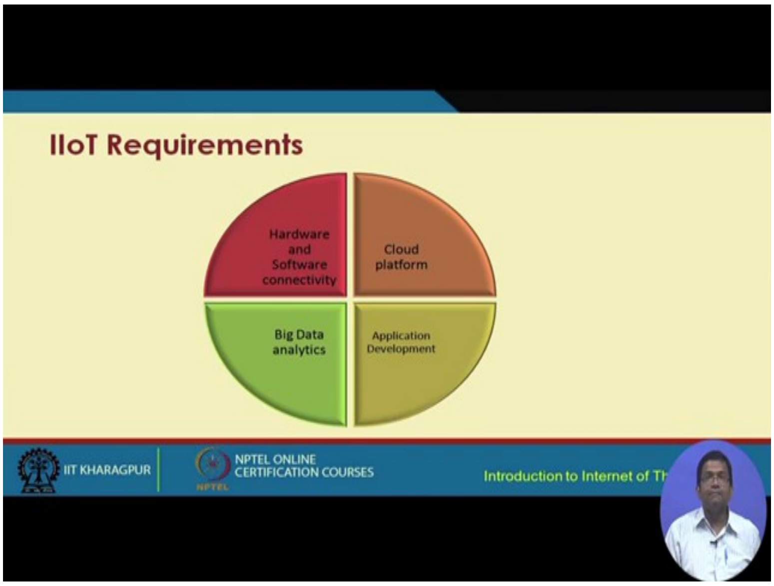
(Refer Slide Time: 13:46)



So, in the IIoT network we have physical objects that are interconnected, we have different systems subsystems that are interconnected, there are different platforms types of platforms that work together, different applications and so on. So, these networks are IIoT networks can communicate with one another, the external environment they communicate with the external environment and different people. So, people are also part of these IIoT networks. So, there are different peoples the different end users stake holders everybody at the enterprise enterprise level you know everything that is there they all form part of IIoT; they have to be internetworked of course, they have to be connected these things the things people processes everything together connected.

The acquisition of IIoT has led to availability and affordability of sensors, processors and other technologies, which facilitate capture and access to real time information. So, all these IIoT devices and where ever they are deployed through sensors, sensors have become affordable they are readily available nowadays, the different processes, other computers other computing devices technologies and so on. They capture lot of data and they offer the data in real time for further analysis; making making things much more efficient from the data that is collected.

(Refer Slide Time: 15:26)



Moving ahead, IIoT for building; IIoT there are 4 broad requirements. We need the hardware and software connectivity, we need a cloud platform and I already told you briefly about the necessity of cloud in the industrial sector and how cloud can help with respect to processing infrastructure data storage and so on and so forth. Application development and big data analytics; big data analytics is very important all these different sensors in the industrial sensors the actuators that are fitted to these different machines, manufacturing equipment and so on. They throw in lot of data they throw in lot of data and that data is very important is very crucial, it can reveal a lot of information and that by mining that data one can predict different things in a to make these industrial processes much more efficient.

(Refer Slide Time: 16:35)

Different other views of IIoT requirements; one is access, access with respect to any time anywhere, anything connectivity and anything connectivity is very important it is a third dimension that has been added to any anytime, anywhere which was the you know pervasive which was the vision of pervasive communication, pervasive systems. So, access can you know one can have access anything can be accessed at anytime from anywhere in IIoT. End to end security is important and that is not only important for IIoT, but for any IoT based system. In fact, for any computer based system.

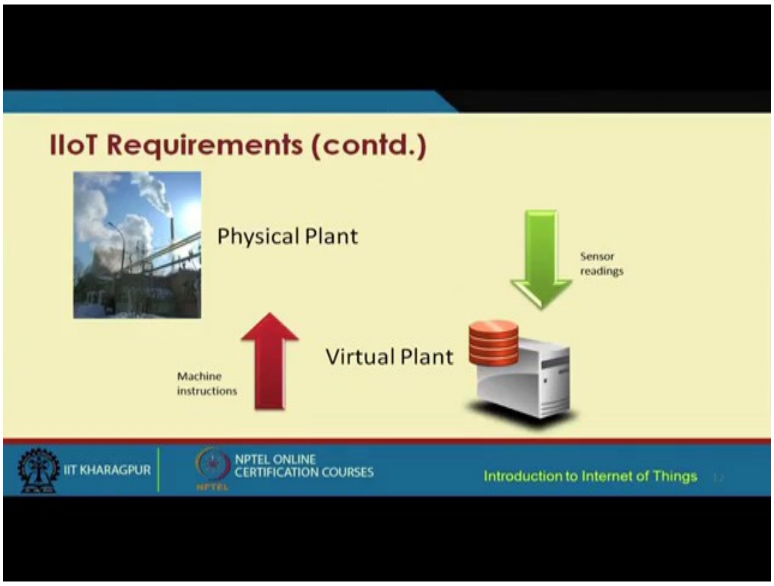
User experience is very crucial; you know ultimately it is all about offering services to the user's different stake holders. So, user experience has to be taken into account as one of the fundamental requirements for building IIoT. So, what the users exactly want, how they are problems can be addressed how it can be solved the problems can be solved, and how through the use of the system that is being developed the IIoT system that is being developed the users can do things better, and how their experience as a whole can be improved.

Transition to smart machines; so, machines by adding sensors actuators etcetera we are making the machine smart. We are making the machine smart. Asset management is very important though assets management you know though these different sensors actuators etcetera the assets can be managed the industrial assets can be managed in a much more efficient way. So, how the assets can be managed this is one of the requirements that have to be considered for building IIoT systems.

Big data and cloud are very important cloud offers storage computational efficiency and so and so forth. Without basically having one to procure and by procure and deploy this computational infrastructure at their own workplaces or industrial in the industry and big data you already told you that all these sensor actuators and each and every thing that we have talked about so far, the enterprise level at the enterprise level the people process things systems and so on and so forth. They are going to throw in a lot of data these data are going to be sent quite the data are going to be sent in real time and they have characteristics they are not only big in volume, they have they come in huge velocities and you know they there are different types of data test data, speech data, multimedia other types of data like images video etcetera all of which coming at the same time it has to be handled and so on.

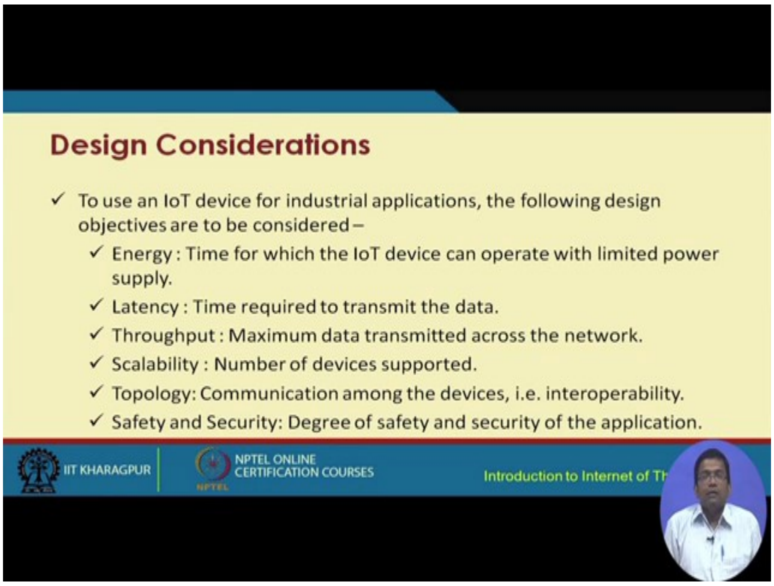
So, this is what we are going to cover in one of the next lectures, when we talk about how to handle data handling and how to analyze the data that is received.

(Refer Slide Time: 20:00)



So, what we what is required is to have a virtualized version of a physical plant. So, through IIoT systems what we are trying to build is a virtualized plant corresponding to a physical industrial plant. So, these physical plant and the different machines in the plant are fitted with different sensors which throw in lot of data the sensors readings, and from these virtualized plant lot of different types of instructions can be sent to the physical plant and the embedded systems that are attached to these machines to these instructions can help to maneuver to perform different operations on these machines.

(Refer Slide Time: 20:58)



There are different design considerations for building IIoT, to use an IoT device for industrial applications, these design objectives have to be considered. Energy is paramount energy with respect to the time for which the IoT device can operate with limited power supply. So, we have limited power supply and we want to extend the lifetime of the IoT device that is installed that is fitted with an industrial machine.

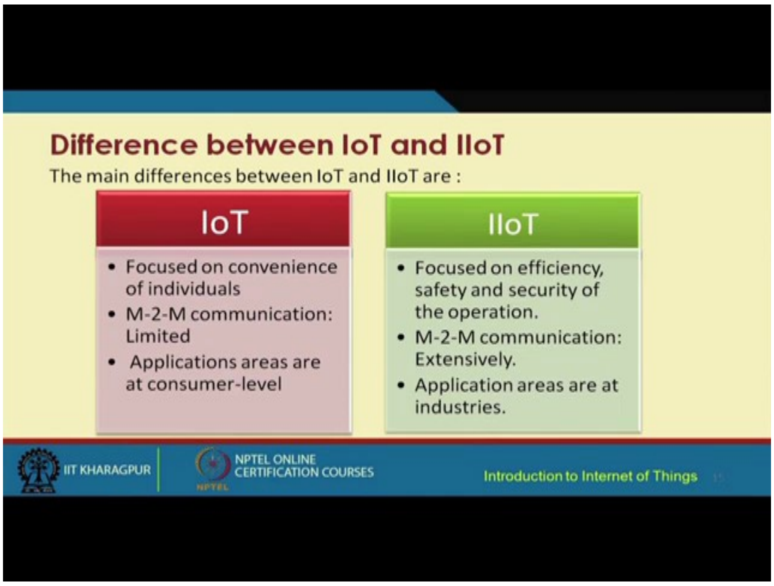
Latency is very crucial it corresponds to the time that is required to transmit the data latency has to be minimized. Because let us say that we are talking about sensors that are fitted to a welding machine. So, you see that if latency is not very minimum then what is going to happen by the time the instruction reaches the machine or you know the data is sent to the operator or from the operator to the machine, what happens is the welding machine might have performed more welding. Even in a fraction of a second. So, you know. So, more part will get welded which is not required.

So, precision with respect to the time is very crucial and when you talk about that latency of operations, latency in the transmission of the data is very crucial, latency has to be minimized to the extent possible. Through put is quite understandable we need maximum data to be transmitted across the IIoT network, scalability likewise is very understable we are talking about not just one or two machines, but large number of machines in the IIoT sphere.

Topology how these different because you know ultimately what is going to happen is this sensors and this communication devices, they have they are going to be internetworked. So, what we are going to have is a network topology and in this particular network topology we have different devices with different specifications, and they have been manufactured individually by different vendors. So, interopreability is very important not only that interoperability is important, but how these devices form the network is very crucial as well. So, the overall network topology formed out of the devices and how these devices interoperate with one another is something that has to be taken as one of the important primary design considerations in building IIoT.

Safety and security likewise I do not need to elaborate further, but are very important issues that also have to be taken into considering industrial safety you know. So, we need to understand this thing properly. When we are talking about automation as a whole in the industry it should not happen you know. So, things have to very reliable, the systems have to be very reliable it should not happen that the sensor is giving a wrong reading because of which a crankshaft or in a some of fuel you know goes through causing accident to the people who are working in the plant right. So, industrial safety is very important. So, IIoT system automation you know systems which offer automation etcetera they have to be very much reliable, and they have to take in to account the degree of safety and the security of the application.

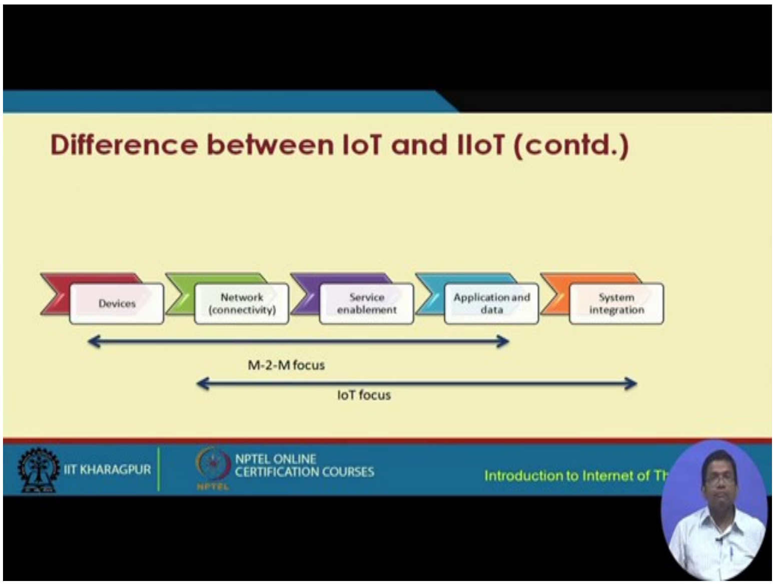
(Refer Slide Time: 25:00)



So, going back trying to understand IIoT vis a vis IoT. So, whereas, IoT traditionally focuses on the convenience of the individuals, IIoT focuses on the efficiency safety and security of operation. In terms of the machine to machine communication and machine to machine communication I already spoke about earlier, in terms of machine to machine communication IoT definitely uses machine to machine communication, but it is not very exclusive you know the use of IoT machine to machine communication in IoT is limited whereas, IIoT extensively uses machine to machine communication M-2-M communication is extensively used in IIoT the whole industrial operation in a plant is automated. So, one machine talking to another machine second machine talking to third to fourth and so on this is quite extensive it is quite present in the industrial sector IIot. So, IIoT heavily depends on machine to machine communication.

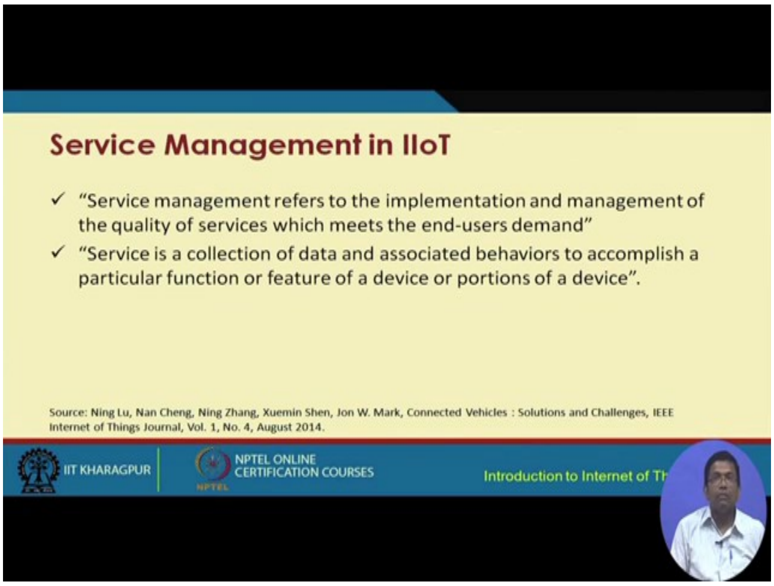
So, whereas, IoT traditionally focuses on applications at the consumer level, IIoT basically focuses on applications at the industrial level at the enterprise level.

(Refer Slide Time: 26:34)



Let us look at one more aspect. So, here M-2-M when we talk about M-2-M. So, M-2-M and IoT. M-2-M focuses on device to device communication, there is a emphasis on communication between devices between machines, and IoT on the other hand focuses on the overall system integration of the system components sub components sub systems integration is a one of the important features of IoT. So, this is what we need to understand. So, M-2-M versus IoT. M-2-M focus on devices of course, both of both M-2-M and IoT they have focus on other aspects like network connectivity service enablement application and data these are there for both M-2-M and IoT whereas, M-2-M focuses on particularly on devices. IoT basically focuses more on the system level integration.

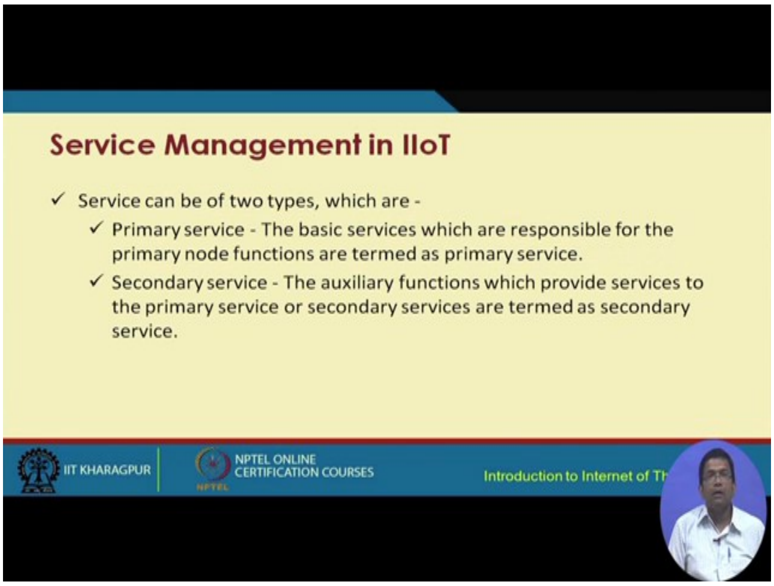
(Refer Slide Time: 27:51)



Now, service management in IIoT is very important it is all about why do you want IIoT we want to offer improved services. So, service management is very crucial. So, service management basically what it is referring to is the implementation and management of the quality of service, which meets the end user demand end users demands are met and increasing the overall quality of service?

So, service is basically a collection of data and the associated behaviors to accomplish a particular function or feature of a device or portions of a device. So, through IIoT solutions the overall services the management of the different services have to be improved.

(Refer Slide Time: 28:44)



So, I will talk about very briefly over here services can be of two types one is the primary service the other one is the secondary service. Primary services are basics services which are responsible for the primary node functions whereas, the secondary services are auxiliary services auxiliary functions which provides services to the primary service or secondary services are termed as secondary service right. So, what we have primary service are basic they are very important, you know you need those services whereas, secondary services are auxiliary services which may or may not be there.

So, with this we come to an end of the first part of IIoT, we have understood the basics of IIoT, how IIoT differs from IoT, what is the difference between IoT and M-2-M. So, this; what we have looked at in in this part of the lecture on industrial internet of things.

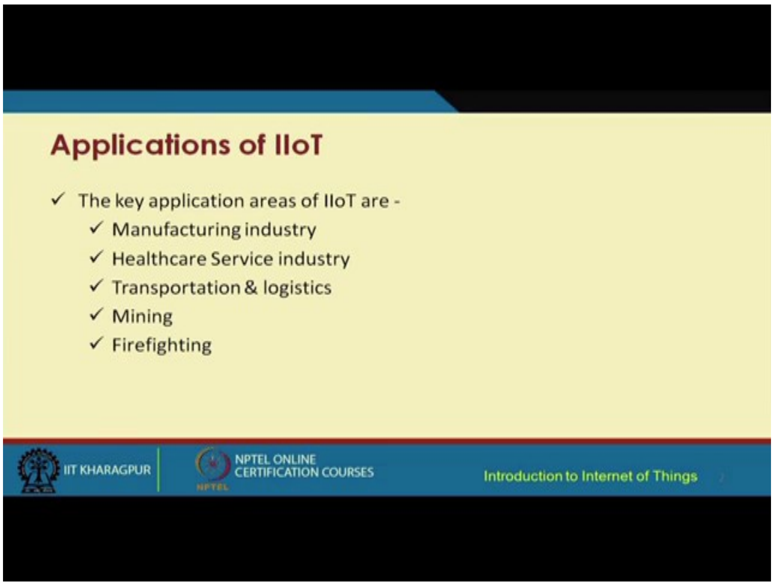
Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 54
Industrial Internet of Things – Part – II

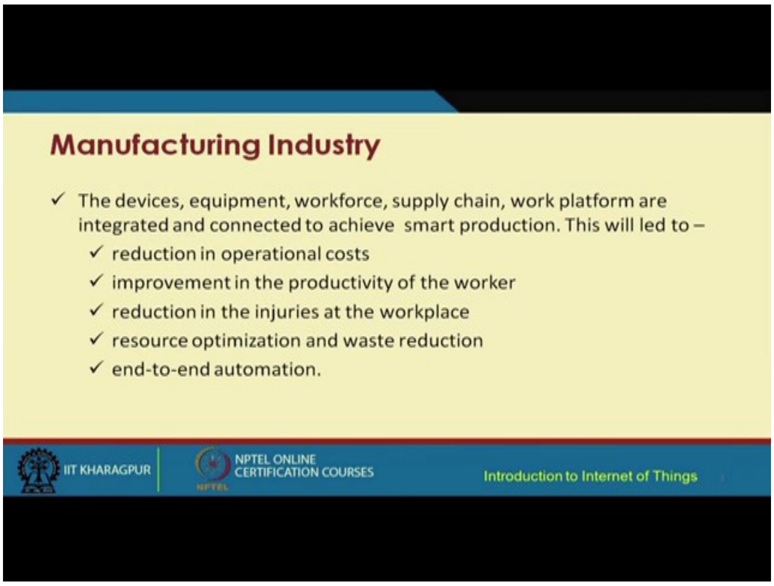
So, let us now continue our discussion of industrial IoT. So, earlier we understood the basics of IIoT, how IIoT differs in principle from regular IoT what is the difference between IoT and M-2-M and having understood all of these different basic concepts we are now about to understand that what are the specific applications of IIoT in the industrial sector.

(Refer Slide Time: 00:54)



So, some of the key application areas of IIoT are manufacturing industry, health care industry, transportation and logistics mining and firefighting.

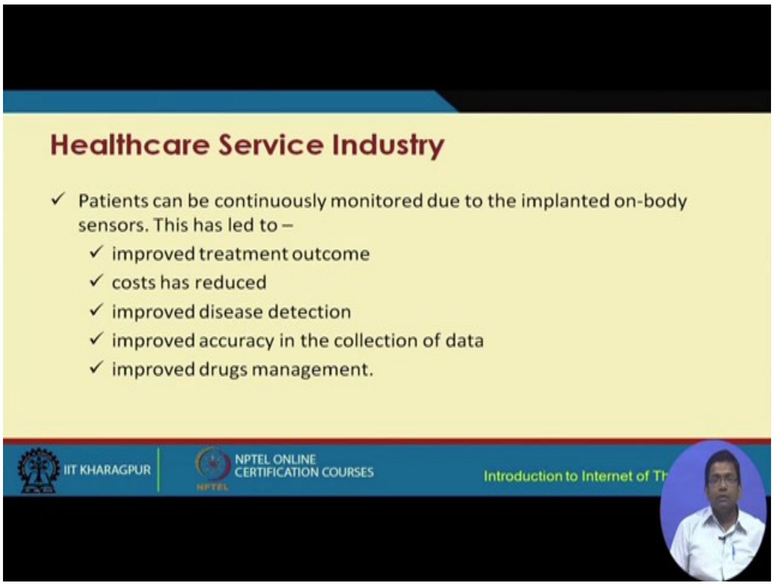
(Refer Slide Time: 01:06)



In terms of manufacturing in a manufacturing industry there are lot of manufacturing devices there are equipments work force supply chain work platform different work platforms are there. So, these have to be integrated and connected to achieve smart production. So, they have to be internetworked. So, we have different manufacturing machines manufacturing devices equipments work force then the entire supply chain manufacturing supply chain from production to the end users the entire supply chain and then the work platform. So, all of these have to be integrated and connected to improve the production overall industrial production.

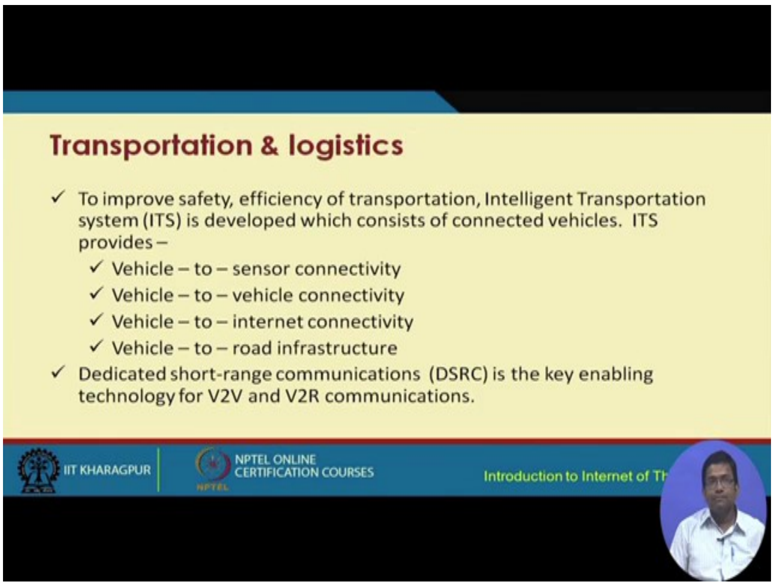
So, these have to be done in order to reduce the operational costs improve the productivity of the worker reduce injuries at the workplace this is very important actually safety applications of IIoT are very important these are very interesting and these are very popular safety applications. So why we want to use IIoT is one of the important applications is to improve the safety in the manufacturing plant in the industrial different other types of plants. Resource optimization and waste reduction is also very important industrial you know this is a very important problem resource optimization is a very important problem in a industrial engineering. So, this has to be taken care of waste reduction as well and end to end automation. So, this is very important in it is a very important requirement in the manufacturing industry and it has to be taken care of.

(Refer Slide Time: 03:17)



In the second application of IIoT is in the health care sector. So, you know using IIoT solutions patients can be continuously monitored due to the implanted on body sensors which can improve the treatment outcome overall costs of treatment can be reduced, improved disease detection can be done and improved accuracy from the data; that is that are collected can be achieved an overall the drugs drugs that are administered on the patients and the overall inventory. The control of the drugs, the procurement control storage and so on of the drugs they can be improved.

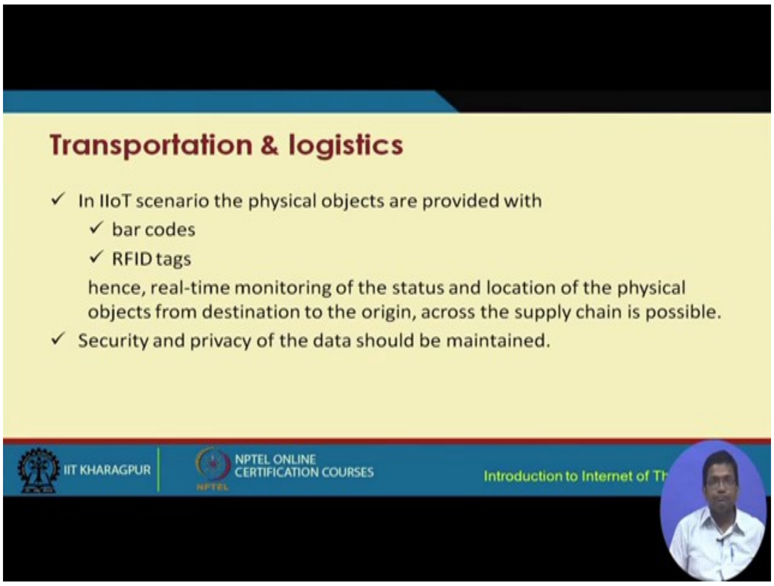
(Refer Slide Time: 04:08)



So, IIoT solutions are very attractive in the health care sector in the transportation and logistics sector as well in order to improve transportation safety, efficiency of transportation, intelligent transportation systems can be developed which consists of connected vehicles. So, one of the key building blocks for transportation IIoT applied to transportation is the concept of intelligent transportation system or connected vehicles. So, intelligent transportation systems come in different forms we have the concepts of in its we have the concepts of vehicle to sensor connectivity, vehicle to vehicle connectivity, vehicle to internet connectivity and vehicle to road infrastructure connectivity.

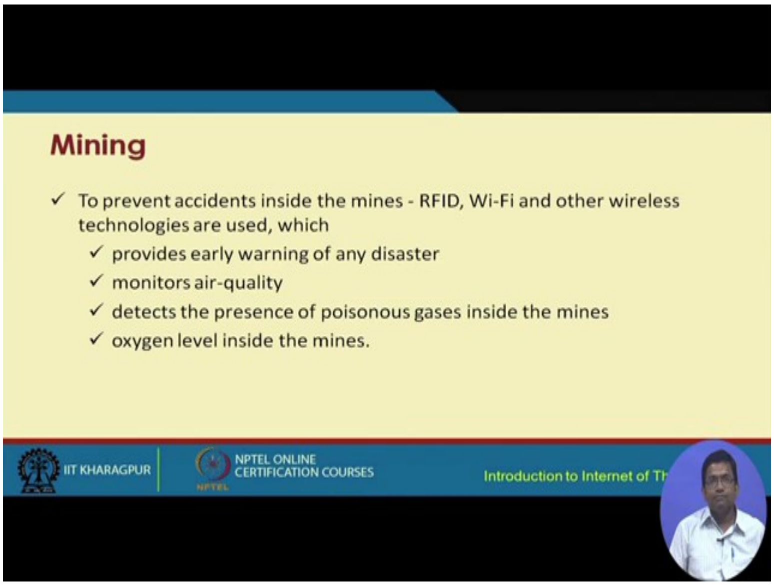
So, there are different types of connectivity's that are required in its there is short range communication in the form of DSRC that enables the realization of vehicle to vehicle and vehicle to road infrastructure communication V2V, V2R sometimes it is also known as V2I, V2 Vehicle to infrastructure communication.

(Refer Slide Time: 05:37)



So, DSRC is very important key enabling technology for achieving the objective of vehicle to vehicle and vehicle to roadside infrastructure communication. In IIoT scenario the physical objects are provided with bar codes RFID tags. So, that real time monitoring of the status and location of the physical objects may be the trucks where they are what you know what is the condition of the different goods that are carried in the trucks all of these things can be monitored in real time from the origin irrespective of where the trucks are entire supply chain can be monitored with IIoT solutions entire supply chain the status of the good that status of the vehicle you know everything can be monitored.

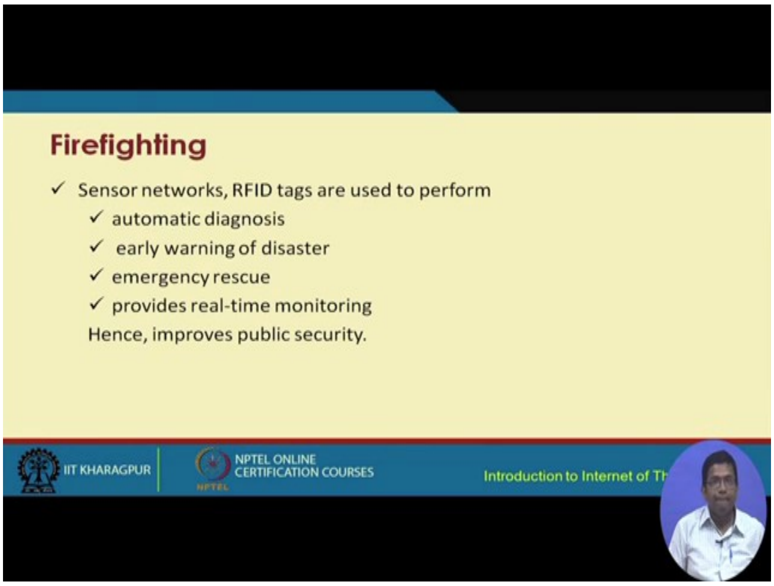
(Refer Slide Time: 06:30)



Security and privacy of the data should also be maintained and that is quite obvious I do not need to elaborate further on this particular aspect. In the mining industry very important industrial IIo, sorry industrial IoT solutions are very important in the mining industry it is very common to have different types of accidents in the mines. So, RFID based solutions are Wi-Fi and different other sensors and other wireless technologies Zigbee, Bluetooth, etcetera can be deployed to collect data to provide early warning before any disaster actually strikes can be used in the mines to improve to monitor not improve, but monitor the air quality what is the air quality

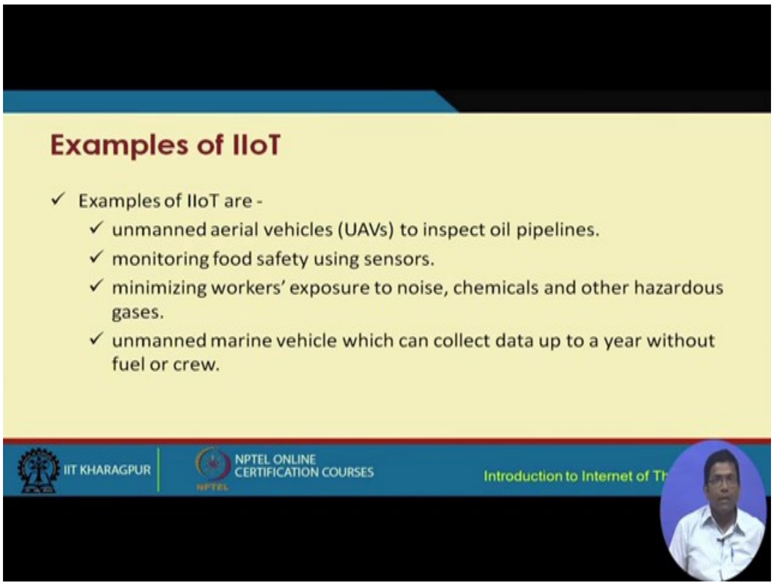
And this is the very important problem in the mining sector you know monitoring the air quality inside the mine detecting the presence of different types of poisonous gases SOx gases NOx gases and you know different other poisonous gases like carbon mono oxide and so on inside the mine which is a very common problem. How much is the oxygen level inside the mine? So, all of these things can be monitored inside the mines using IIoT solutions.

(Refer Slide Time: 07:47)



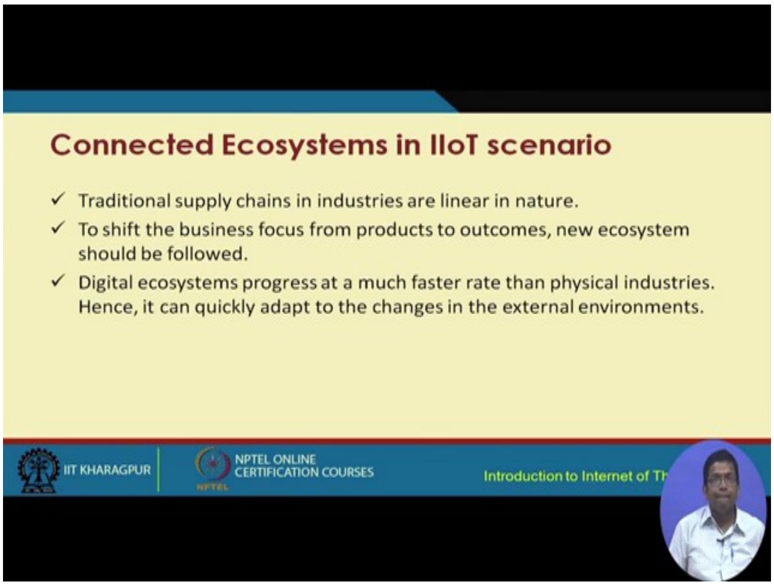
Firefighting is another RFID tags can be fitted to these different devices for firefighting for automatic diagnosis early warning in the you know in the firefighting in the fire infrastructure that are deployed typically in the buildings different RFID tags different sensors can be fitted to these you know fire detection devices emergency rescue and providing real time monitoring. So, all these will improve the overall overall security and safety of public infrastructure.

(Refer Slide Time: 08:37)



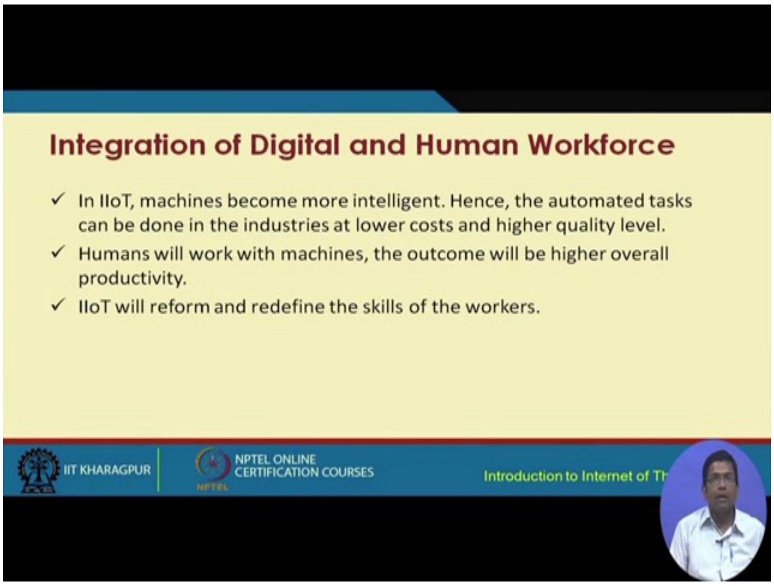
So, some of the examples of IIoT include use of unmanned aerial vehicles or the drowns to inspect oil pipelines monitoring food safety using sensors minimizing workers exposure to noise chemicals hazardous materials and so on unmanned marine vehicles can be deployed to collect data you know annually or throughout the year throughout the months and so on without any fuel or crew.

(Refer Slide Time: 09:12)



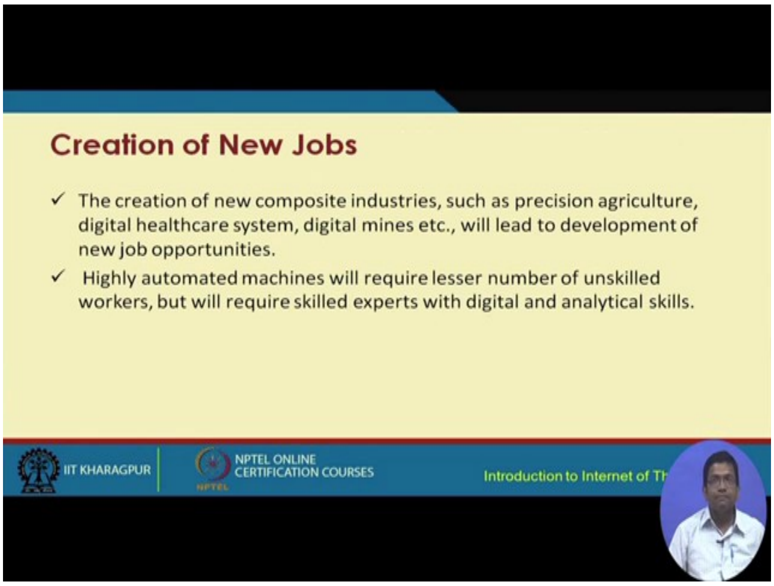
So, what we have are connected ecosystems in the IIoT domain. So, what we have is we have traditional supply chains and these traditional supply chains in these industries are linear typically linear in nature. So, it is required to shift the business focus from products to outcomes and for that these digital ecosystems can come IIoT based digital ecosystems can come to rescue. So, digital ecosystems progress at much faster rate than the physical industries. Hence it can quickly adopt sorry adapt to the changes in the external environments.

(Refer Slide Time: 09:57)



So, it is required to integrate digital technologies with the human work force. So, you know IIoT cannot be exclusively M-2-M this we have to remember we have to have humans in the loop. So, humans will work with machines and the overall outcome will be improved productivity of the system.

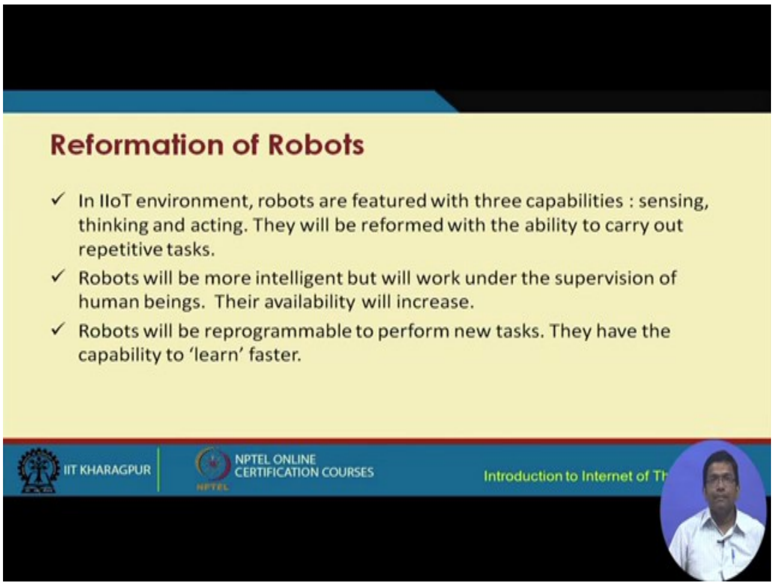
(Refer Slide Time: 10:26)



So, IIoT will reform and redefine the skills of the workers. New jobs can be created with the help of IIoT it is not that you know typically people think that automation or IIoT based solutions will cut down on the number of jobs, but that is not true. So, jobs new jobs get get created because you know new technologies get introduced.

Things like a you know new composite industries precision agriculture digital health care digital mines these require you know skilled man power and these skilled man power is what is required and you know this automation through IIoT is in turn going to create new jobs with requiring new skill sets and you know. So, this basically you know IIoT will not cut down on the required number of jobs in the industries.

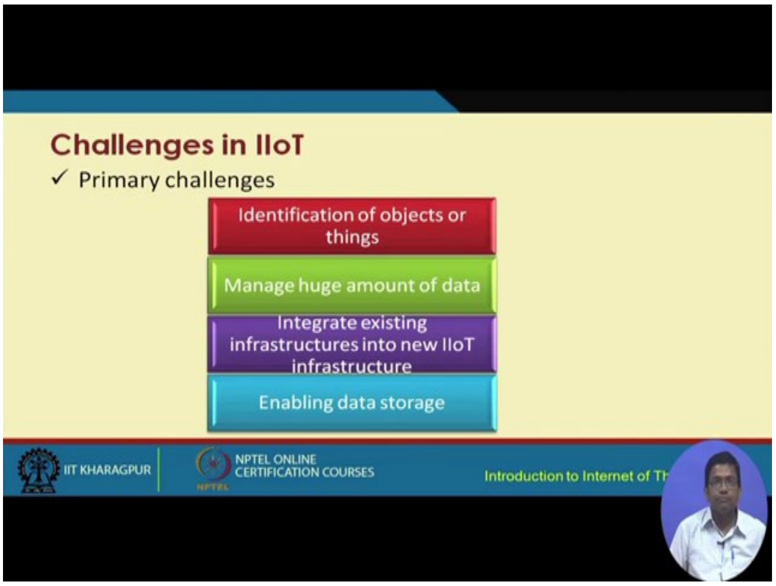
(Refer Slide Time: 11:29)



Robots robots have traditionally been used in the industry and in IIoT robots are a very important component you know in a new form in a new way robots can be used and these robots can sense they can think they can act they can perform different tasks. So, they will be formed with the ability to carry out repetitive tasks robots will be more intelligent they are more intelligent and they walk under the supervision of, they can also work under the supervision of human beings their availability increases and they can be programmed reprogrammed and so on and so forth to perform new tasks and that way they can learn faster.

So, robots in a reformed manner can be used in the IIoT to perform the industrial processes in a much more efficient manner in much more faster way decisions can be made and so on; over all improving the industrial processes industrial you know efficiency industrial safety and so on.

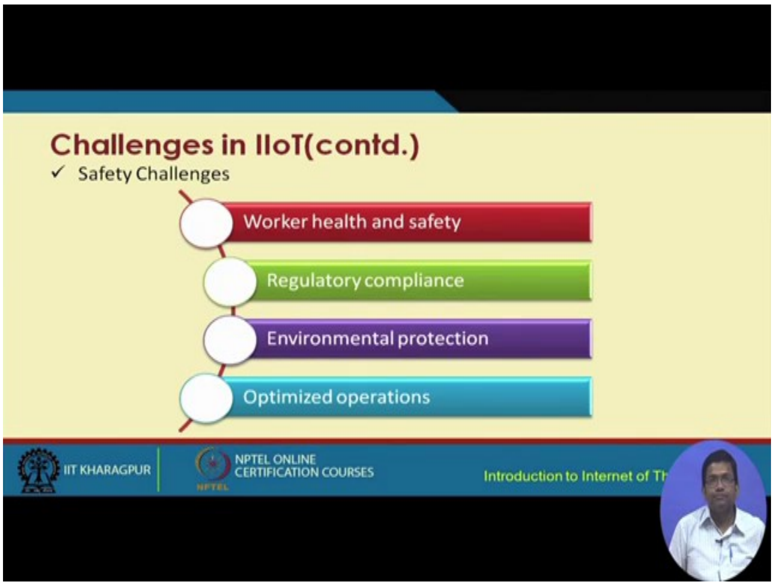
(Refer Slide Time: 12:42)



So, some of the challenges of IIoT, building IIoT are listed over here identification of objects or things is important and we already looked at the identification of these things you know how do you associates identifiers to these things we have already looked into these in the context of regular IoT and the same applies here as well.

Managing huge amount of data is another challenge to be worked on in order to address the problems of IIoT in order to deploy IIoT solutions integrating existing infrastructure into new IIoT infrastructure and enabling data storage these are some of the challenges behind IIoT. There are safety challenges as I told you before safety is very important. It is a fundamental problem in the industry in the industrial sector safety is crucial.

(Refer Slide Time: 13:31)

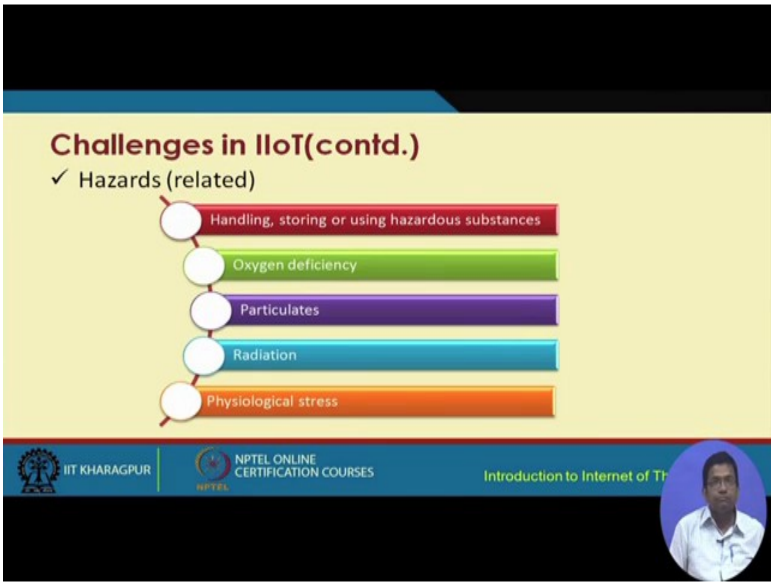


So, whether we are talking about the health care industry because you know in the health care industry as well in the hospitals and health care workers they are exposed to lot of problems they are exposed to lot of challenges and which can harm their health and so on.

The same thing for if we are talking about mining industry if we are talking about the transportation industry if we are talking about the steel industry and different other industries there are lot of safety challenges that are there and so, workers health and safety are of primary concern in this industry. So, worker health and safety regulatory complains there are different regulatory bodies in a requiring you know complains of the machines the people their processors in the industry and so on. So, these and regulatory compliance with respect to safety particularly is very crucial.

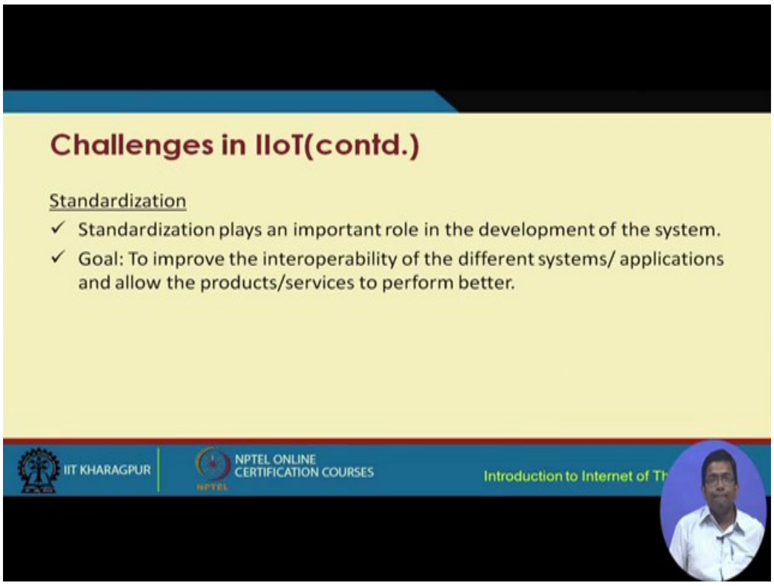
Environmental protection is very important you know industries and environment they often do not go hand in hand. So, lot of challenges exist and lot of challenges are posed by the industries on the environment in which they work then optimized operations. So, these are some of these challenges particularly concerning safety in industrial safety that have to be taken care of through IIoT solutions.

(Refer Slide Time: 15:21)



There are different hazards as well handling of different hazardous substances storing of the hazardous substances and so on oxygen deficiency particulate matters. So, particulate matters like you know fly ash and so on then radiation different types of radiation electromagnetic radiation and so on and physiological stress all these are different types of hazards.

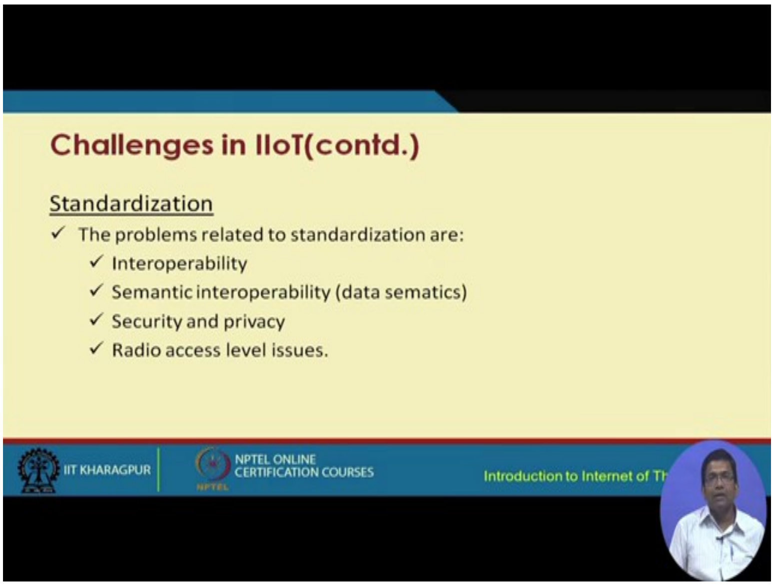
(Refer Slide Time: 15:55)



That have to be taken into consideration for offering challenges through the use of IIoT. Standardization is very important in the development of any system. So, in the context of

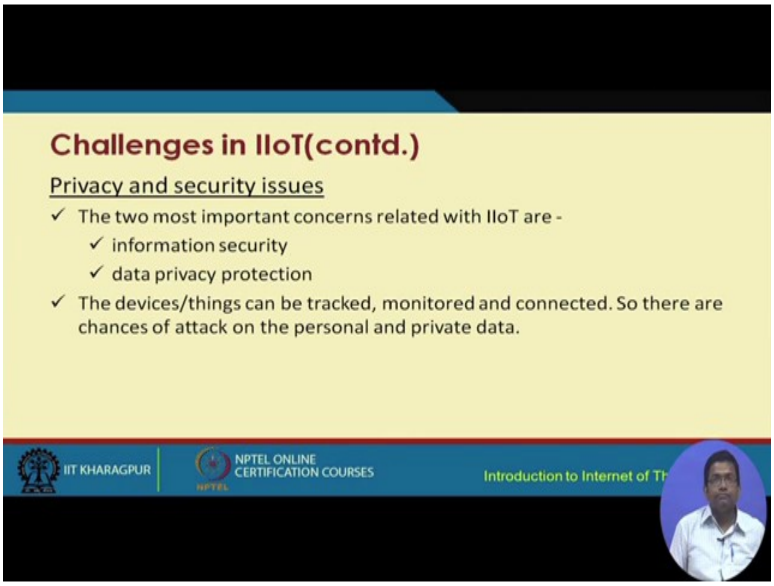
IIoT what is required is to improve the interoperability of the different systems applications and allowing the products and services to perform better.

(Refer Slide Time: 16:12)



In terms of standardization the problems related to standardization include interoperability semantic interoperability. So, there is a difference. So, in semantic interoperability basically one is focusing on data semantics. So, the meaning; so, the you know interoperability in terms of semantics is what semantic interoperability specifically takes care security and privacy and radio access level issues.

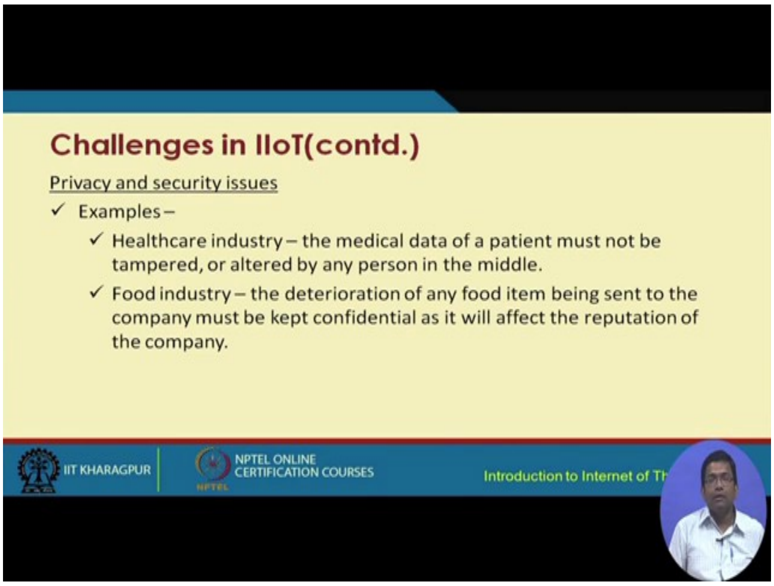
(Refer Slide Time: 16:42)



There are different privacy and security issues as well the two most important concerns needed with IIoT are information security and data privacy protection the devices and the things can be tracked monitored and connected. So, they there are chances of attack as it happens in any other type of network as well this IIoT is also a network; it is a huge network where different machines crucial machines there are different systems humans everybody is connected.

So, these are prone to different attacks there could be different vulnerabilities in these networks. So, consequently, you know. So, these has to be taken care of the security issues have to be taken care of privacy is very crucial because from the industry there are different data the sensors are collecting.

(Refer Slide Time: 17:44)



So, the privacy of these data have to be take care of. So, information security data privacy protection all these are very crucial issues in the context of IIoT building of IIoT.

So, for example, in the health care industry the medical data of the patient must not be tampered or altered by any person in the middle in the food industry the deterioration of any food item that is being sent to the company should be kept confidential as it will affect the reputation of the company.

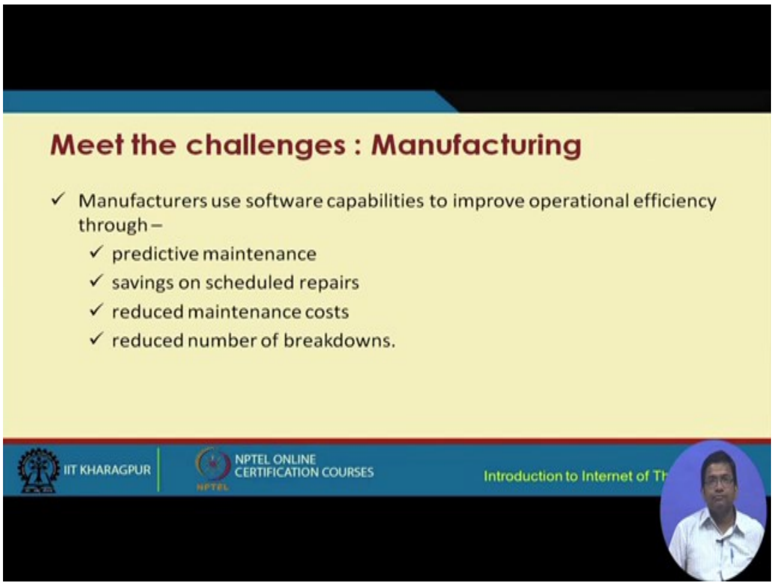
(Refer Slide Time: 18:13)

So, these are very important you know privacy challenges or security challenges posing the building of IIoT solutions. Through IIoT a sorry though IIoT provides new opportunities, but few at factors may cause the hindrance in the path to success these include the lack of vision and leadership lack of understanding of values among the management employees costly sensors and in adequate infrastructure. So, these are some of the risks that are that are faced by people who want to the management who want to deploy IIoT in the industry.

(Refer Slide Time: 18:47)

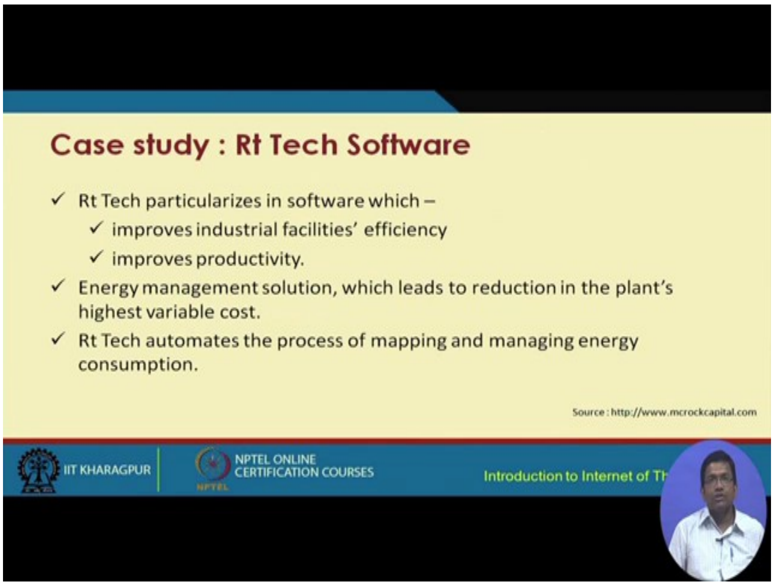
So, other challenges include improvement at the sensors miniaturization of the sensors is very crucial you know we are talking about you know day by day we are talking about very small scale small sized sensors that can perform as good as if not better than these existing big sized sensors. So, miniaturization of the sensors is very important nowadays, we are talking about name spaced sensors which make the senor the shape of the size of the sensor very small and these seniors can perform very well as well even if they are small in size. They can perform very well and the overall by through the miniaturization process the overall cost and energy consumption the overall cost can be brought down and the energy consumption can also be addressed can also be improved because small sized sensor is lightly to consume less energy compared to bigger sized sensors.

(Refer Slide Time: 19:42)



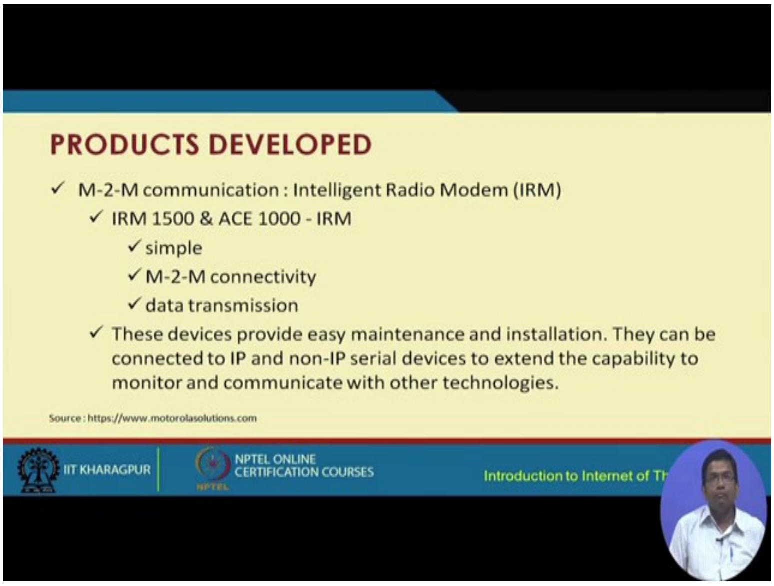
So, the others challenges with respect to manufacturing. So, you know when we are talking about manufacturing typically these are software based computer based and these are used to improve the overall operational efficiency. So, predictive maintenance savings on scheduled repairs reduced maintaenance cost maintenance costs and reduced number of break downs are important challenges and important issues that have to be taken into consideration while trying to introduce IIoT in the manufacturing industry.

(Refer Slide Time: 20:19)



So, there was an industry the Rt tech software. So, this basically particularizes in software which improves the industrial facilities efficiency and improves the overall industrial productivity. So, energy management solution which leads to reduction in the plants highest variable cost was a produced was designed and this particular company automates the processes of mapping and managing energy consumption.

(Refer Slide Time: 20:52)

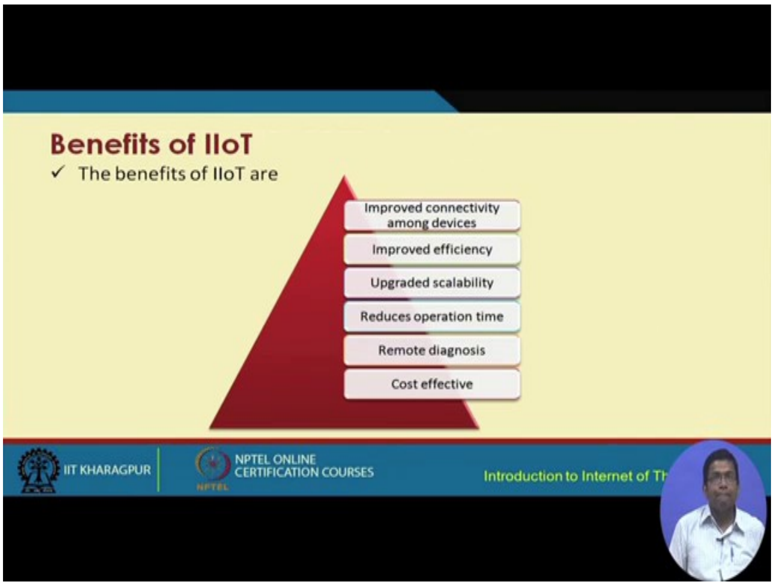


The products that they develop include M-2-M based communication based systems and intelligent radio modems and these are the some of these products and their specifications given over here these devices provide easy maintenance and installation they can be connected to IP or non IP devices to extend the capability to monitor and communicate with other technologies.

(Refer Slide Time: 21:16)

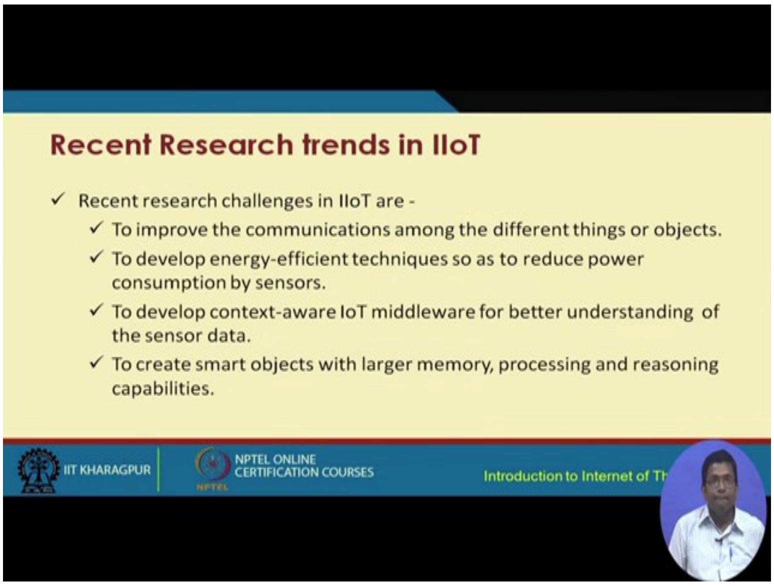
So, this is a solution that they have developed a product that they have developed it is known as control which offers IO link to the master gateway. So, it can be easily integrated into the industrial network with existing and new installations, it supports Ethernet and IP and also supports the mod bus TCP. So, there are different benefits of IIoT improving the connectivity among devices improving efficiency updating the scalability.

(Refer Slide Time: 21:42)



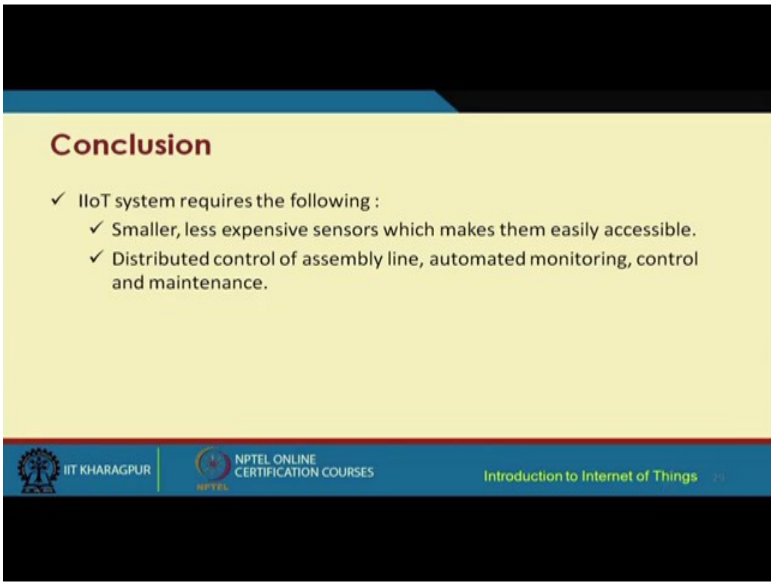
So, easily one can scale up by the use scale up in the industrial sector industrial processes can be scaled up, industrial you know overall industrial productivity can be scaled up through the use of IIoT reduction in the operation time can be achieved in the industry through the use of IIoT solutions remote diagnosis can be performed quite efficiently with the help of IIoT and IIoT solutions offer cost effective solutions.

(Refer Slide Time: 22:24)



In terms of the research recent research trends one is to improve the communication among the different things or objects to second is to develop energy efficient techniques. So, as to reduce power consumption by the sensors third is to develop context aware internet of things middleware for better understanding of the sensor data and the forth is to create smart objects with larger memory processing and reasoning capabilities.

(Refer Slide Time: 22:55)



So, these are some of the different features the different applications of IIoT and how IIoT can improve the productivity in the industry in the different plants manufacturing plants the health care sector and so on.

So, IIoT systems they have requirement for very small sized less expensive sensors which are easily accessible and so, this basically will help in the furthering the use of IIoT more in the industry then the second thing is the assembly line. So, you know controlling the assembly line automates monitoring control and maintenance of the industrial processes and the industrial product lines these can be achieved efficiently with the help of industrial IoT.

(Refer Slide Time: 23:57)

So, these are some of the references and these can be you know. So, this reference is good for understanding connected vehicles it was published in the IEEE Internet of Things and this is something that I should mention that on internet of things there is a journal which is called the IEEE Internet of Things journal which has number of papers on the different aspects of industrial internet of things.

(Refer Slide Time: 24:45)

So, this concerns basically in transportation sector like this there are different other problems and solutions mining related papers are also available, safety related papers on the use of IIoT are also available. So, these are the different references. And so, with this we come to an end of the discussions on industrial IoT.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

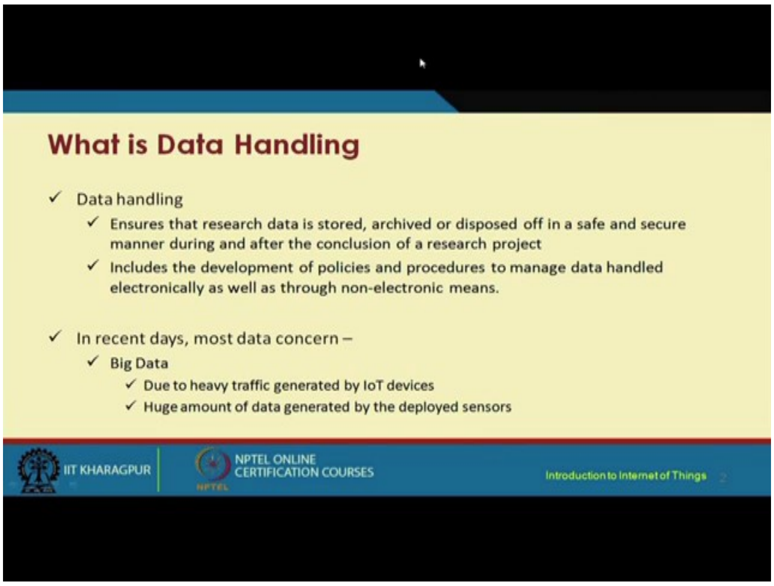
Lecture – 55
Data Handling and Analytics – Part – I

So far, we have understood the different building blocks different technologies about IoT how to build IoT using different technologies we have already gone through in the different lectures. So, we need to now understand that the IoT systems as a whole comprising of devices such as different sensors, actuators and different other communication devices like Wi-Fi 3G, 4G and so on we have mobile devices. So, you know all of these in the IoT world they are huge producers of data. So, IoT is heavily data intensive it is heavily data intensive. So, lot of data gets produced in the IoT deployments in the in the IoT implementation.

So, these data have to be number one properly handled and number 2 is they have to be analyzed to make sense out of the data. So, that things can be made much more efficient where ever the IoT solutions are deployed those problems can be solved can be addressed much more efficiently. So, this is the requirement of the data analytics. So, we have 2 things being discussed in this lecture number one how to handle the data, data handling and number 2 is the data that is generated and is received may be collected at a server either in a centralized way or may it can be distributed the data can be collected in a distributed fashion. So, that data has to be analyzed to make sense out of it to make things better.

So, this is what we are going to look at. So, what are the subtleties what are the important issues concerning this thing. So, this is what we have to understand and this is what we are focusing on in this particular lecture. So, this is divided into data handling and analytics is divided into 2 parts so; however, in both of these lectures what we are going to do is we are simply trying to motivate ourselves and try to understand because this is a this is a introductory course on internet of things here we are not going to understand about the different methodologies for data handling we can or how to how to perform the how to perform the handling of the data or how to analyze the data that we are not going to understand in detail we are simply going to understand that what are the tools the methodology that out there that can be used for handling and analysis of the data.

(Refer Slide Time: 03:27)



So, we start with data handling data handling basically ensures that the data is stored properly, archived properly and disposed off in a safe and secure manner during and after the conclusion of the project. So, I am talking about a project in general in order to understand data handling. So, here we are considered we are considering the development of the policies and the procedures about how to handle the data electronically as well as well as through non electronic means. So, in the IoTs sphere most of the data have certain features which are analogous to the features of big data in other words we are talking about IoT systems producing big data and what is big data that we will understand later, but for now we will just conceive of big data as data that is extraordinarily big in different ways and what are those different ways that we will see later on.

So, due to heavy traffic generated by these IoT devices there is huge amount of data that is created by the different sensors and the different other IoT devices huge amount of data is generated and that data it is big in size continuously big streams of data flow through the network. So, are generated in the network for example, if there is a camera if there is a camera that is fitted. So, that camera basically streams in lot of data continuously. So, in a in a particular hour when the camera stream data is collected you know that will that is a that is huge in size and we are talking about not just one or 2 hours, but we are talking about collecting lot of data over days and months and years and so on.

So, that data has to be at number one stored, number 2 analyzed and then how you are going to handle you know as long as it is not required after that it is no longer required how you are going to dispose of that particular data. So, all these things have to be taken into consideration when we are planning or we are designing an IoT system.

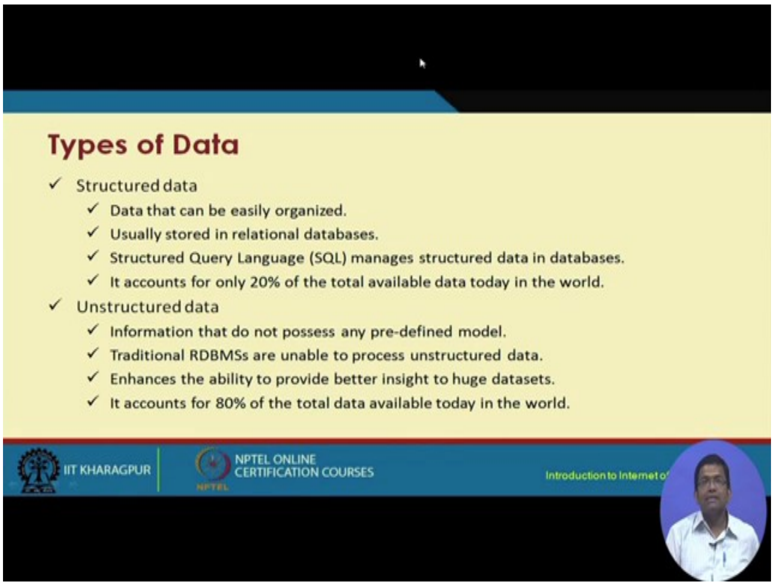
(Refer Slide Time: 06:03)

So, I was mentioning to you about big data. So, big data there are different there are different definitions of big data. So, one of these definitions talks says that big data technologies describe a new generation of technologies and architectures designed to economically extract value from very large volumes of a very wide variety of data by enabling high velocity capture discovery and or analysis. So, big data shall mean that the data of which the volume acquisition speed or data representation limits the capacity of using traditional relational methods to conduct effective analysis or the data which may be effectively processed with important horizontal zoom technologies.

So, what it means you know all these fancy words have been used in these definitions. So, what it means 2 things data that is huge in size that flows in large velocities that is generated and disseminated in large velocities have to be handled in real time this is one issue, second issue is these data are typically unstructured they are typically unstructured for example, you know text; huge text; Facebook data, Twitter data; you know all these social network data or the data that are generated from the telescopes the sky monitoring telescopes the data that are generated from you tube and so on. So, these have characteristics which are unstructured they cannot be stored using traditional relational database technologies.

So, how do you handle such data? So, this is a big concern in big data. So, that has to be taken care of. So, you know we cannot we cannot simply be concerned about simply deploying a network without being concerned about how to handle the data that this network is going to produce that is why data handling and big data handling is important.

(Refer Slide Time: 08:17)

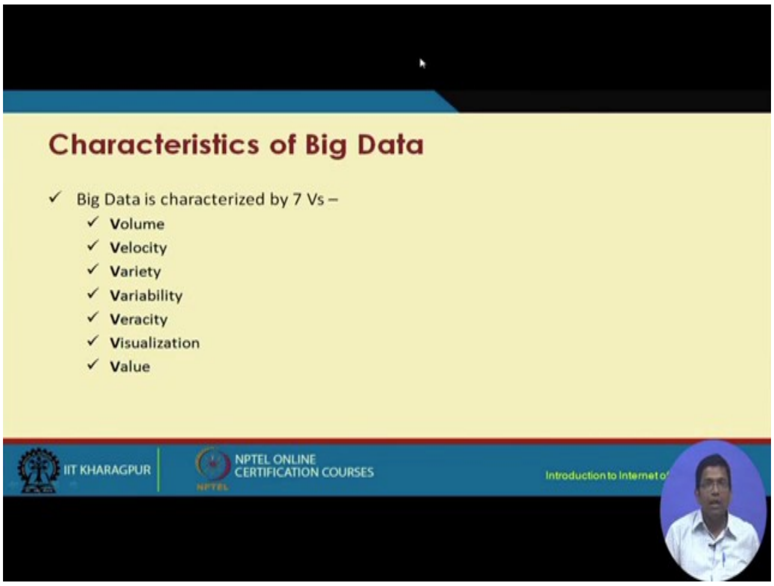


So, we have as I was telling you earlier broadly 2 categories of data structured data like what we have been using library information system student information system accounting information system these are good examples of structured data.

So, these data are easily organized they can be stored in relational databases relational tables you can perform different queries on these data that are stored in the tables and; however, these type of structured data accounts for only twenty percent of total available data in the world today and definitely it is a very small amount of data in the IoT systems. So, IoT systems produce mostly unstructured data which cannot be stored in the form of relational tables.

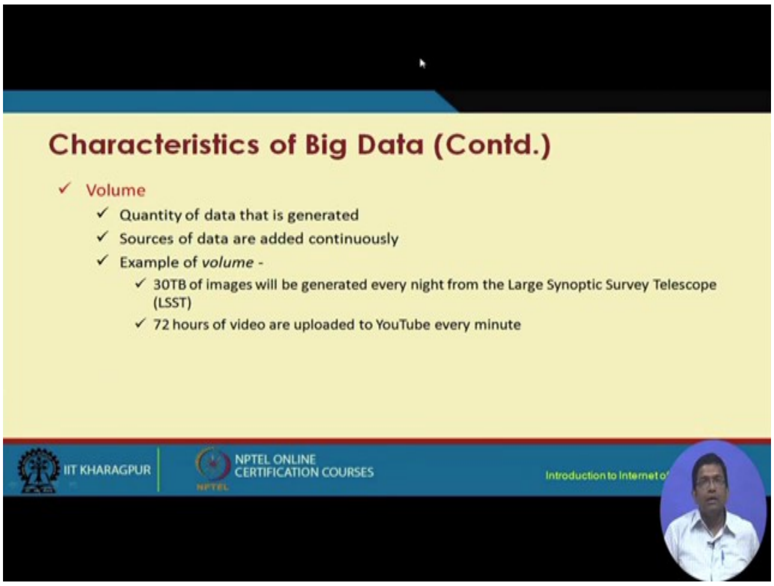
So, there is not abide by any pre defined relational model for the storing of the data traditional RDBMs techniques are unusable and these data they are very huge in size they are very huge in size and you know most of the data more than 80 percent of the total data that is available in the world today are in the unstructured form, text fields video, audio speech, you tube data you know telescope data all these are good examples of unstructured data even the data that are produced from most of the IoT devices are unstructured most of the sensor data are unstructured cameras produce unstructured data. So, how do you handle these data?

(Refer Slide Time: 10:09)



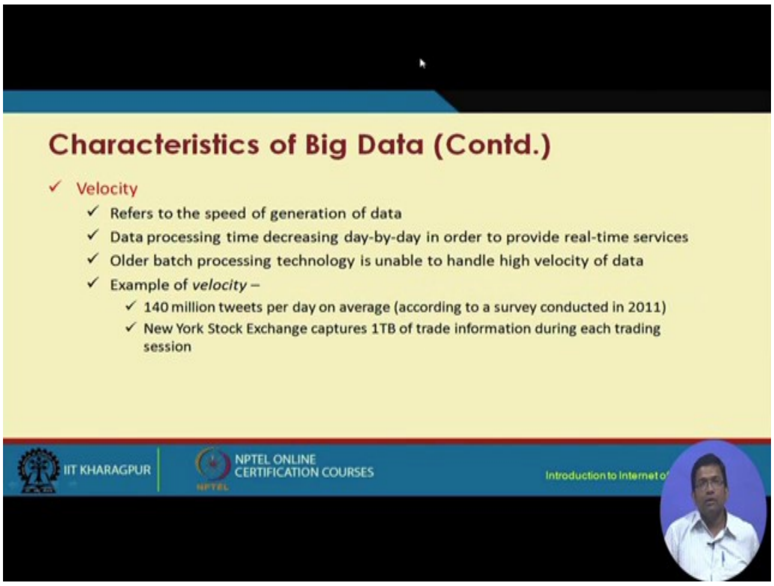
So, some of these characteristics of big data earlier it started with a 3 V then came the 5 V definition and now people are talking about 7 V's of big data. So, what are these Vs number 1, volume number 2, V is velocity number 3 is variety, number 4 variability, number 5 veracity, number 6 visualization and number 7 value.

(Refer Slide Time: 10:45)



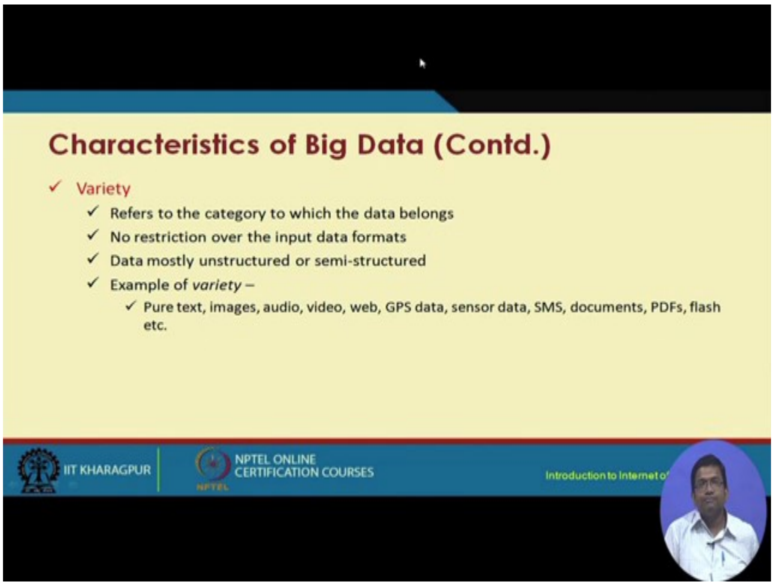
So, these are the 7 different characteristics in to the form of fees of big data. So, let us look at each of them one by one. So, volume; so, big data are characterized with large volumes of data and the quantity of the data that is generated is huge in volume we are talking about more than tera bytes of data several tera bytes of data of images video and so on and so forth you tube you know YouTube basically in every minute you tube in the YouTube 72 hours of video are uploaded. So, it is a huge amount of data huge in terms of volume. So, this has to be in every minute if it is so much. Then just imagine that how much it is going to be every day and in a year how much it is going to be.

(Refer Slide Time: 11:40)



Velocity as the name suggests; it concerns the speed of generation of the data. So, data processing time is decreasing day by day in order to produce real time services older batch processing technology is unable to handle high velocity of data. So, we need new technologies to handle this high velocity of data. So, these IoT devices mobile phone sensors and so on in huge speeds you know high rate the data is being generated for example, with respect to velocity hundred forty million tweets are generated per day on average the New York stock exchange captures 1 tera byte of trade information during each trading session.

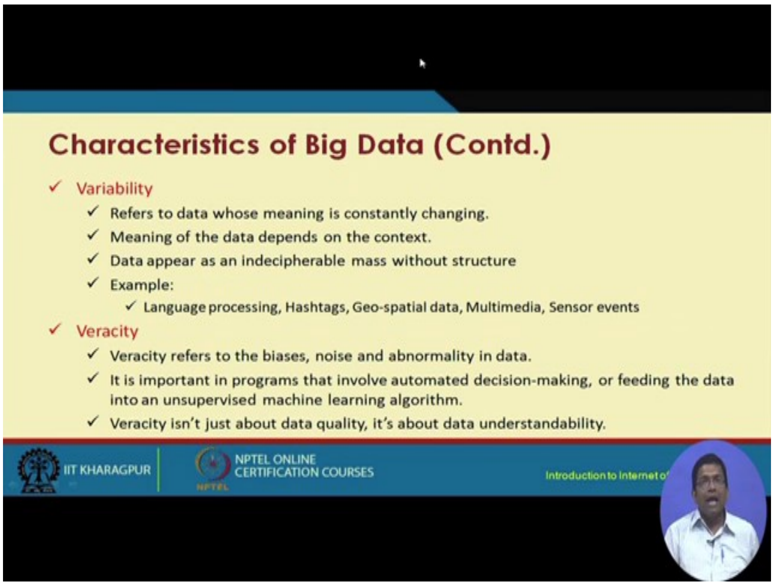
(Refer Slide Time: 12:41)



So, just imagine that how much data at what speed is generated in the IoT world.

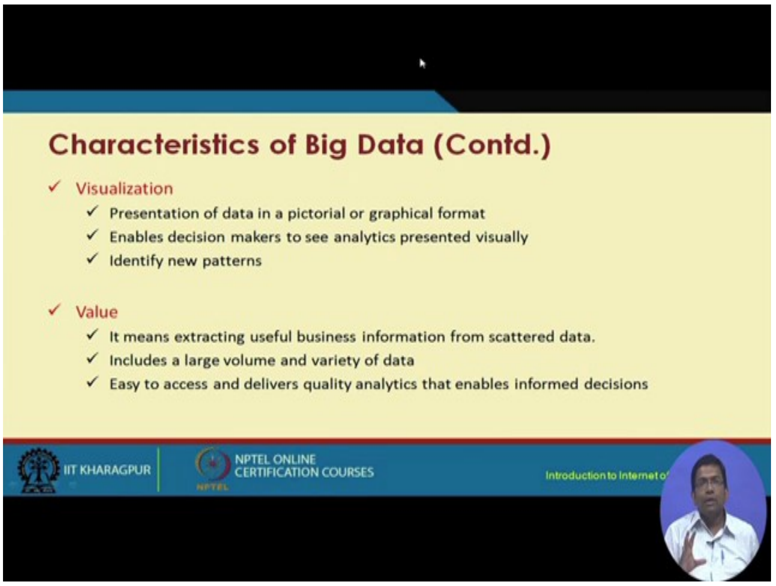
Variety refers to the category to which the data belongs and most of the data are either unstructured or they are semi structured and examples could be variety could be that pure text data, images, audio, video, web, GPS, then sensor data, SMS, documents, PDFs, flash, etcetera, etcetera. So, all these different varieties of data flowing through a single pipe in the IoT world single pipe huge amounts of data huge volumes of data at high velocities data which is highly varied not only consisting of text, but text audio video images web sensor and so on. So, everything flowing together.

(Refer Slide Time: 13:43)



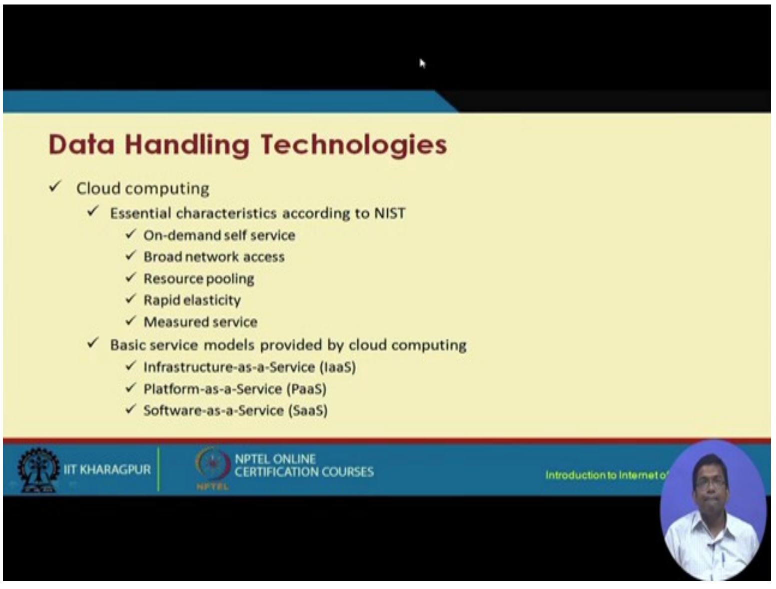
Then we have variability which refers to the data whose meaning is constantly changing the meaning of the data constantly changes depending on the context. So, examples could be language processing. So, language you know it is context dependent. So, you know sometimes language processing it is context driven. So, the meaning basically varies with context hashtags, geo-spatial data, multimedia, sensor events and so on veracity refers to the biases, noise abnormality that exists in the data. So, the IoT data that is typically generated is highly veracious. So, it is important in programs that involve automated decision making or feeding the data into an unsupervised machine learning algorithm. Veracity is not just about data quality it is also about understanding the data.

(Refer Slide Time: 14:44)



Visualization concerns how to present the data pictorially or in a particular easily understandable format it enables the decision makers to see the analytics that are presented visually and identify new patterns value basically means that extracting useful business information from the scattered info. So, how much value the data has from the variety you know. So, from the data; from that how much value it has it includes a large volume and variety of data it is easy to access and deliver quality analytics that enables informed decisions.

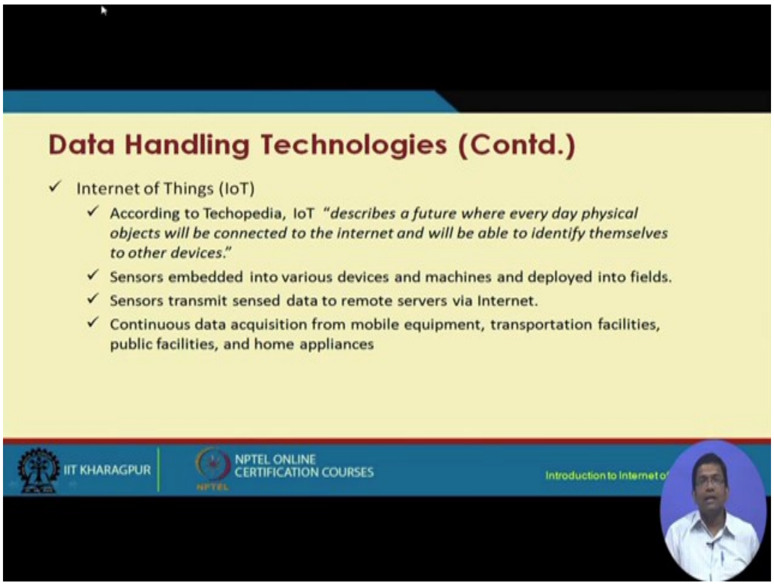
(Refer Slide Time: 15:21)



There are different data handling technologies that are available for use cloud is one such popular technology. So, here in cloud, cloud basically has some of the essential characteristics as per the definition of NIST on demand self service broad network access resource pooling rapid elasticity measured service measured service means what depending on the amounts of computational resources that are used; it will be built accordingly rapid elasticity means if I need more resources the resources are going to be made available through a pooling based mechanisms. So, resources are going to be pooled from different physical devices and I do not have to own these resources this infrastructure I do not have to own, but I can still get access to these on an on demand manner depending on my requirement and I will build accordingly.

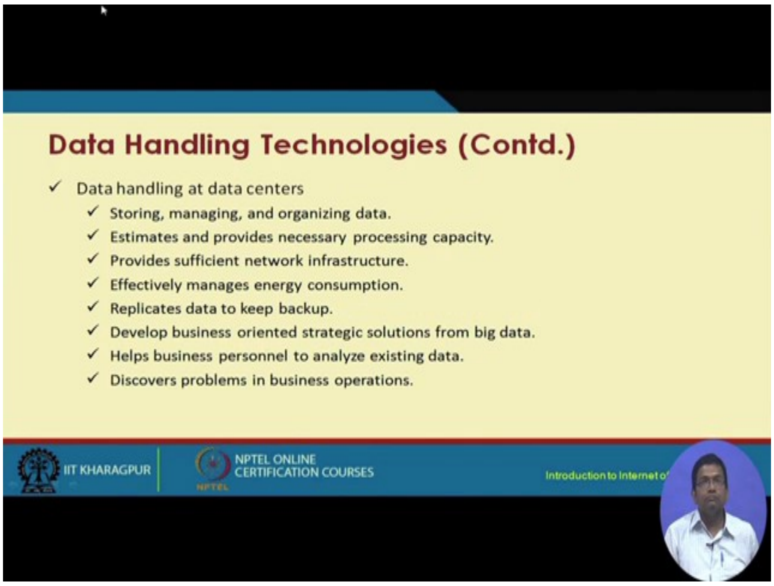
So, some of these basic service models that are there and some of which we have already covered include infrastructure as a service, platform as a service and software as a service.

(Refer Slide Time: 16:51)



So, cloud is cloud with this 3 basic service models IaaS, PaaS and SaaS is a very important data handling technology that is available to us second is internet of things. So, in the IoT world the sensors that are embedded to the different devices and machines they generate lot of data the sensors transmit this sense data to remote servers via the internet and these data they can be either handled at the back end or these data can also be processed locally at the age or in the interim somewhere in the intermediate layer. So, continuous data acquisition from mobile equipment transportation facilities public facilities and home appliances are an important characteristic of IoT and the data that is handled data that is generated in the IoT have to be handled accordingly.

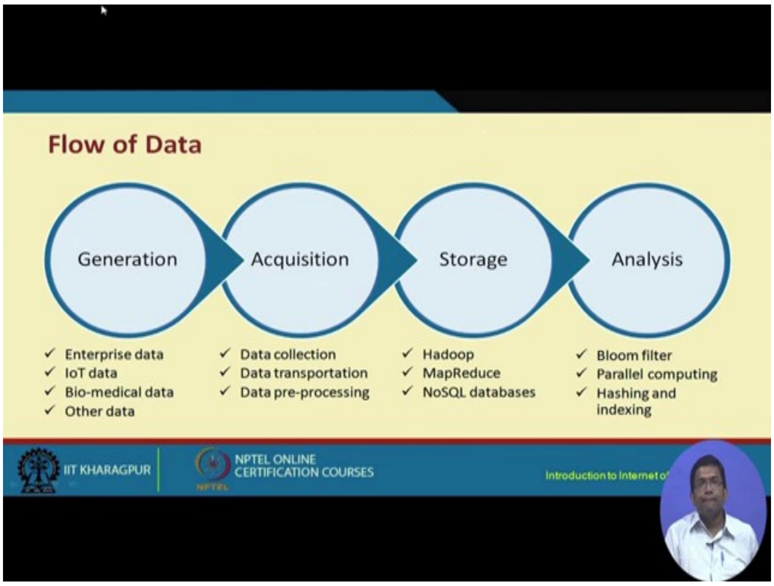
(Refer Slide Time: 17:43)



Datacenters basically concern you know storing lot of data managing the data organizing the data these data that are generated in the data centers that are that are that exist in the data centers.

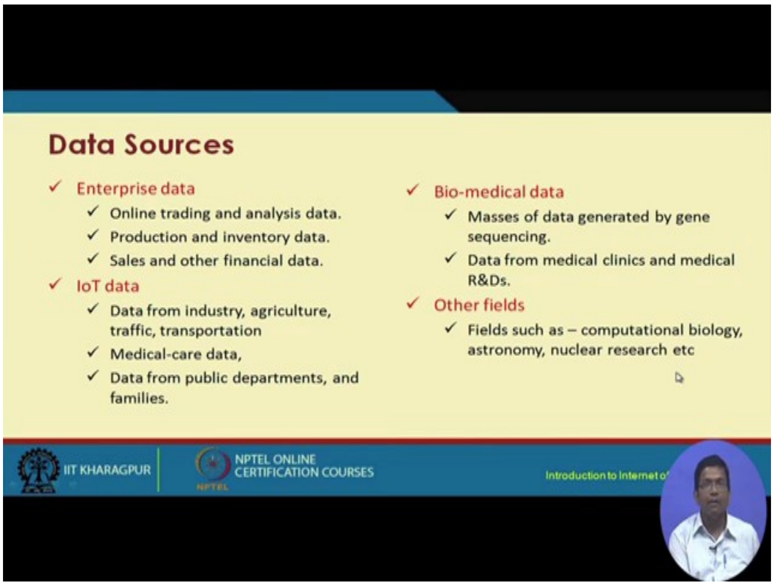
They are they have to be replicated, they have to be backed up they provide sufficient network you know sufficient network infrastructure has to be provided in order to handle this data and this data they can be analyzed in order to discover problems in the business operations.

(Refer Slide Time: 18:25)



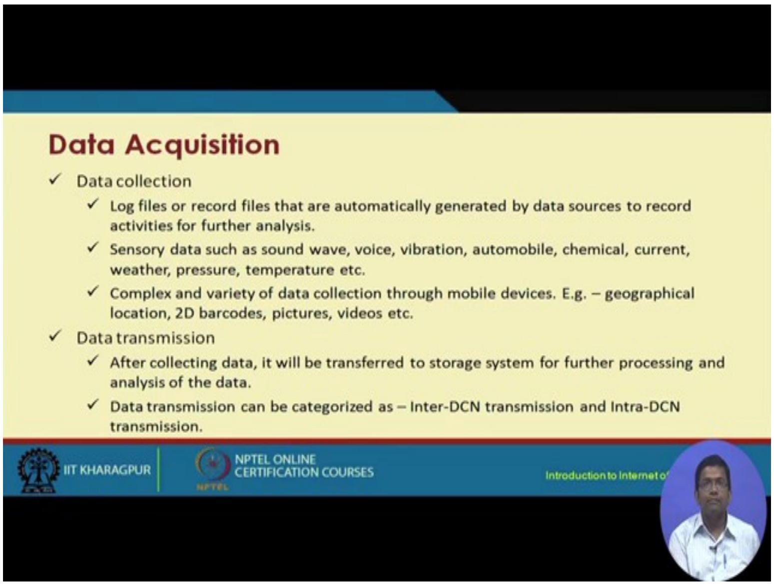
So, this is how the data flows from generation to analysis. So, first the data is generated then comes acquisition of the data storage of the data and finally, analysis of the data. So, in terms of generation of the data from enterprise systems data can be generated from IoT systems from biomedical devices and different other devices all of which are good sources or generators of data in terms of acquisition after the data generation acquisition of the data; data are collected data can be transported data are preprocessed and then data have to be stored we have different technologies for doing it we have Hadoop technology for storage of data MapReduce, NoSQL databases and finally, they have to be analyzed.

(Refer Slide Time: 19:35)



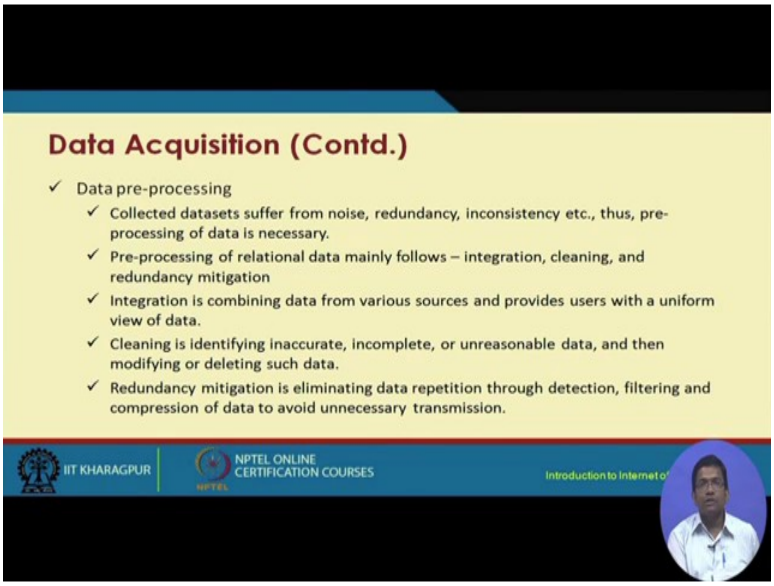
So, for this we have the bloom filter, parallel computing technologies, hashing mechanisms, indexing mechanisms and so on. The different sources of data include enterprise data, IoT data, biomedical data, and other field data from computational biology from nuclear research from astronomy and so on.

(Refer Slide Time: 19:52)



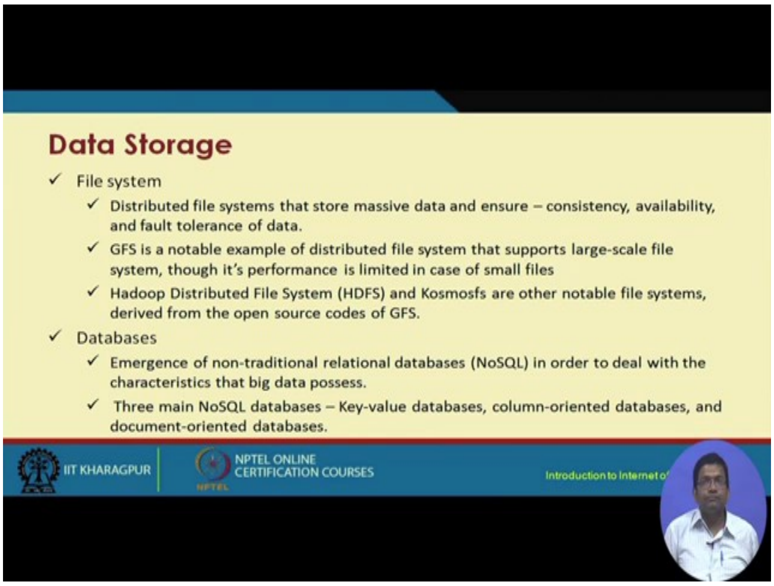
Now, comes the data acquisition which concerns data collection from log files from different other records activities interviewing if required collecting data from the sensors from the sound sensors voice vibration automobile chemical current weather pressure temperature etcetera and so on. So, after the data are collected they have to be transmitted. So, after the after collecting the data the data have to be transferred to a storage system for further processing and analysis.

(Refer Slide Time: 20:39)



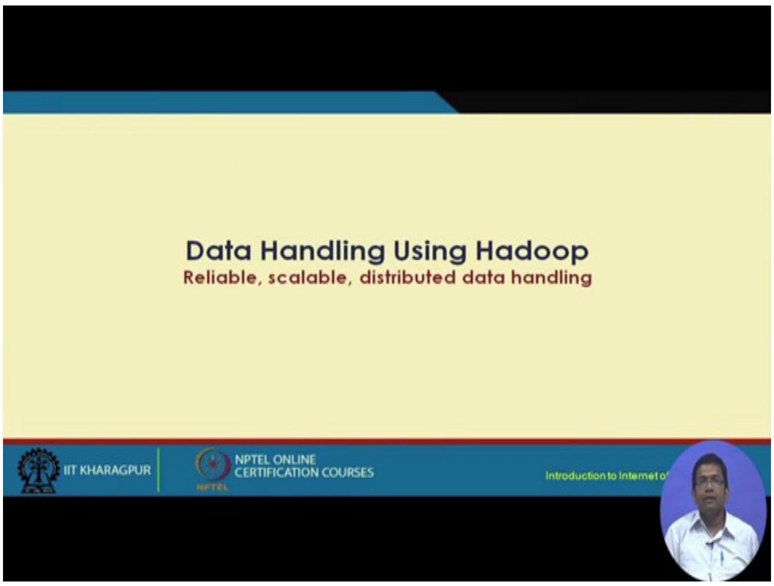
So, data transmission can be categorized as in term data center network transmission and intra data center network transmission then the data have to be preprocessed this collected data suffer from noise redundancy inconsistency etcetera. So, these have to be removed they have to be preprocessed the data have to be preprocessed the preprocessing of the relational data mainly follows integration cleaning and redundancy mitigation integration is combining the data from various sources and providing users with a information with uniform view of the data cleaning of the data is required in order to remove inaccuracies, incompleteness and unreasonable behavior of the data unreasonable characteristics of the data and then either modifying the data or to remove these problems or deleting these data all together.

(Refer Slide Time: 21:31)



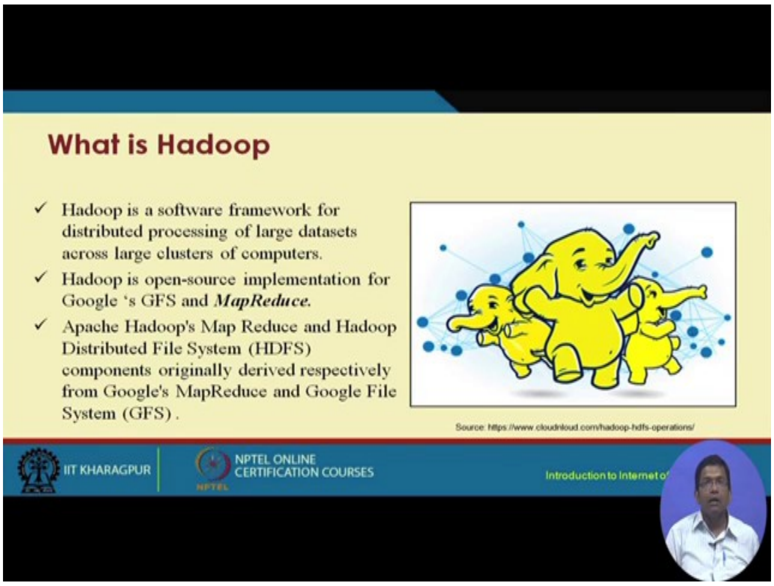
Now, the data after acquisition the data has to be stored the data can be stored in the file systems or in data bases. So, if we are talking about relational databases SQL is good enough; however, with the kind of data that is exhibited then unstructured data that is exhibited these NoSQL is very useful. NoSQL basically uses 3 different types of databases one is the key value database the second is the column oriented database and the third is the document oriented data base.

(Refer Slide Time: 22:18)



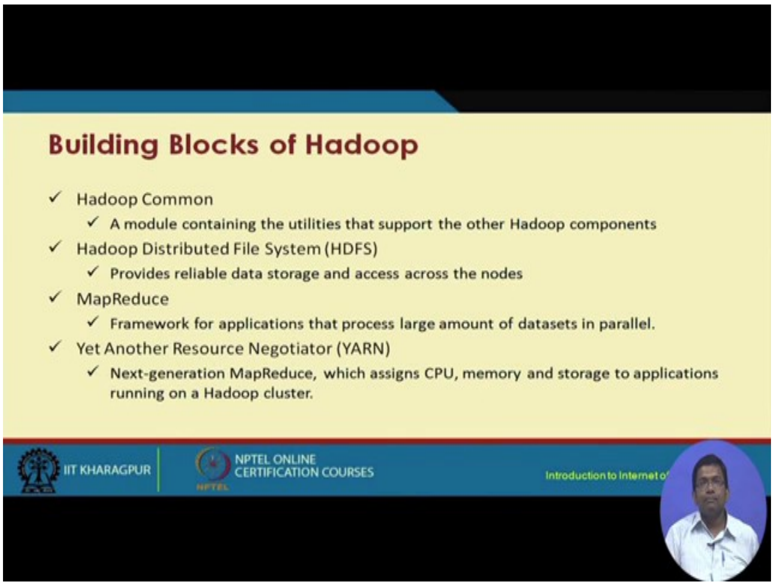
So, this is about the data handling the different aspects of data handling for this what technology do we have for handling this kind of data what technology do we have we have the Hadoop technology.

(Refer Slide Time: 22:36)



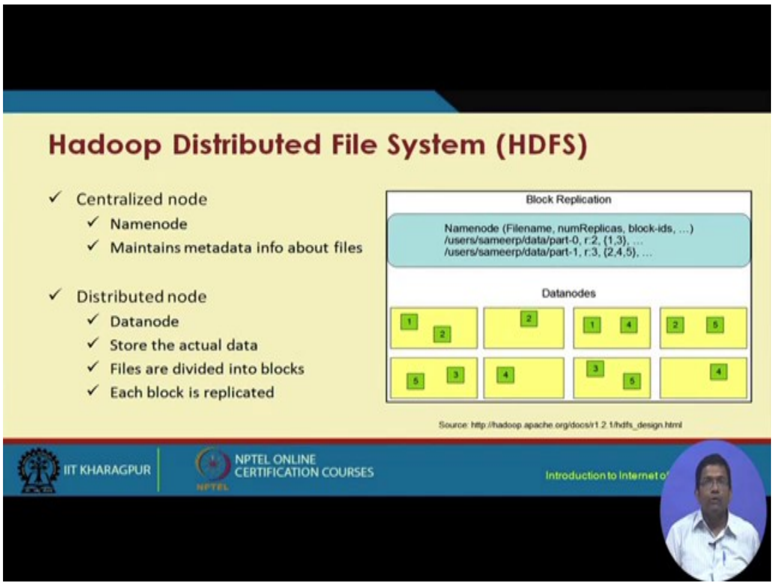
So, what is Hadoop this is basically a software framework for distributed processing of large datasets across large clusters of computers it is a open source implementation for Google's GFS and MapReduce. GFS is basically the Google file system and MapReduce apaches apache Hadoops MapReduce and Hadoop distributed file system which in short is called is well known as HDFs has different components which are originally derived respectively from GFS, Google's, MapReduce and GFS full file system.

(Refer Slide Time: 23:20)



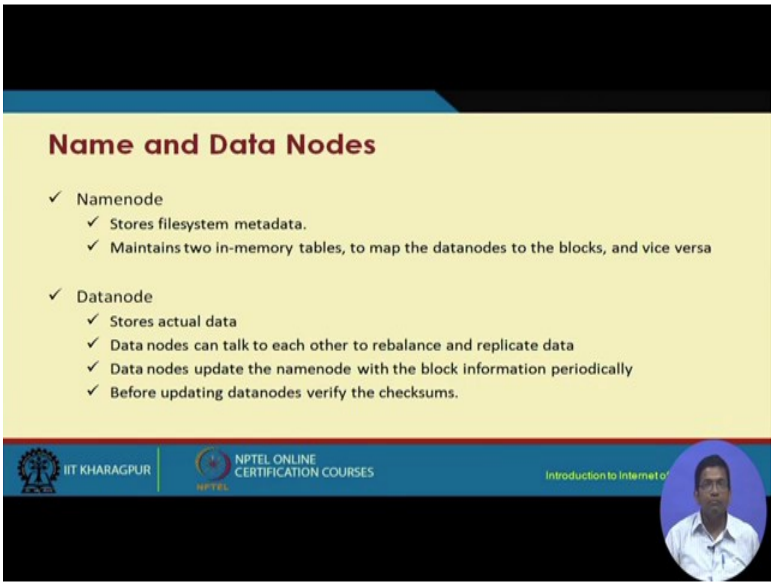
So, these are building blocks of Hadoop; Hadoop common HDFs is Hadoop distributed file system MapReduce and YARN which stands for yet another resource negotiator so, without going through each of these in further detail.

(Refer Slide Time: 23:41)



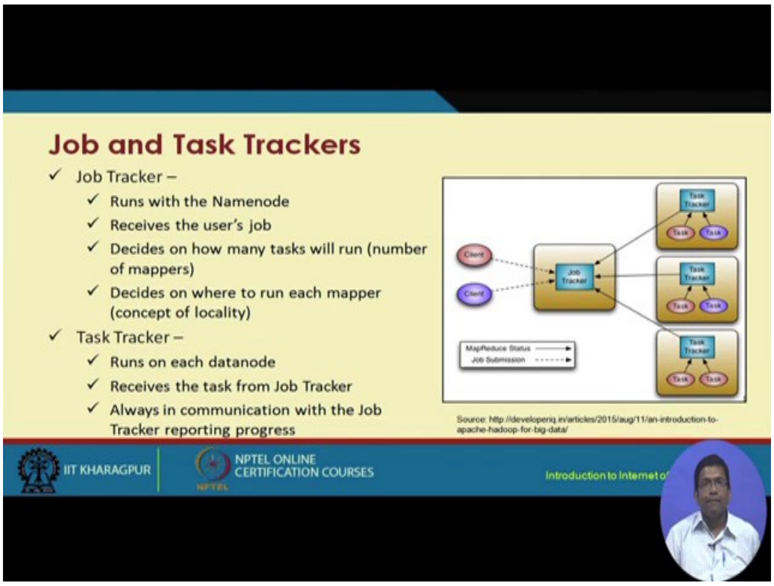
We will just look at only HDFs the Hadoop distributed file system. So, in HDFs which is which is basically the important thing in Hadoop. So, in HDFs there are 2 different types of nodes we have the name node and we have the data node. So, the name node is a centralized node which maintains the metadata information about the different files storing the data and data node is a distributed node that stores the actual data in the form of files which are again divided into blocks and each of these blocks is replicated and this is what is shown over here in this particular figure. So, what you see over here are these data nodes with replication of the blocks and this is the name node. So, name node has the metadata and the data nodes have the actual data and these data nodes are fragmented into blocks and these blocks are replicated and consequently we have more reliability in the storage of the data in Hadoop HDFs.

(Refer Slide Time: 24:57)



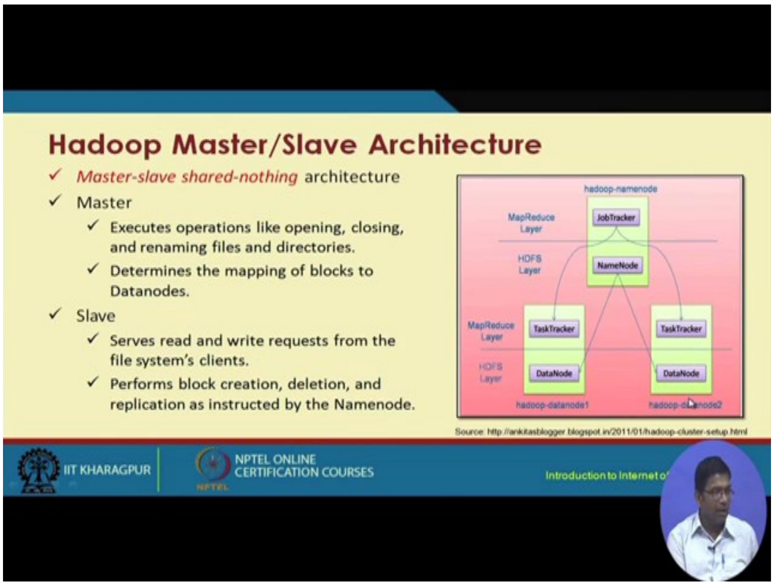
So, we have the name node which stores the file system meta data and the data node which stores the actual data.

(Refer Slide Time: 25:06)



Now, we also have these job and job trackers. The job tracker basically runs with the name node it receives the users job and decides on how how many tasks will run and the job tracker basically runs on each data node receives the task from the job tracker and it is always in communication with the job tracker reporting it the progress that is made. So, as we can see over here we have the job tracker and these different tasks which are monitored through the task tracker. So, we have the job tracker running on the name node and the task tracker which is running on the data nodes.

(Refer Slide Time: 25:57)



So, here what we see is the master slave architecture in Hadoop. So, we have this kind of thing we have the name node like this which contacts the metadata, the name node and then we have these different data nodes. This name node has the job tracker and the name node information and this name node basically points to the data node of the data node in the in the data node that is installed right and then we have the MapReduce.

So, the map; so, what we have the task the task tracker is basically linked with the job tracker job tracker and the task tracker. So, job tracker in the name node is related to the; is linked with the task tracker in the data node. So, the job tracker decides in the MapReduce layer the name node in the HDFs layer task tracker in the MapReduce layer data node in the HDFs layer and so on. So, this is the architecture the master slave architecture in Hadoop.

(Refer Slide Time: 27:17)

So, with this we come to an end of the discussions on the file handling and particularly focusing on file handling of this lecture on file handling and data analysis and here some of these references are there and with this we come to an end. And so, what we have discussed is how data handling is important what are the different sources of data how data have to be handled and how Hadoop and its different components can come as an aid for handling data which is which has the features of big data data that is generated from the IoT systems how it can be how Hadoop can be used in order to handle this kind of data.

Thank you.

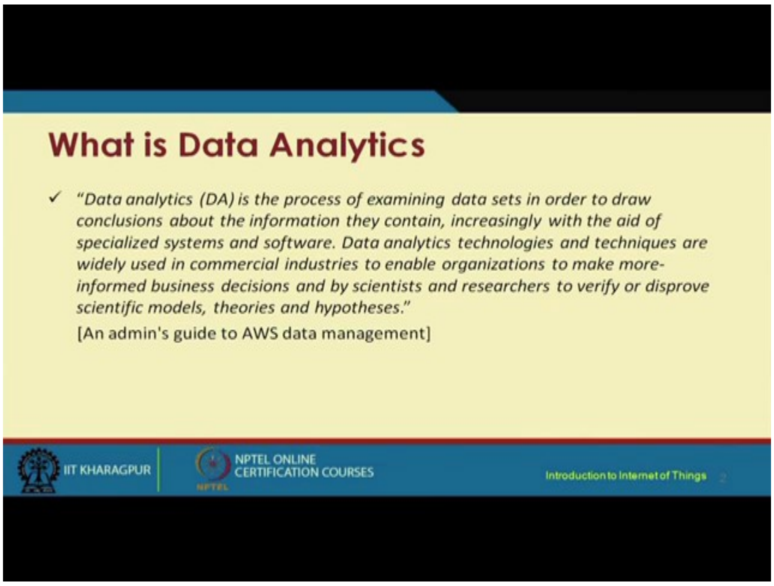
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 56
Data Handling and Analytics- Part- II

In this lecture on data analysis and sorry Data Handling and Analytics. In the first part we will focused mostly on data handling, and in the second part we are going to focus mostly on the analytics.

So, having captured the data and storing it in the cloud or in the server or whatever storage mechanisms we have. We now have to use the data, for using it we have to analyze it, we have to analyze the data. So, for this there are different tools, different methodologies that they are; the most common the most primitive once are based on statistical methods; so basic statistical methods can be applied applied on the store data in what order to make more sense out of that data in order to get more insight into that data it is stored.

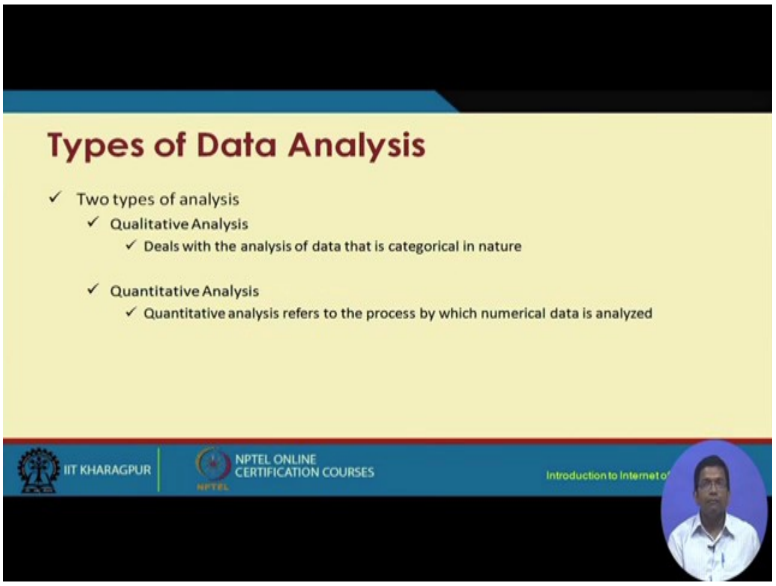
(Refer Slide Time: 01:20)



So, we have data analytics. Basically, the data have to be analyzed. So, in the context of IoT people talk a lot about data analytics. So, what is the state analytics? I am going to read one of these definitions. So, data analytics is the process of examining the data sets in order to draw conclusions about the information they contain. That means, what information is contained in this data sets. Increasingly with the aid of specialized systems and software; so with different specialized software, systems, etcetera to get insight into the data that is existing.

Data analytics technologies and techniques are widely used in commercial industries to enable organizations to make more informed business decisions and by scientist and researchers to verify or disprove the scientific models theories and hypothesis. So, this is basically the premise in which data analytics basically work and the different concerns of data analytics are basically: I mentioned in this particular definition.

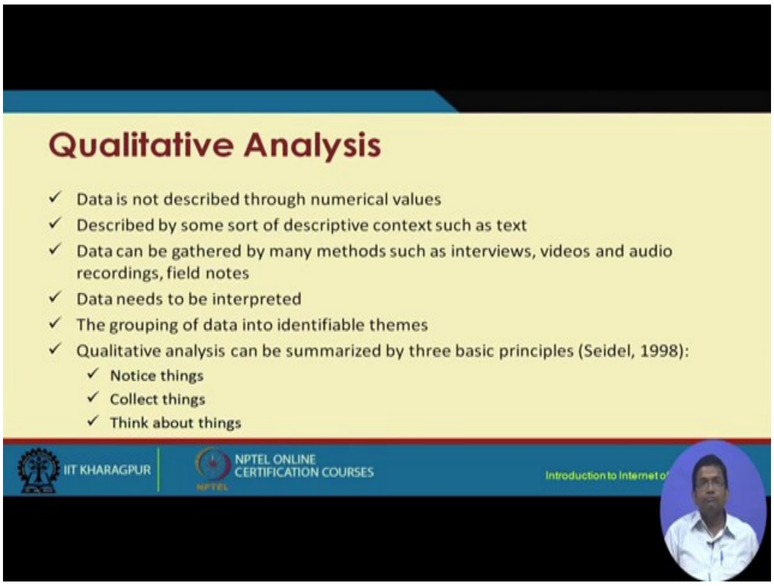
(Refer Slide Time: 02:39)



So, when we talk about analysis in general broadly analysis comes in two forms. So, we can either perform qualitative analysis on the data that has been obtained or we can perform quantitative analysis. So, qualitative analysis basically deals with the analysis of data that are categorical in nature- so qualitative analysis. Whereas, quantitative analysis refers to the process by which numerical methods can be used; numerical data can be analyzed through quantitative analysis.

So, categorical data: qualitative analysis is good enough, for numerical data quantitative analysis quantitative methods are useful.

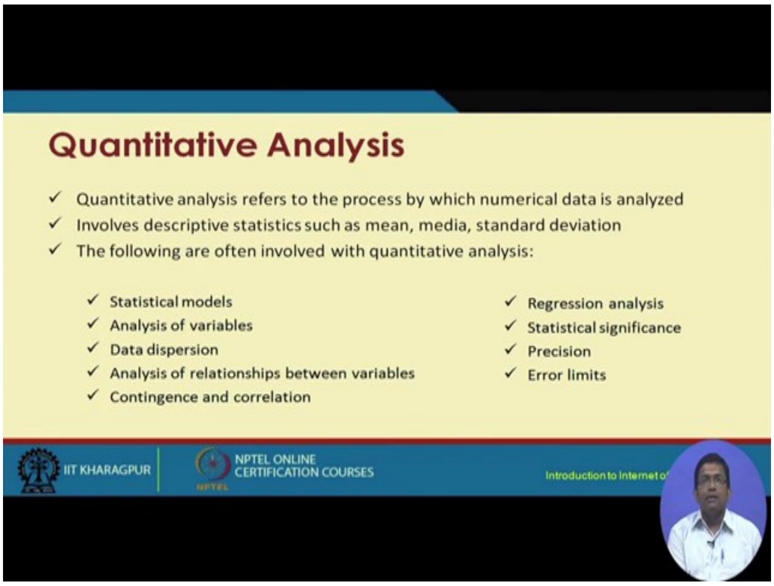
(Refer Slide Time: 03:31)



So, qualitative analysis data is not described through numerical values, but are described by some sort of descriptive contexts such as text. This qualitative data can be gathered by many methods such as from interviews, interviewing different people, from videos, from audio recordings, field notes you know industry manuals and so on.

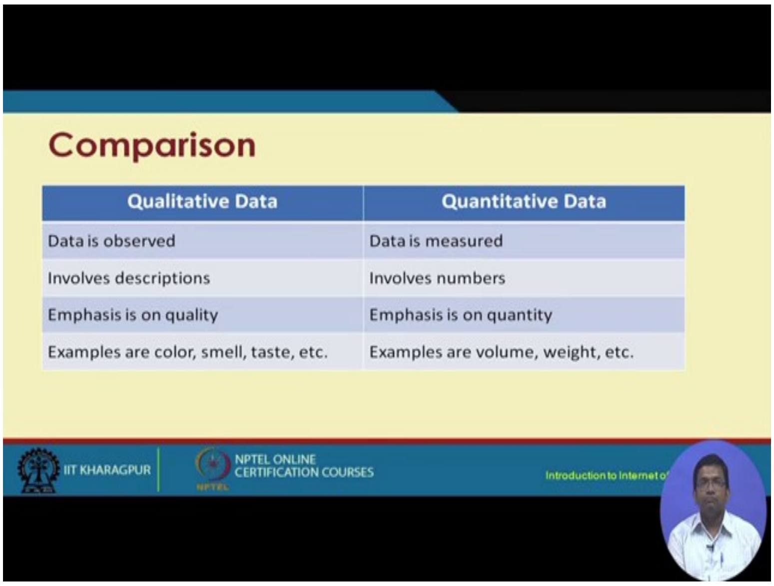
This data needs to be interpreted; the grouping of the data can be where should be performed into identifiable themes in quantitative qualitative analysis. And the qualitative analysis can be summarized by three basic principles. Notice the things collect the things and think about it. We do not need to get into details of each of these.

(Refer Slide Time: 04:27)



Next one is the quantitative analysis. So, quantitative analysis is on the numeric data using different statistical methods such as descriptive statistics, more specifically finding out the mean of the dataset median standard deviation and so on. The following are often involved with the quantitative analysis, statistical models and analysis of variance, then data dispersion analysis of relationship between variables, contingency and correlation, then regression analysis, statistical significance, precision, error limits and so on.

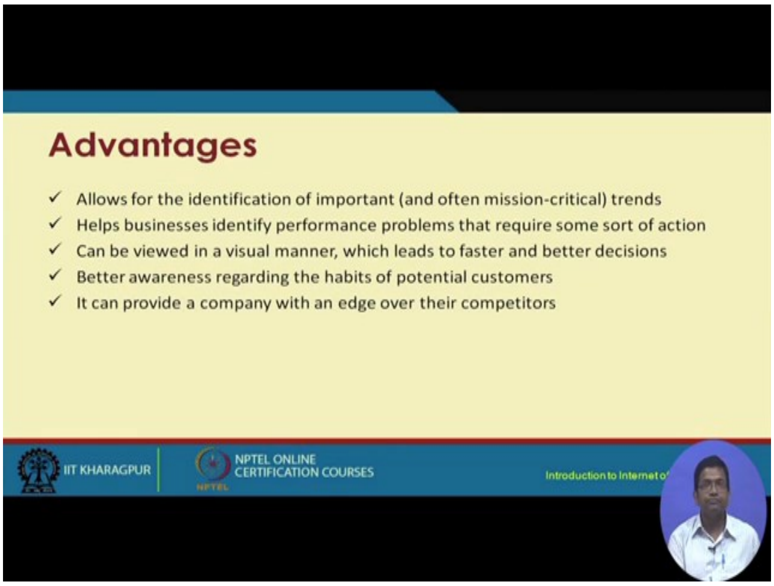
(Refer Slide Time: 05:18)



So, these are the different quantitative methods that are used for quantitative analysis of data.

Now comes the comparison between qualitative data and quantitative data. So, qualitative data can be mostly observed, whereas quantitative data can be measured. Qualitative data involves descriptions its more qualitative it involves descriptions, on the other hand quantitative data involves numbers, numeric's and so on. Whereas, in qualitative data the emphasis is on quality, in the quantitative data the emphasis is on quantity. Examples of qualitative data include colour, smell, taste, etcetera which cannot be quantified so easily. On the other hand quantifiable data include volume, weight, etcetera; these are numbers these are figures which can be used to perform different numerics.

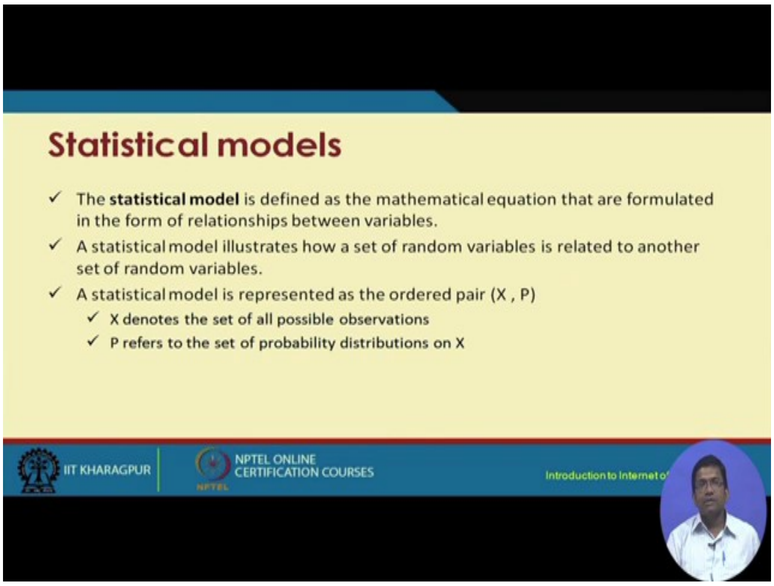
(Refer Slide Time: 06:14)



The advantages of data analytics is that: it allows for the identification of important trends, it helps the businesses identify performance problems that we require some sort of action- some prediction can be performed. By analysis of the data fast data something you know, so the businesses they can understand that what has gone wrong quantitatively we can be done or even qualitatively. So, data analytics are useful for that.

So, the analytics can also be performed in a visual manner and that can help in faster and better decision making. Analytics can provide a company with an edge over their competitors.

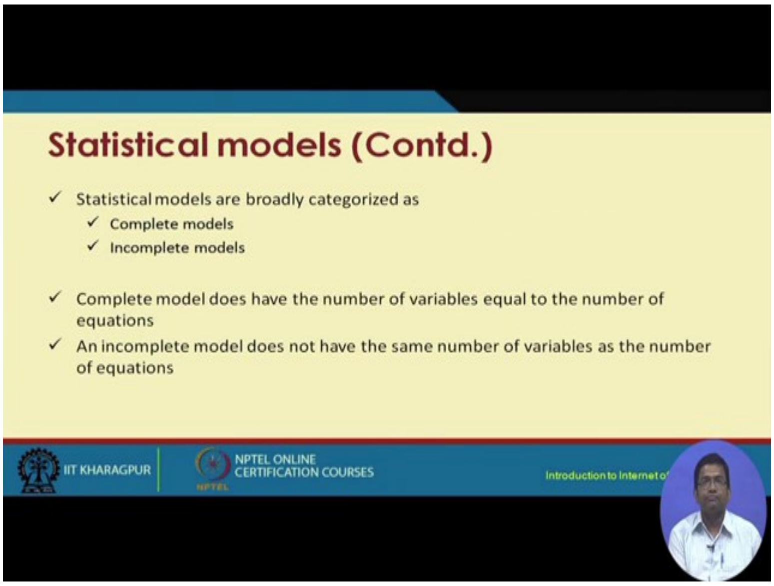
(Refer Slide Time: 07:00)



So, that is the reason actually data analytics has become very popular in the industry, not only in the industrial almost in all spheres of life data analytics has become very popular. And because you can get more insight into what is going on in the processes that are occurring around you.

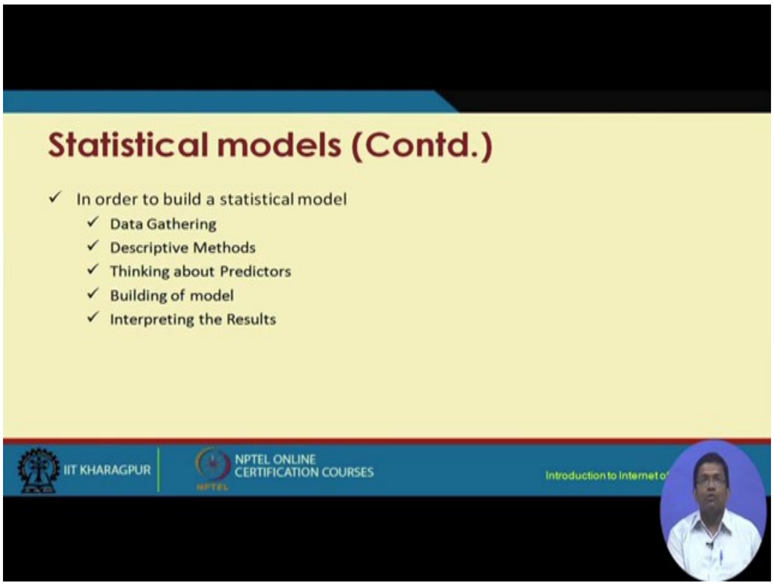
Statistical different models of statistical; statistical models can be adopted in order to perform quantitative analysis. And a statistical model can is defined as the mathematical equation that is formulated to form the relationship between variables. A statistical model illustrates how a set of random variables is related to another set of random variables. And it is a statistical model is represented as an ordered pair X P; where X denotes the set of all possible observations and P refers to the set of probability of distributions on X.

(Refer Slide Time: 08:05)



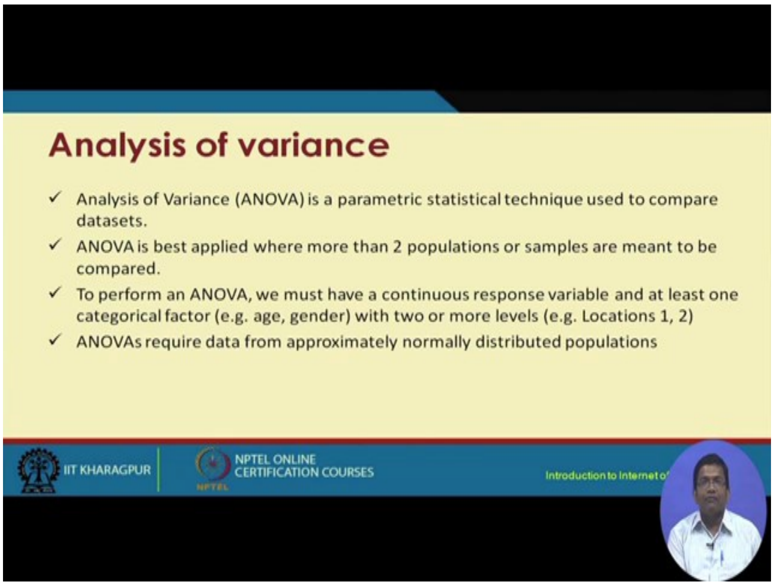
Statistical models are broadly categorized as complete models and incomplete models. Complete models have the same number of variables as the number of equations. So, the number of equations and the number of variables in the complete models are the same. So, if we have the number of variables equating equating with the number of equations what we have is a complete model. And in an incomplete model the number of variables and the number of equations are not the same- they do not match.

(Refer Slide Time: 08:39)



So, in order to build a statistical model it is required to gather the data, perform descriptive methods, think about what are the predictors, then build the model and then interpret the results.

(Refer Slide Time: 08:55)

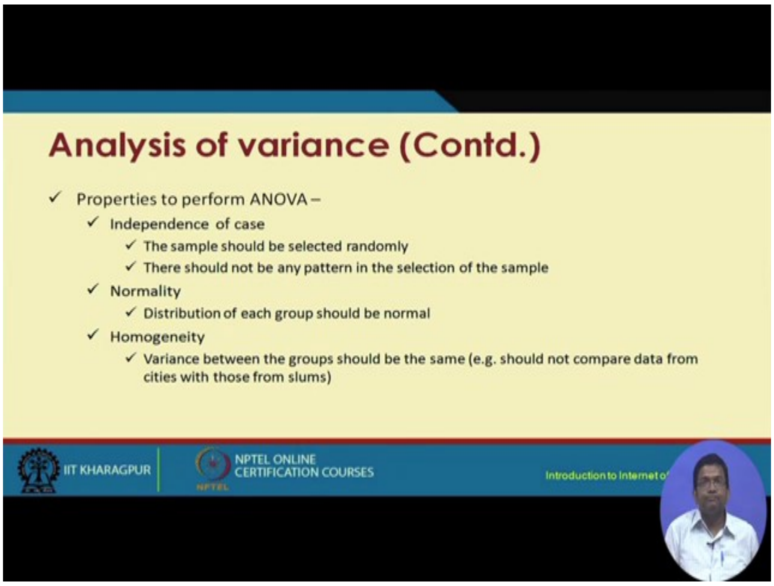


Analysis of variance in short known as ANOVA analysis: is a parametric statistical technique that can be used to compare two data sets- two or more data sets they can be compared. So, ANOVA is best applied when more than two populations of samples are meant to be compared. So, we have one dataset, we have another dataset, we want to compare these two populations to see that what is the you know how much is the correlation between these two datasets, what sort of similarity exits between these two database sets.

So, to perform ANOVA one has to have a continuous response variable and at least one categorical factor. For example, age gender, etcetera, with at least two or more levels example location 1, location 2, etcetera. So, what it means is basically levels mean that one location: one location Kharagpur another location Kolkata. So, these are two different locations corresponding to two different levels. And categories mean the age is one category. So, with respect to a particular category like age you know. So, at two different locations what is the similarity or what is the dissimilarity; similarly with respect to gender or any other category.

ANOVA requires data from approximately normally distributed population. So, this is a very important assumption or a very important requirement that you know. So, normal distribution is required for performing; normal distribution of the data set has to be there in order to perform ANOVA analysis.

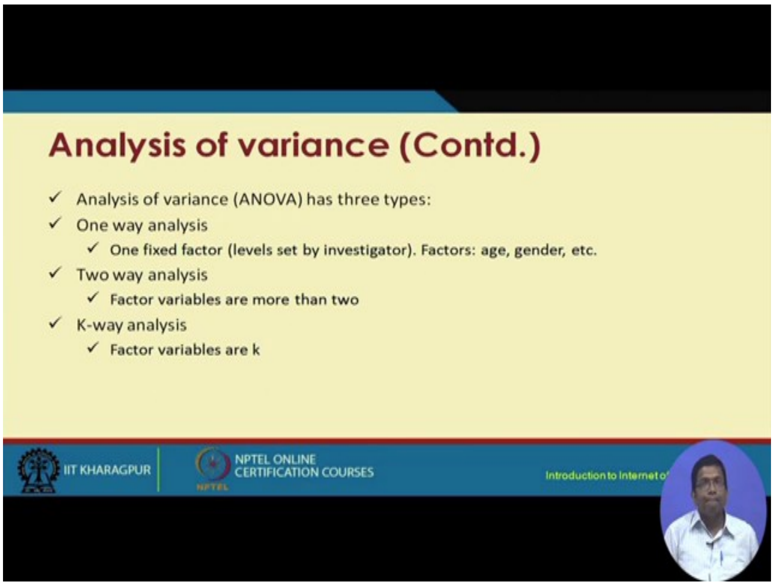
(Refer Slide Time: 10:42)



The properties to perform ANOVA: one is the independence of case, the sample that is selected should be random; random is selected there should not be any bias, there should not be any pattern, in the selected sample. Normality is the second property which constant the distribution of each group should be normal, so normal distribution of the data within the group; and homogeneity which constants variance between the groups and this should be the variance should be the same. So, we should not have a scenario to compare the data from cities with the data from maybe slums areas or maybe the data of Kharagpur compared with the data of Kolkata.

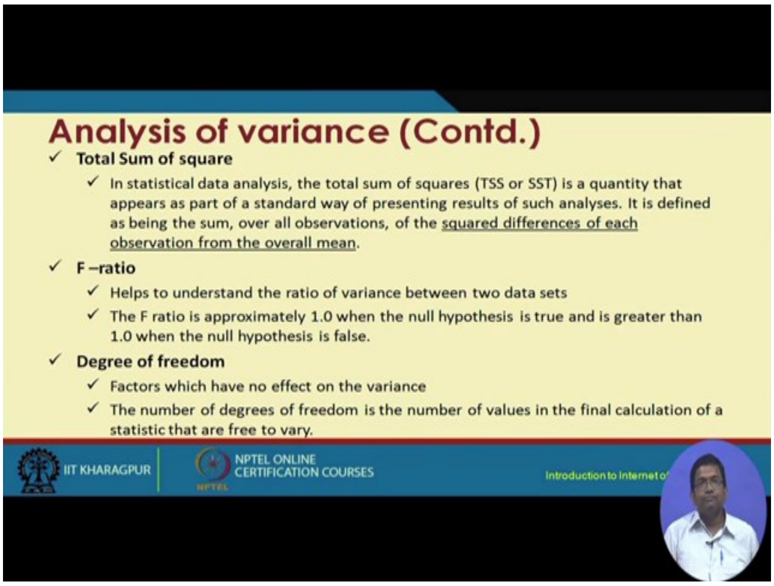
So, because we have a town we have a city so two different datasets you know compare of comparing with each other. So, they have huge variance. And the variance should be as much minimal as possible.

(Refer Slide Time: 11:50)



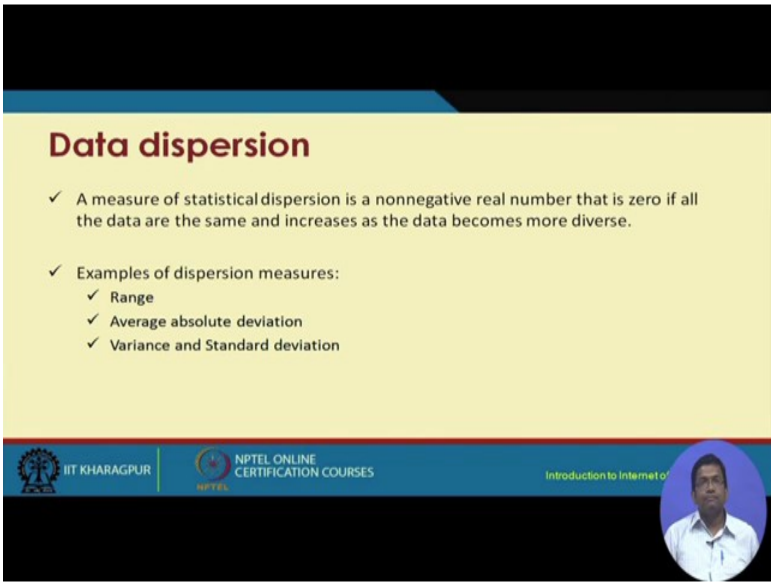
Analysis of variance has three different types: one way analysis which constant one fixed factor. For example, the factors could be age, gender, etcetera. Could be two way analysis where two or more or two factors are going to be involved. So, both maybe both age and gender will be considered in a two way factor two way ANOVA analysis. And it can be k way analysis where k factor variables are involved.

(Refer Slide Time: 12:21)



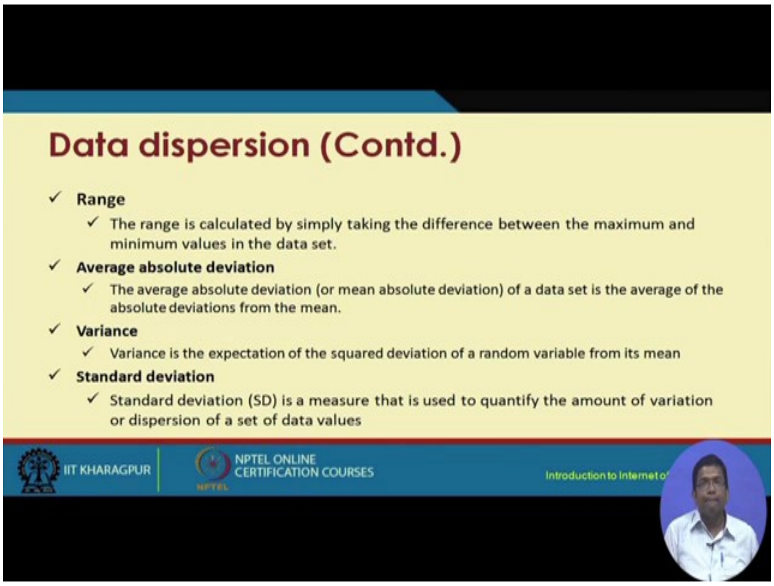
Then there are different ways, different features that are there for performing analysis of variance- total sum of square is 1, f ratio is another and the degree of freedom. So, all of these things have to be taken into consideration in order to perform and its variance. I am not going to put through these, because this is not essentially a course in statistical methods. And these are all available, but what is important is that ANOVA analysis can be used in order to perform analytics on the data that is obtained from IoT systems.

(Refer Slide Time: 13:01)



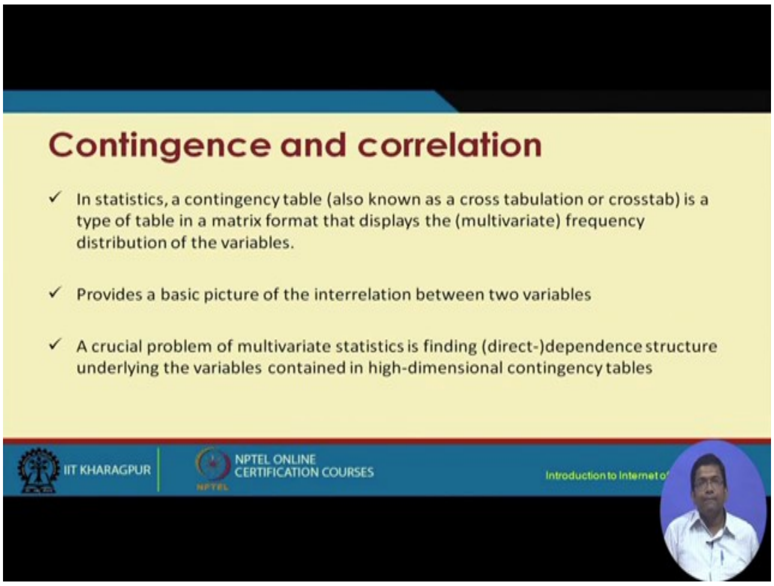
The next concept that has to be understood is data dispersion. Data dispersion concerns how much is the dispersion; that means, dispersion is basically a measure of the statistical. So, it is a measure of statistical dispersion a non negative real number that is 0 if all the data are the same and it increases as the data becomes more diverse. Examples of dispersion measures include: range, average, absolute deviation, variance, and standard deviation. So, typically when we talk about dispersion we typically talked about in terms of variance and standard deviation.

(Refer Slide Time: 13:58)



So, how much the deviate from the norm from the norm? So, this is what dispersion constants. So, here as I already mentioned so range and what is meant by it the absolute standard deviation is given. So, the average of the absolute deviation is given, variance and standard deviation here well known methods of dispersion deciding. And these are given over here.

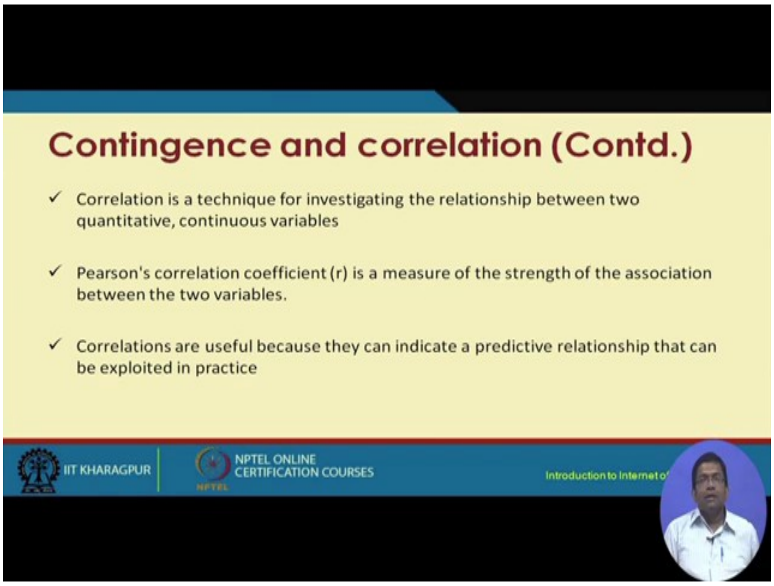
(Refer Slide Time: 14:19)



Next comes a contingence and correlation. So, in statistics a contingency table is a type of table in a matrix format that displays the multivariate frequency distribution of the variables.

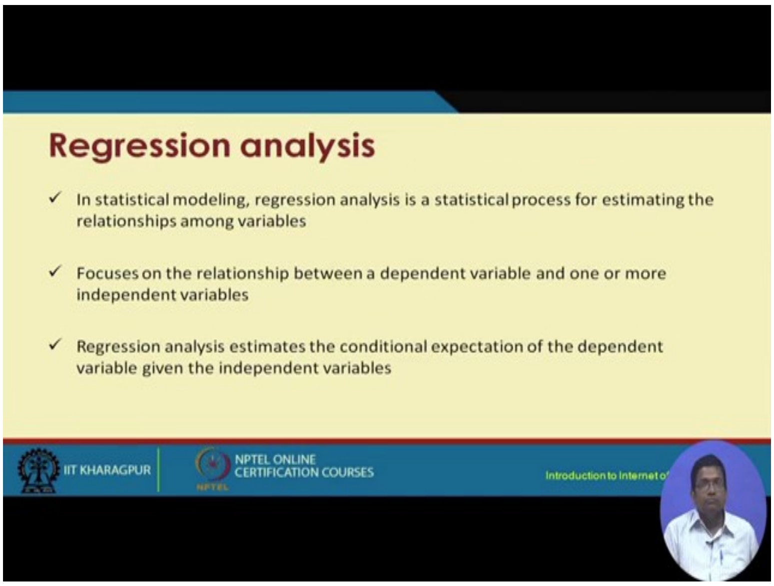
It provides the basic picture of the interrelation between two variables. Correlation is a technique for investigating the relationship between two continuative continuous variables.

(Refer Slide Time: 14:42)



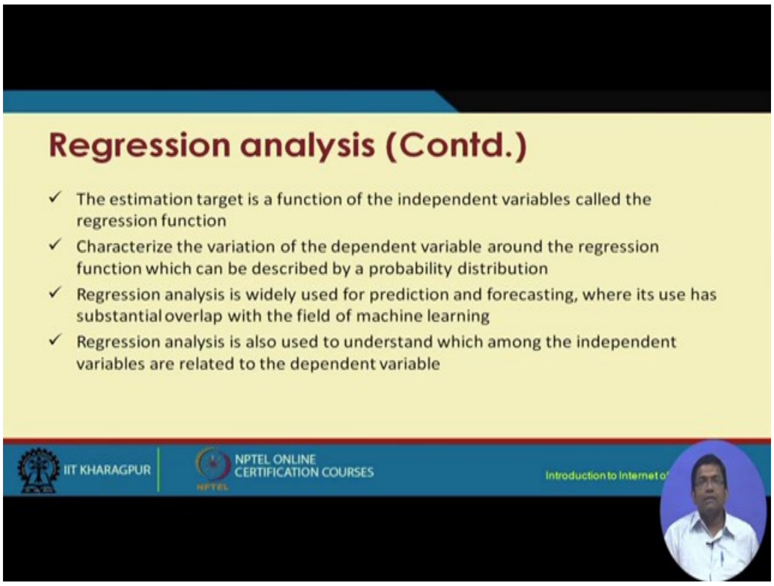
So, they have to be continuous variable this is very important. And how much they are correlated these two variables how much they are correlated and what is the relationship between them. So, a popular measure is the Pearson's correlation coefficient. And it basically measures the strength of association between two variables.

(Refer Slide Time: 15:13)



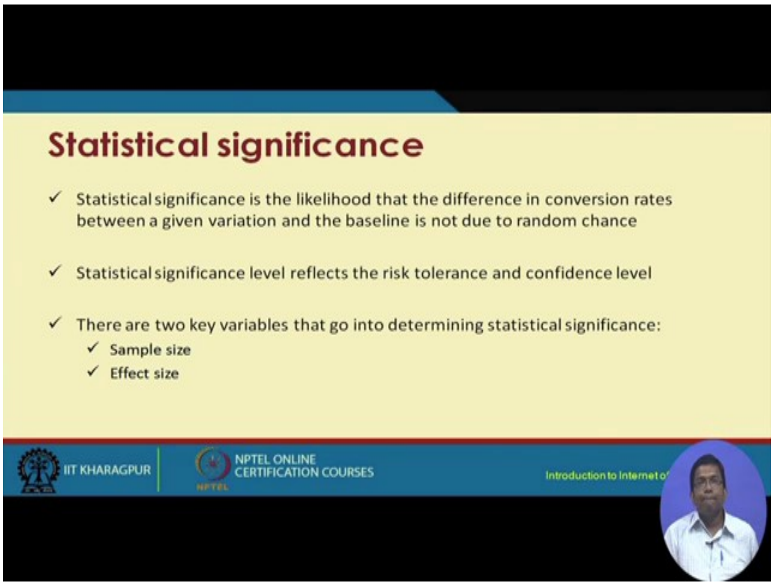
Then comes regression analysis. So, regression analysis basically tries to estimate the relationship among the different variables. It focuses on the relationship between independent variable and one or more independent variables. So, we have a dependent variable and we have an independent; we have one or more independent variables and how the dependent variable relates to one or more of these variables taken at a time or taken together.

(Refer Slide Time: 15:47)



So, regression analysis estimates the conditional expectation of the dependent variable given the independent variables. The estimation target is a function of the independent variables called the regression function. It characterizes the variation of the independent variable around the regression function which can be described by a probability distribution. So, regression analysis is helpful in different ways: it can be used to understand how the independent variables are related to the dependent variable one at a time or taken together.

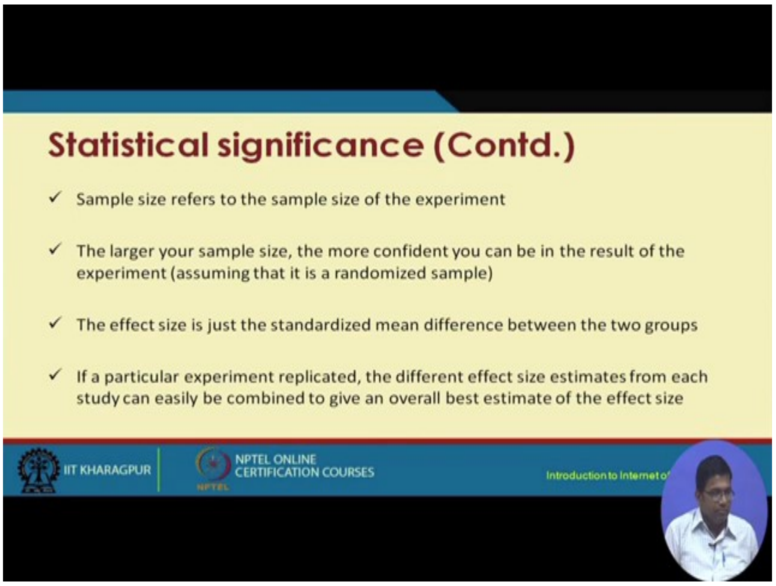
(Refer Slide Time: 16:16)



Statistical significance is important. It basically measures the likelihood that the difference in conversion rates between given variation and the baseline is not due to any random chance. So, statistically how much you know the results are significant is something that has to be measured. So, statistical significance basically reflects the risk, tolerance and the confidence level. So, how much is the confidence on the results that are obtained.

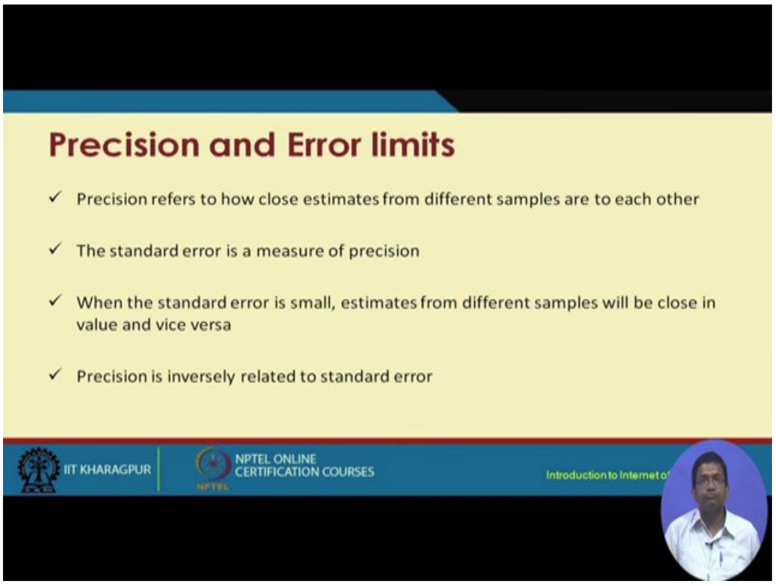
So, this is measure through statistical significance. So, typically there are two key variables that are required for determining statistical significance: one is the sample size the other one is the effect size.

(Refer Slide Time: 17:07)



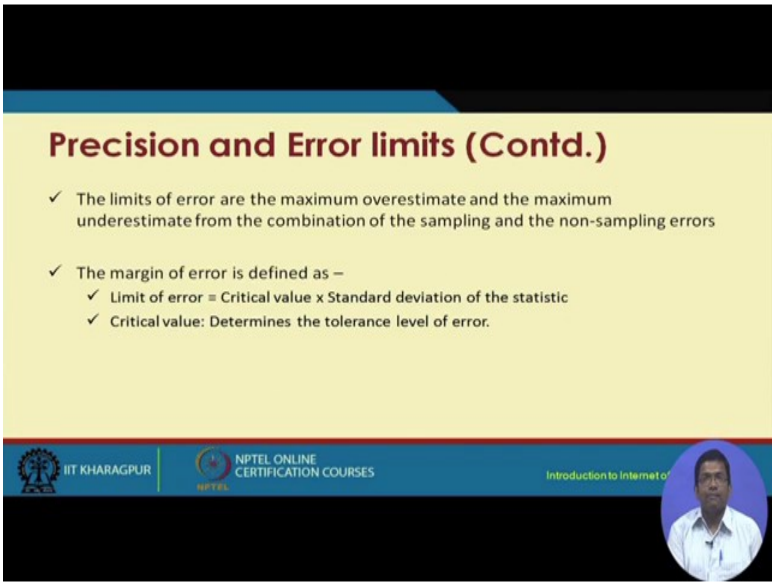
The sample size refers to the sample size of the experiment. The larger the sample size is the more confident one can be on the result of the experiment. And the effect size is just the standardized mean difference between the two groups. So, if a particular experiment is replicated the different effect size estimates from each study can easily be combined to give an overall best estimate of the effect size.

(Refer Slide Time: 17:38)



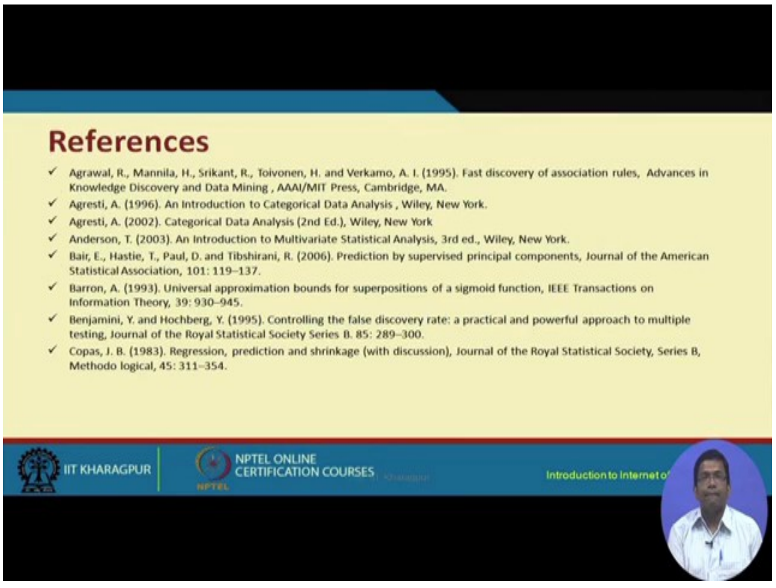
Precision and error limits are important. So, precision basically concerns how close the estimates are from the different samples to each other. The standard error is a measure of the precision, when the standard error is small the estimates from the different samples will be closed in value and vice versa. So, precision is inversely related to the standard error.

(Refer Slide Time: 18:03)



So, this precision and error become hand in hand, the limits of the error and the overestimate and the underestimate are taken into consideration while considering the error limits.

(Refer Slide Time: 18:19)



So, as I was mentioning at the outset that there are different statistical tools that additional statistical tools like correlation analysis, regression analysis, analysis of variance can be used in order to understand to how to get insight on the data that is obtained that is collected. But these are the basic analytic methods.

And what we have not discussed over here and we have intentionally confined ourselves to not discussing things like how text can be how text can be analyzed textual data or how video data can be analyzed and so on. So, that requires video data images can be analyzed and so on; so different other types of data can be analyzed. So, this we have intentionally not discussed, because that requires specialized training in text processing, video processing, image processing, and so on. And we do not want to get into the depth of those types of analytics.

So, these are the differences. So, with this we come to an end. And as I was telling mentioning before data handling, data analytics are very crucial in the context of IoT because lot of data gets generated in the IoT domain. And this data not only have to be analyze, but prior to analyzing they have to be handled. They have to be handled using technologies such as cloud, we have to be handled with technology such as Hadoop and so on.

And once they are handled that means, the data have been stored, they have been cleaned and stored and so on then they have to be analyzed. For analysis we have these different statistical methods, we have different other methods based in machine learning, image processing, video processing, text processing and so on. So, those are advance methods which we do not cover in this particular lecture, in this particular course.

Thank you.

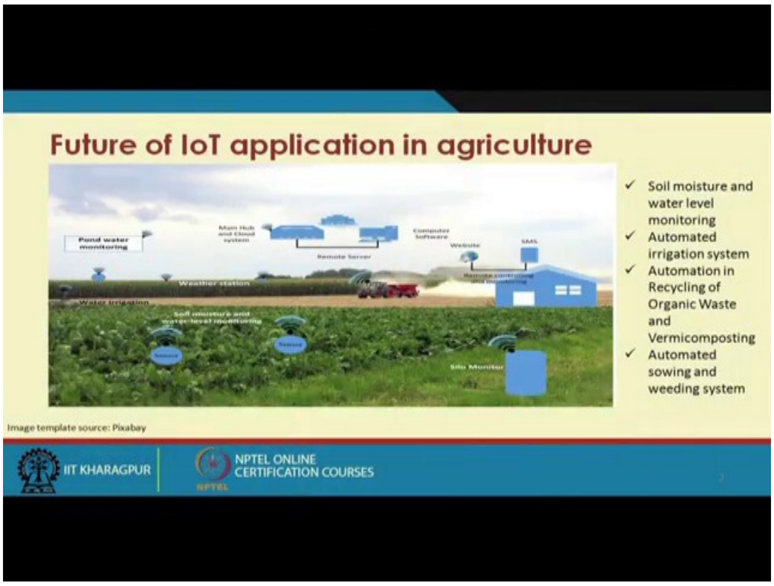
Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 57
Case Study: Agriculture

Having gone through the different concepts of IoT, the basic concepts the networking concepts, the communication concepts, the connectivity establishment concepts, the practical hands on on IoT in the previous lecture we will now go through a case study of how IoT has been used. And this particular case study is on agricultural use, so agricultural use of IoT more specifically on use of IoT for smart irrigation and this is basically based on a project that I have executed along with my colleague Professor N S Raghuwanshi from the Department of Agriculture and Food Engineering of our Institute IIT Kharagpur and here I am going to show you how IoT can come as help as help for building systems that can make irrigation smarter.

So, it is a smart irrigation management system the system that we have developed the name is AgriSens. AgriSens system and this is accessible this particular system is accessible publicly through the URL agri sys; agrisys.iitkgp.ac.in.

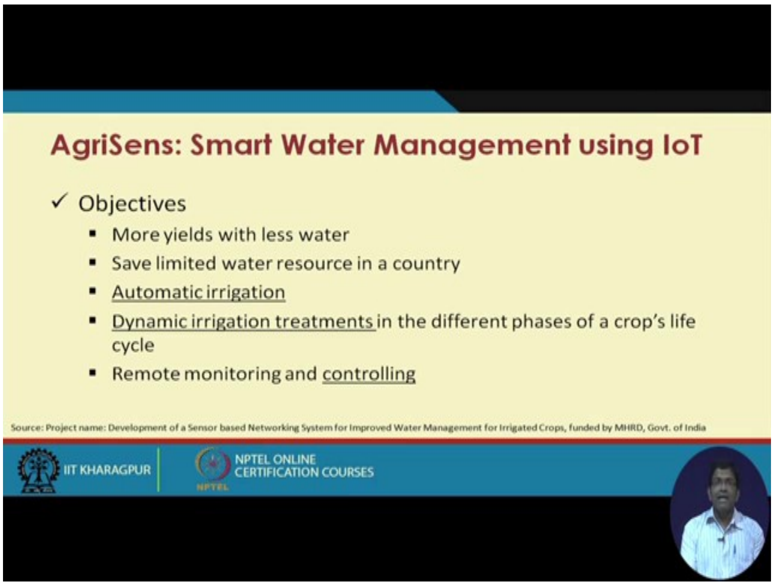
(Refer Slide Time: 01:57)



So, let us look at some of these different aspects of this particular system. So, before we go further I would like to show you a hypothetical scenario through this particular figure. So, what is going to happen the use of IoT in agriculture what is going to happen in the future? So, the picture that we see in front of us is an agricultural field a hypothetical one where there are different types of sensors that are planted sensor such as for soil, moisture and water level monitoring for automated irrigation performance performing automated irrigation.

Automated recycling of organic waste vermicomposting automated sowing and weeding and so on and so forth, so many different things automated systems fitted with sensors fitted with different actuators these are going to be used for making agriculture smarter. So, we in this particular project in the AgriSens system we have developed the system with a focus on water management using IoT smart water management. So, how do we do it?

(Refer Slide Time: 03:24)

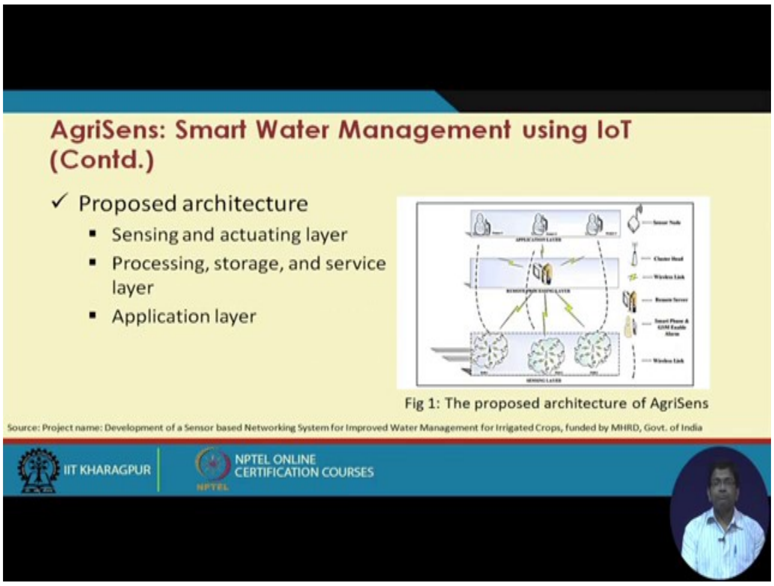


So, the objectives of this smart water management system the AgriSens system are that how less water can be used for getting more yield in in terms of crop productivity; that means, and typically you know. So, what happens is for plants such as rice; that means, paddy plants wheat and so on. These basically are dependent on the soil moisture the water level in the soil and so on and so forth and many other climatic factors.

So, the whole objective is that how can we monitor the soil conditions how much is the moisture content of the soil how much is the water level the stagnant water level particularly that is useful information for paddy crops paddy plants and how we can automate the irrigation process whenever the soil becomes dryer. So, if it becomes dryer below a certain threshold level how to automate this particular thing. So, automated irrigation how do we perform with the help of this these different sensors.

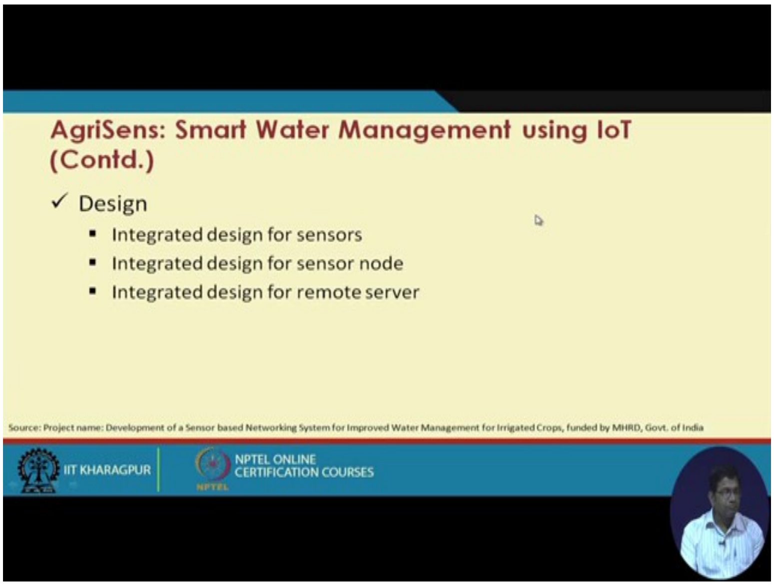
So, what we do is that based on these different sensed information through the soil moisture sensors water level sensors from the field we learn certain analytics based on the data that is received, and then if though if it is found out by the system autonomously by the system without any human interference if it is found out by the system that the water level has gone down or the soil moisture level has gone down or those are all climatic conditions are no longer prevailing. Then to take some actions, the actions can be in terms of sending some control signal for example, switching the pump on to irrigate the field and so on and so forth and there can be done remotely as well as well as autonomously automatically.

(Refer Slide Time: 05:36)



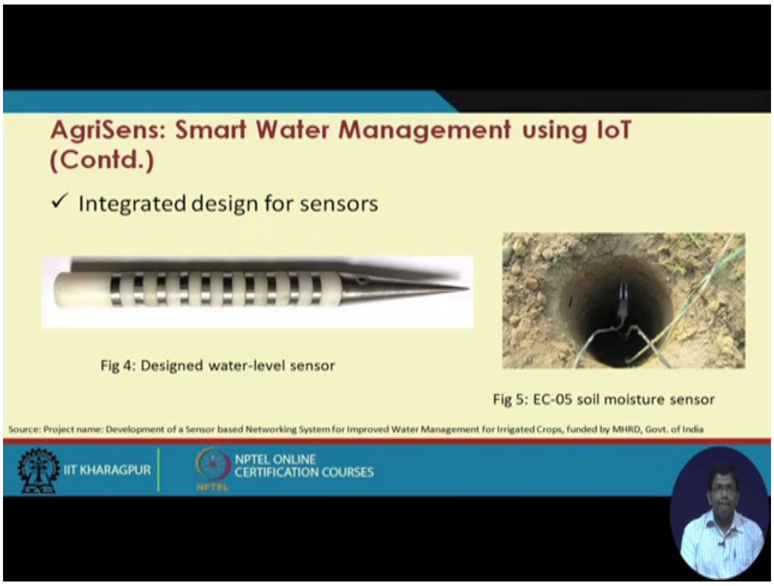
So, this is what the AgriSens system does. So, this is the proposed architecture of the AgriSens system for offering smart water management. So, we have different layers of the system so we have the sensing layer the remote processing layer and the application layer the sensing layer basically has different types of sensors soil moisture water level etcetera which through data from different clusters this through data through their cluster heads to the remote processing server and different analytics and run and those data are made available to the different applications in the application layer.

(Refer Slide Time: 06:17)



So, this particular project involved different objectives such as the design for the sensors, designing the sensor node as such and the design of the remote server and the communication framework. So, as part of this project what we did is we developed a sensor that can be used for monitoring the water level in the field. So, this is this particular sensor which we have developed in our lab for monitoring the water level in the field.

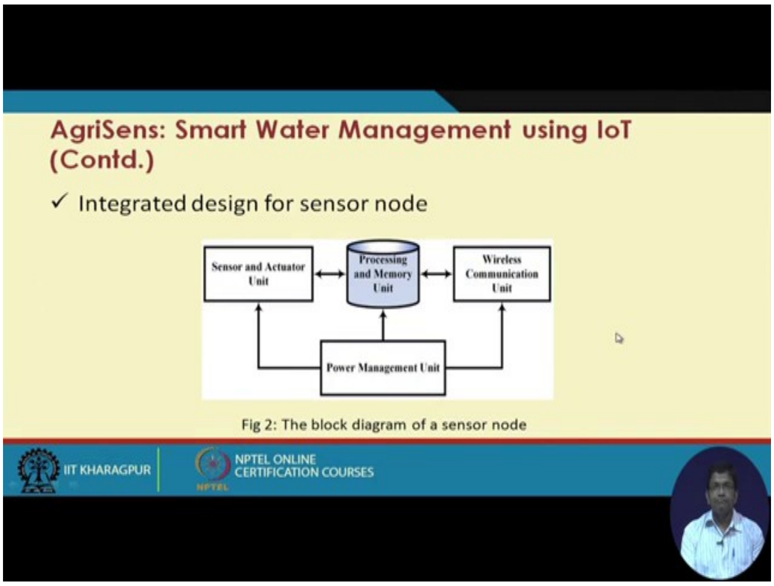
(Refer Slide Time: 06:40)



So, another sensor which we did not develop, but we have procure is the EC 05 soil moisture sensor which in this particular figure as you can see in this particular picture as you can see has been put it has been you know dug inside the surface of the earth.

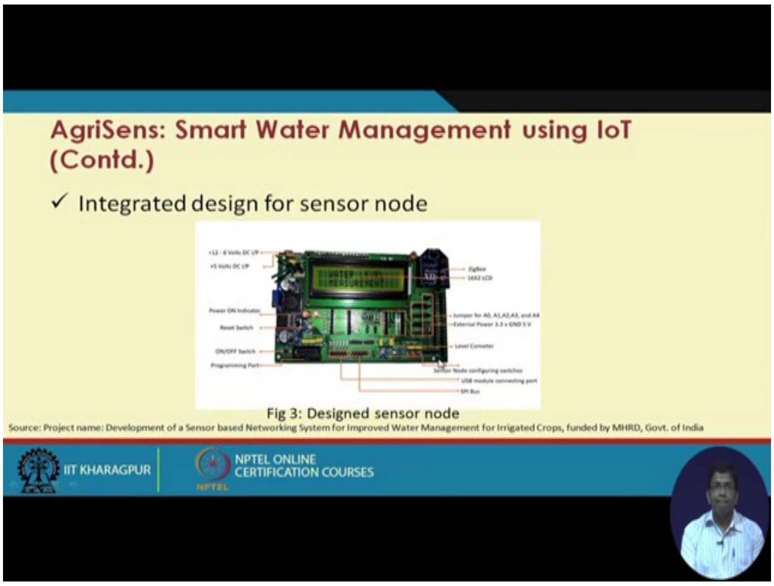
So, soil moisture sensor is basically put inside is installed inside the level the level of the mud level of mud or level of earth. So, it is inside it is dug inside.

(Refer Slide Time: 07:40)



So, this is the overall design of the sensor node. So, here basically what we have is apart from the sensors and actuators we have a processing unit and the memory unit we have wireless communication unit and we have the power management unit.

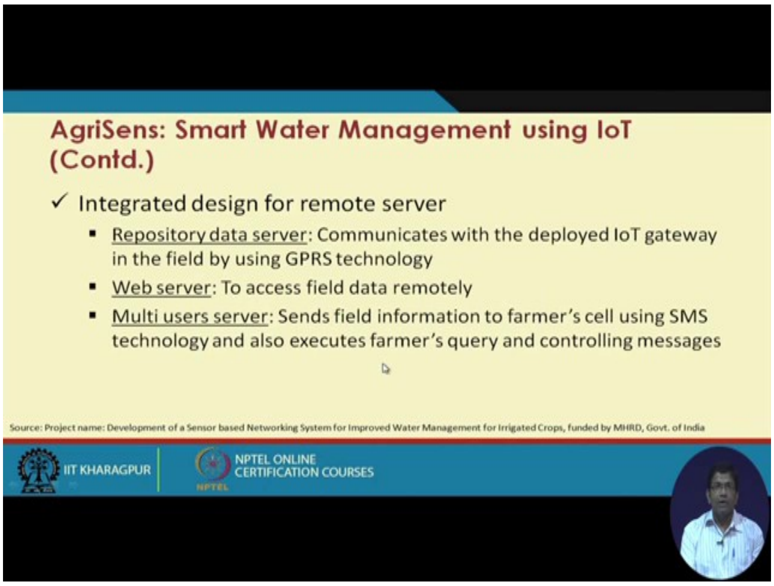
(Refer Slide Time: 08:01)



So, this is the integrate design of a sensor node that we have developed this is this one node and this node basically as you can see over here it comes with an LCD and it is powered by Zigbee for communication and Zigbee in one of the previous lectures on connectivity technologies we have already gone through Zigbee. Then it also has a power supply it has different power supplies then it has a power on indicator, a reset switch, the on off switch and different sensors can be fitted to this particular core.

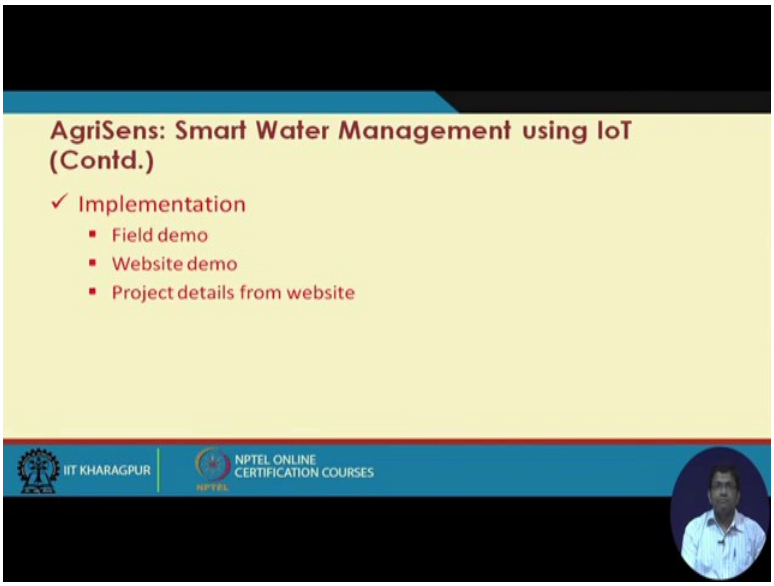
So, this is the censor board that we have designed and which can be used for agricultural purposes smart irrigation purpose.

(Refer Slide Time: 09:00)



Then the remote server basically it has a repository which can take all the data from these different sensors these IoT nodes through the IoT gateways and there is a web server which basically stores in the field data remotely; that means, the web server are typically stored away from the field and that is where the data are all stored for use in the future. And there are multi user servers which basically send the field information to the farmer's cell using SMS technology, and also executes the farmer's query and controlling messages. So, basically this basically helps in informing the farmers about the field conditions with the help of SMS and different sending different SMS's.

(Refer Slide Time: 09:50)



So, we will now look at a field demo and thereafter I am going to show you few other different aspects of this particular system. So, I am going to now take you to the field and show you how the system is deployed and how it functions at the field.

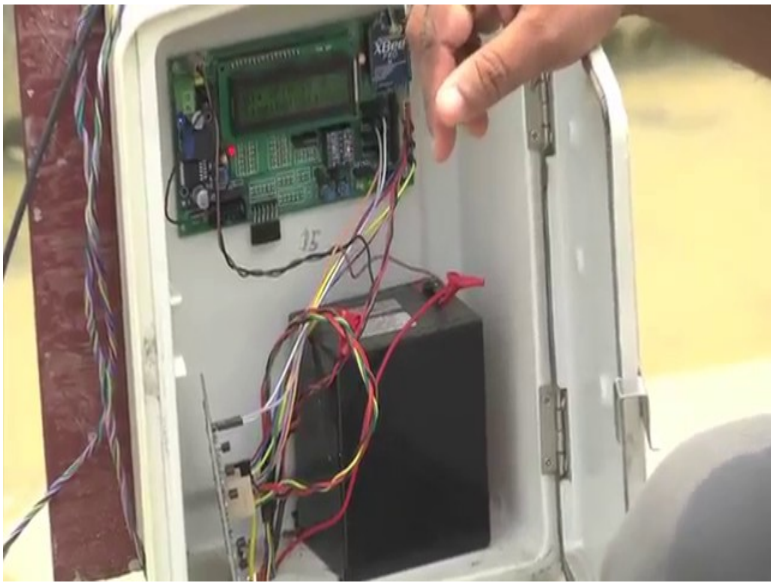
Now I am going to show you one of the implementations of internet of things in agriculture. More specifically this is for irrigation purpose how IoT can be used for irrigation purpose and what we are doing is this is actually by the way developed as a sponsored project of MHRD and IIT Kharagpur and this was being developed along with my colleague Professor N S Raghuvanshi of the department of agriculture and food engineering at IIT Kharagpur.

So, what you see over here is an agricultural field. So, in this field, this field is divided into a 6 by 5 grid and each of these grid elements has a size of 3 by 3 square meters.

(Refer Slide Time: 11:05)

And so in each of these grids what we have is a sensor node and at this point actually you cannot see any crops because the crop the season has gone and the crops have been harvested, but this is the infrastructure that we have. So, this is a solar powered sensor node and if we look here in this node we have through this node actually we have two different sensors - one is a soil moisture sensor which is basically buried in ground and there is another sensor which is the water level sensor. So, the soil moisture sensor basically as this name says that it basically sensors the soil moisture and the water level sensor is how much is the stagnant water level in this particular grid. So, this is what it measures.

(Refer Slide Time: 11:32)



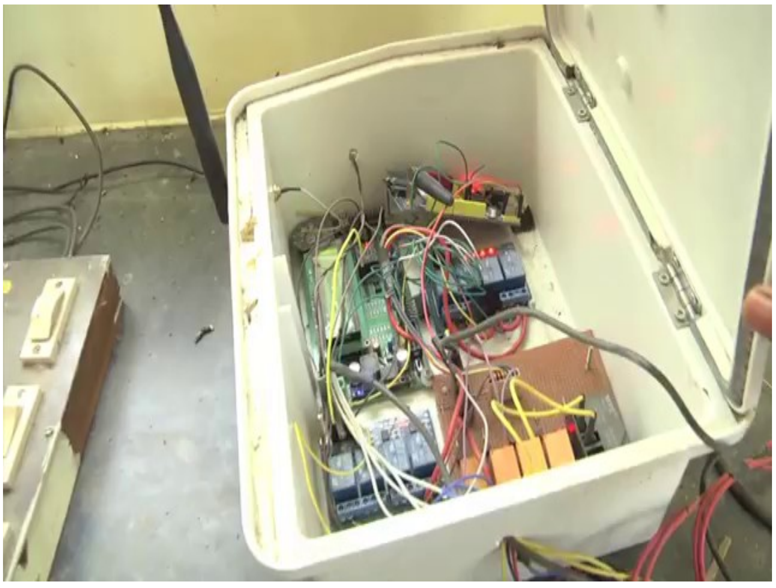
And these two sensor data are sent to this particular node. So, this node basically has you know it is Zigbee power and this data has Zigbee communication with the cluster head. So, here actually what we use is a cluster based approach cluster architecture for sensor deployment. So, from this node from every node that we have here the data are sent via Zigbee to the cluster head and from the cluster head. Cluster head basically supports two types of communication one is the Zigbee communication for intra cluster communication and the other one is the GPRS communication from the cluster head to the control room where the servers are there for further analysis.

So, this is the architecture that we have and so the sensor data you know are being in the sense from these two sensors - one is the soil moisture and the water level sensor and if the water level has gone down or the soil moisture is not adequate enough. So, automatically we have the valves the solenoid valves and the solenoid valves will be turned on, so here is one solenoid valve that you can see on your on my left here the solenoid valve and likewise every field has other solenoid valves. So, there is another solenoid valve there.

(Refer Slide Time: 13:29)

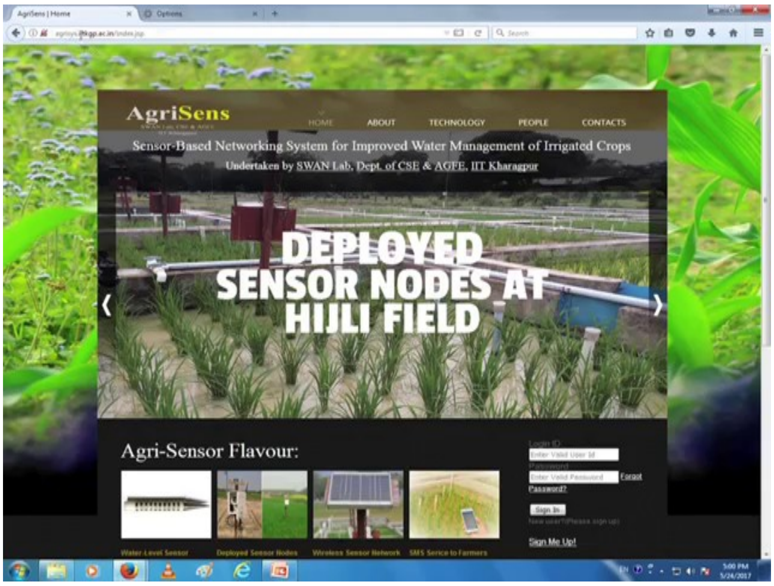
So, what is going to happen is the pump you know it is going to turned on will be turned on and the water is going to be you know the field is going to be irrigated by those this solenoid valves. So, as you can see over here the valve has been turned on just now and the field is going to be irrigated with the water because there is no I am not adequate water in the field.

(Refer Slide Time: 14:22)



So, as I told you that we are actually following cluster based architecture for the sensor deployment so here what we have is a cluster head this cluster head has support for both Zigbee communication which is happening through this particular node and there is also support for GPRS communication through this particular board. And additionally we have the different relays as you can see here for turning on the pumps if it is required to irrigate the field and so through this antenna basically this communication is happening with the with the external world. So, this is how the cluster head looks like.

(Refer Slide Time: 15:08)



So, now I will show you the web interface for this AgriSens system. So, as I mentioned to you earlier it is accessible through the URL agrisys.iitkgp.ac.in and we have deployed this particular system in two locations one in (Refer Time: 15:31) IIT Kharagpur and the other one in a distant village close to Bidapur.

So, this is the overall you know web interface and as we can see over here that it gives lot of information about the water level sensor that we have developed the deployed sensor nodes you can read more, the wireless sensor network that is there and the SMS service that is offered to the farmers. So, more information is available through this site and also through these different links the people that are involved I already mentioned to you that it is being it has been done by our group the swan group of the department of CSE along with the agriculture and food engineering department at IIT, Kharagpur.

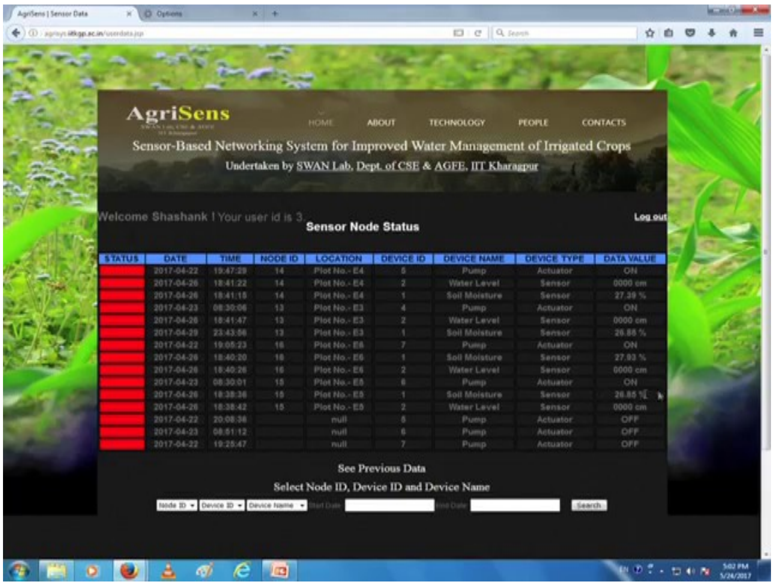
(Refer Slide Time: 16:30)

So, here you know we can through this particular portal we can look at the field conditions and the different sensors you know the different health monitoring on the different sensors that are there.

(Refer Slide Time: 16:39)

So, if you login using the login credentials, this is basically the node status from one of the fields as we can see these are the different status that I had mentioned and these are the different status that I had mentioned.

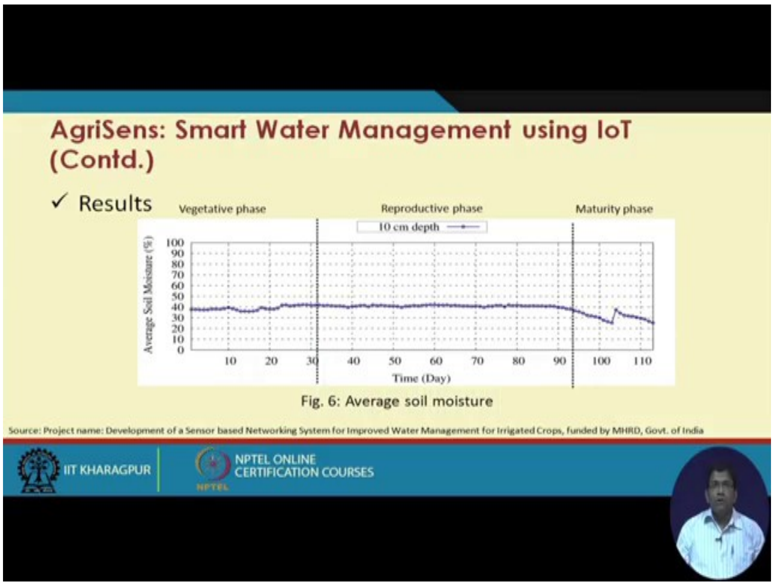
(Refer Slide Time: 16:54)



So, we have red colour implying that now actually the clock has already been harvested it was a paddy, paddy field where the sensor nodes are deployed. So, crop has already been harvested that is why it is showing red colour means that the sensor node is not sensing any further data. And also the different status messages you know so can be obtained through this particular portal and previous data also one can see through this and, so this basically you know helps in remote monitoring of the field you know even if one is in another part of the world still they you would be able to monitor the field conditions. So, this is how the overall portal looks like.

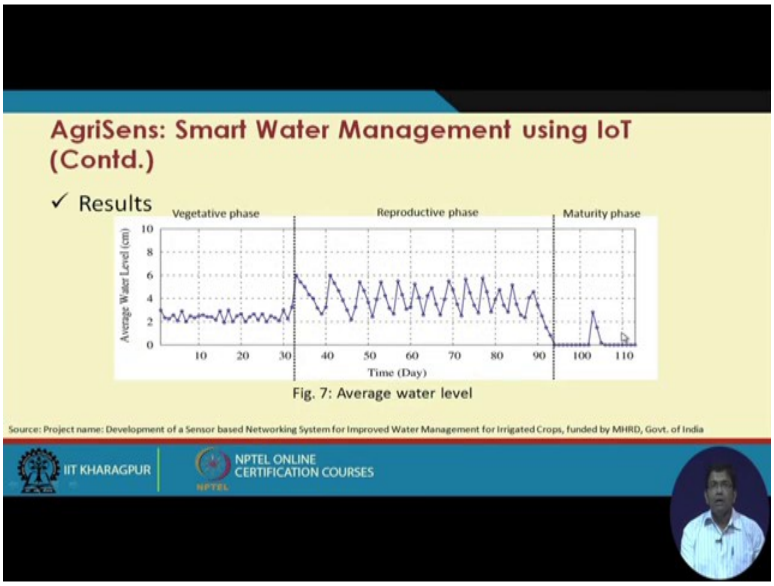
So, now, I will show you some of the plots of the data that I received at our server.

(Refer Slide Time: 18:10)



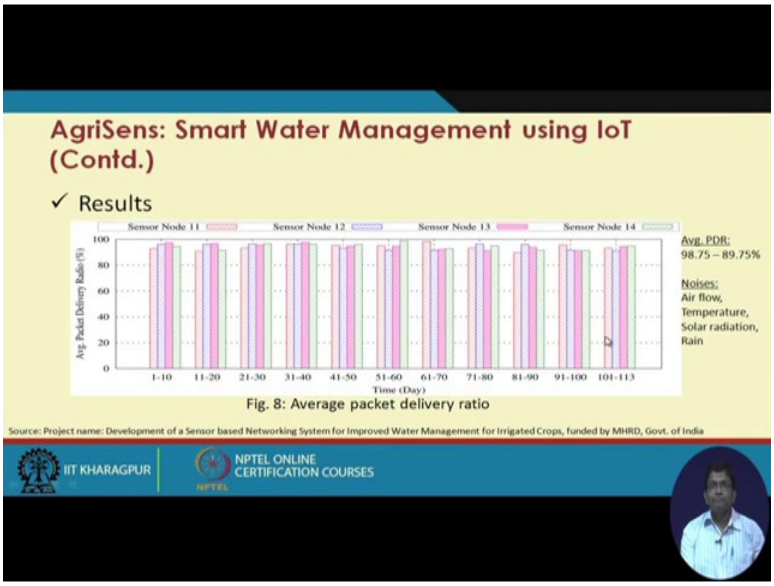
I have already shown you how the different sensors are deployed in the field and these are some of the results that we have received some of the data that we have received with respect to things such as the soil moisture. So, this is the soil moisture data with respect to the time. So, here actually we have some 115 days data and as you can see over here the soil moisture variation with respect to the different phases of crop growth during the paddy season is basically plotted over here. So, this particular phase is shown to be the vegetative phase and the soil moisture variation is shown in this particular plot. Then we have the reproductive phase where the soil moisture varies like this and then we have the maturity phase and in the maturity phase as you can see that there are some variations in the soil moisture of the field.

(Refer Slide Time: 19:21)



The next one is the water level. So, here actually we can see that in the vegetative phase the water level fluctuations are there, but it is not too much, but then during the reproductive phase the water level fluctuations are quite huge. So, whenever the water level goes down the field is irrigated, again water level goes up, again it goes down and so on and so forth. So, this is the reproductive phase and then we have the maturity phase where the water level variations are as shown.

(Refer Slide Time: 19:52)



And then this plot basically shows the packet delivery ratio and as we can see over here the packet delivery is not so bad you know it is between like 90 percent to 100 percent. There is some packet drop that has happened and these packet drops could be due to different reasons such as different presence of different noises interference and so on, due to things such as air flow, temperature, solar radiation rainfall and so on. So, these packet drops are quite common, but as you can see that mostly the system overall is quite reliable.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 58
Case Study: Healthcare

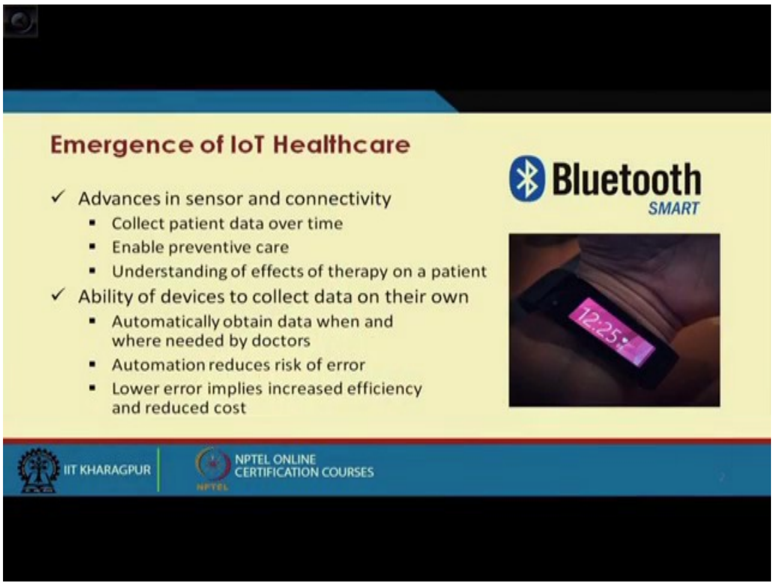
Now, we are going to cover some case studies particularly focusing on healthcare, so the use of IoT for healthcare. So, we have seen in the previous lectures in the different modules that we have covered so far in this course that different types of sensors are possible and these sensors can help in sensing whatever they are supposed to sense. So, in the context of healthcare there are different sensors that have been fabricated that has that have been developed to monitor the physiological condition of human beings. So, for example, there can be body temperature sensor which can measure exactly what a normal temperature normal thermometer does, there can be blood pressure sensor which can measure the blood pressure of human being. There can be likewise different other types of sensors for example, pulse oximeter sensor, ECG sensor, EMG sensor and many other different types of sensors.

So, in the IoT sphere these different sensors which have been developed individually by different companies different research labs and so on they can be used to build the sensor nodes and we have in a previous lecture we have already gone through what are the different components of a sensor node. So, sensor is one of the one of those components likewise there are different other components there is a processing unit that is required there is a communication unit there is a power unit and so on.

So, all these different units put together is basically a sensor node and the sensor node can sends the physiological parameter based on the sensor that is fixed with that particular node. And likewise in the human body there could be different sensors which can be basically you know sense sensing the different physical physiological phenomena and sending to the sensor node either singly or different sensor nodes together they can be sending different data to one particular one particular such node and from that node the data can be sent elsewhere for further processing and so on.

So, what we have? We have number one the sensing number two is the communication of the sense data to somewhere and then from that place the data either has to be you know it has to be processed locally or it has to be sent somewhere else for better processing for faster processing and dissemination of the results of the processing. So, this is exactly what is typically done in most of the IoT healthcare solutions. So, in this particular lecture I am going to cover what are the different IoT healthcare sensors that are there and how these can be used to build different systems that can help in continuous real-time with remote monitoring of patients which is taken up as a specific case study and this is the system which is known as the AmbuSens system that we have developed in our lab in the swan lab of IIT Kharagpur and so in the little part we are going to talk about what this particular system does and some of the important salient features of this particular system, AmbuSens system.

(Refer Slide Time: 04:10)



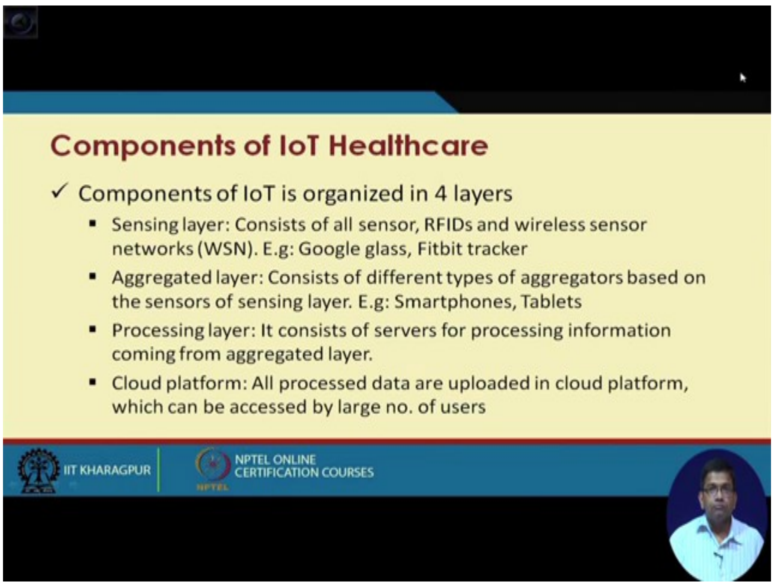
So, you know when we talk about the sensors the sensors in the context of health care the sensors they can collect the patient data over time and I have already mentioned what kind of data. So, these data could measure blood pressure or body temperature or you know oxygen saturation in the blood and so on and so forth. So, this data is collected and this data can be analyzed further either locally or remotely for you know for different purposes for example, to enable preventive care. So, you know preventive care means like you know you collect a data over time and based on that you try to understand that whether there is a critical element that is going to come in the future for that particular patient so this is number one.

Number two is that if a particular patient is in the hospital for instance then that patient you know is typically you know it is the patient is under different types of medications and the patient is fitted with different types of devices and so on. So, understanding the effects of the therapy, therapy that is being you know subjected to that particular patient, the effects of the cell therapy on the patient. So, this is another advantage of using the sensors. And connectivity basically what it does is the connectivity will allow these sense data to be sent remotely for remote processing decision making and so on.

Now, that the devices they have different types of ability to collect data they can you know they can either automatically obtain the data and the data can be sent to doctors you know then and there itself or it can be the data can be stored in some server or something like that where then will be some kind of analytics that will be run that will be executed. And based on the analytics if somebody in if a patient is likely to get some serious condition then the corresponding doctor is going to be notified. So, as you can understand that by automating these things with the help of sensors and connectivity what we are trying to do is number one we are trying to reduce the manual intervention; that means, the attention of the doctors continuously.

Second thing is the chances of error the risks of errors occurring also get reduced because automation inherently basically reduces the chances of error and that overall you know these things would overall increase the efficiency while reducing the cost of operation cost of you know maintenance and operation of a of healthcare system.

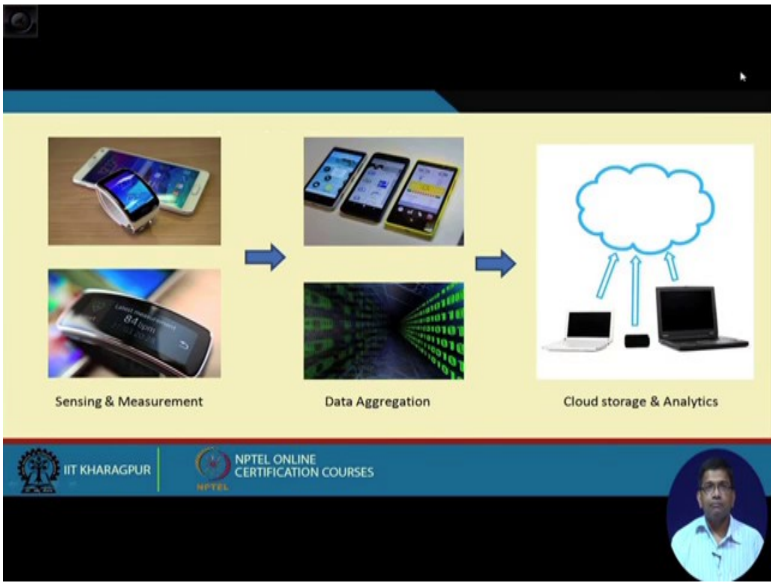
(Refer Slide Time: 07:09)



So, there are different components of IoT healthcare. So, I already mentioned that you know there has to be sensors the physiological sensors. So, these sensors are part of the sensing layer and the sensors you know they could consists of all these different types of sensors that I mentioned the RFIDs you know sensor networks and so on and Google glass and fitbit tracker these are some of these different devices that execute in the sensing layer.

Then you have the aggregated layer which basically you know aggregates the data that are received from the sensors of the sensing layer and this data aggregators could be things like you know smart phones or tablets and so on. So, what these data aggregated does is from the different parts of the human body the different sensed data that are obtained these are basically connected and these are you know these are put together and you know and instead of sending the individual data together you know reduced number of data are sent forward from that particular aggregator node. So, then you have the sensing layer the aggregator layer and then we have the processing layer where basically the processing layer and the cloud platform these are responsible for the storing of the data and the processing of the data that have been collected and analyzing further that you know what action should be taken based on the received data.

(Refer Slide Time: 08:49)



So, we have these different types of sensors as part of the sensing and measurement. So, you have these different sensors the smart watch and blood pressure sensor and so on which would sense and measure the physiological conditions data are sent to these different aggregator nodes you know which could be like these different PDS or you know mobile phones, smartphones and so on. And from the data aggregator the data are sent further from the aggregator by the way this segregator is also known as the LPU sometimes the; that means, the local processing unit. So, typically if you are talking about a human body the body area network. So, typically in a body area network you have a single LPU which receives the sensor data from the different parts of the body.

So, every human being has that LPU which is a smartphone or a tab or something of that sort and that particular device connects receives all these data and this data is further processed in the cloud and in the different servers. And based on that you know different decision making can be made and based on the decisions the corresponding stakeholders could be informed about what is happening with the patient if it is required.

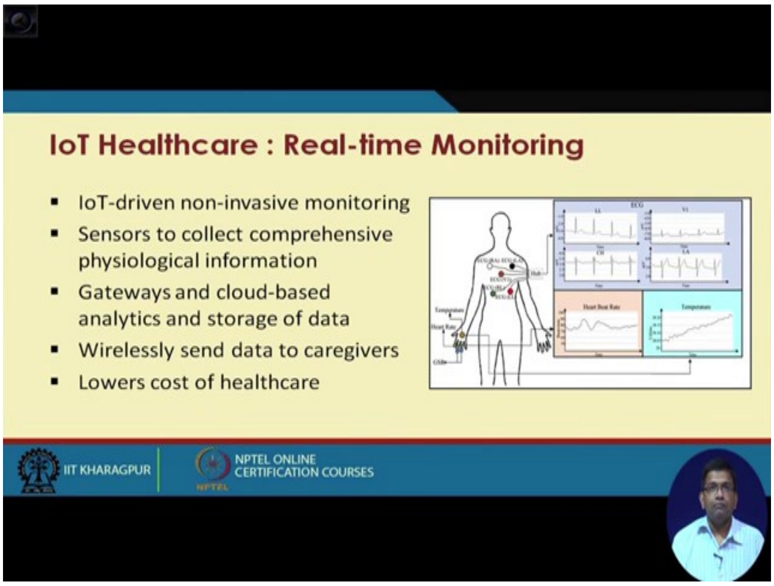
(Refer Slide Time: 10:16)

So, there are different directions of research in IoT healthcare number one is remote health care and this is where we have done a little bit of work in our lab and so what happened says you have the all these different sensors the blood pressure monitor sensor the temperature sensor and so on which typically are developed by different vendors different companies. So, what happens is you know at the same time remotely with the help of the sensors the doctors and the paramedics you know they can the healthcare professionals in general they can monitor the condition of different patients in a large scale you know in numbers they can monitor the different patients even remotely. So, that is the remote health care.

So, this wireless IoT different solutions being health care to patients rather than bring the patients to the health care. So, typically you know earlier what is used to happen or the in the traditional healthcare the patient should have to go through the healthcare facilities like hospitals or the nursing homes and so on. And in the IoT based health care what happens is all these different medical devices they are portable they are wearable and so on. So, they can be the human beings the patients they can wear and only thing that has to be done is that somehow this data from this wearable sensors have to be sent to the corresponding medical professionals for example, your personal doctor you know the family doctor and so on who you know if it is required you know the doctor would intervene further maybe because of some serious condition going on in the patient and so on.

So, securely in this sort of systems would capture a variety of medical data through IoT based sensors analyze the data with different smart algorithms and this wirelessly this data that is obtained from this different sensors are sent wirelessly to different medical professionals for for the recommendation.

(Refer Slide Time: 12:13)



Real-time monitoring is possible as a result of the use of the different sensors this biomedical this you know physiological sensors real-time monitoring is possible. So, earlier what is to happen is that if you need to monitor you know if you need to know how much is your blood pressure you would have to go to the hospital and get your blood pressure measured or even if you have a blood pressure measurement device at home you know typically what happens is you do not measure it all the time right.

So, in the case of this kind of system where there are different sensors the blood pressure sensor you know the blood pressure sensor would be you know with the help of the sensors it will be possible to monitor the condition of the patients in real-time round the clock it is possible. But then you know it depends on the implementation policies and so on that how often this measurement is going to be done based on the requirements of the stakeholders. The sensors are used to collect comprehensing physiological data then that this data are sent to the cloud through the gateways for further analysis and storage rather storage analysis.

So, wirelessly this systems would send the data to the caregivers and thereby overall the system as a whole would reduce or would lower the cost of healthcare. So, this is the schematic of you know how such a system would work you have these different sensors these different heterogeneous sensors you know denoted by different colours. So, these sensors would sends and send the data and that those data would be made available to the remote doctors and the doctors can monitor in real-time how much how with the heart rate is varying for a particular patient or how the body temperature is varying and so on.

(Refer Slide Time: 14:11)

And the next advantage is of preventive care. So, in preventive care what you need to do is you know you have some of this target group of patients treated with different physiological sensors and for instance in the case of seniors senior citizens who do not have any caregiver at home they could be fitted with different sensors and one of the common problems with this senior people is that you know they often fall down right.

So, fall detection is an important problem and this fall detection is part of this preventive health care and so what happens is if there is an emergency situation that occurs and the detection of this emergency situation and alerting the family members under those situations. For example, the senior citizen has fallen down at home. So, if there is a proper system IoT healthcare system in place then the corresponding people in the person's family or the different relatives they could be they could be informed about this particular event; that means, the falling of the person.

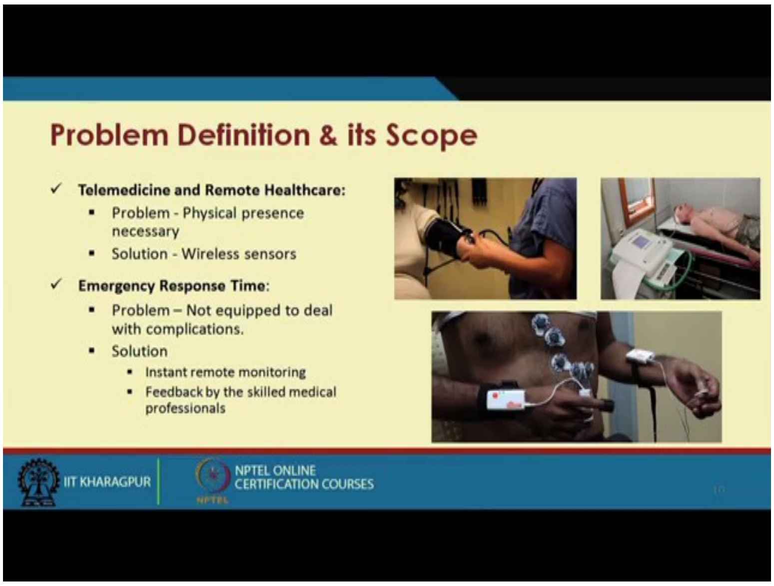
Then there are different interesting tools from machine learning that that could be used to track the trend and to predict what is going to happen in the future for example, if there is any anomaly detection of the anomaly and how this anomaly is varying with time and what can be done in the future to prevent. So, all these things are possible with the layer with the help of different machine learning tools. So, now, we come to the AmbuSens system and as I already told you initially this AmbuSens system has been developed by us and it was actually funded by a joint project supported by IIT Kharagpur and MHRD through funds from MHRD government of India.

And, so this in this project we have developed a system which can help in remote monitoring remote continuous monitoring of patients in ambulances when they are transferred from remote health care centers to city hospitals you know which is a very typical kind of scenario that happens in the case are in a for health care in our country and we have developed a system for that and Neeloy Saha he is going to explain to you about the different functionalities of the system how it works how it has been built what are the different challenges and so on.

And thereafter we are going to go through simulation which will an animation sorry an animation which will which will show you how IoT healthcare solutions can be deployed in order to give better healthcare to the different citizens of a country.

Hi, I am Neeloy Saha a research scholar under doctor Sudip Misra and I will discuss about the different facets of the AmbuSens system. The AmbuSens project mainly aims at addressing the shortcomings of the existing healthcare infrastructure in our country with a particular focus on ambulatory healthcare using the communication and the sensing technologies of the internet of things.

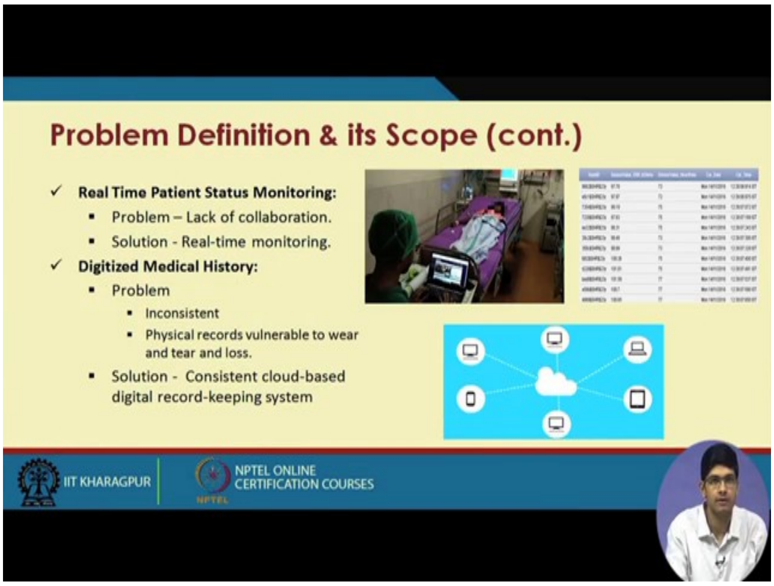
(Refer Slide Time: 17:29)



One of the main problems of the existing healthcare system is that it is more of a manual operating system that is it requires the physical presence of the patient at the health care centers. So, using the variable sensing technologies and the wireless sensors which are often small in size and variable, using the AmbuSens project we attempt to bring the healthcare closer to the patients.

Another problem that is existing in the traditional healthcare is and that is especially pronounce in the case of ambulatory healthcare is that of emergency response type. Often times the medical personnel or the technicians who accompany the patients in the ambulance are not well equipped to deal with any complications that may arise that is because they do not have the technical expertise to deal with such complications. Using the AmbuSens projects and its instant real-time monitoring capabilities we have the provision for remote feedback and monitoring by the skilled personnels at some remote place and this significantly can help in dealing with such complicated complication and such problems that may arise during transit in an ambulance.

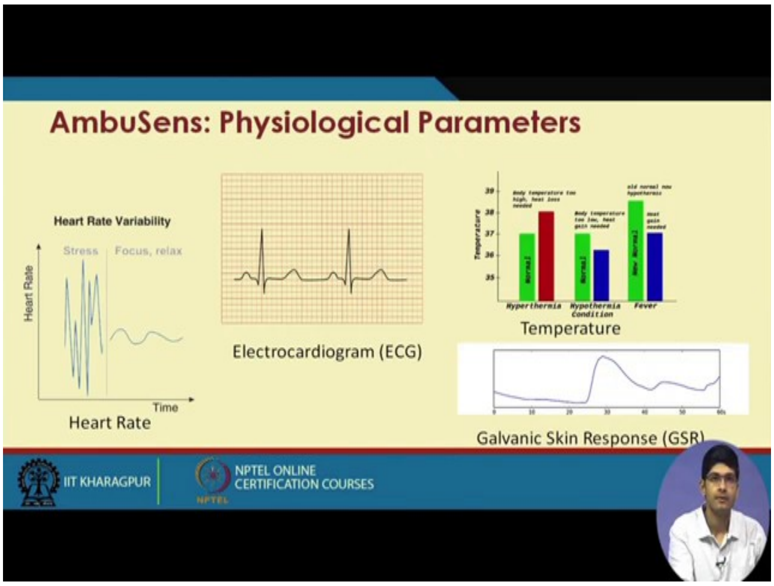
(Refer Slide Time: 18:54)



Another problem that often arises is that of real-time monitoring; for example, let us consider a case in which a patient is transferred using an ambulance from a primary or secondary care hospitals in some town or rural area to a specialized clinic in the city. So, while the patient is actually going from the town to the city in the ambulance the condition of the patient is not monitored at all. This may lead to some problems such as the patient condition may degrade over time and when the patient actually reaches the destination the destination hospital the doctors they are may not be equipped to deal with that condition.

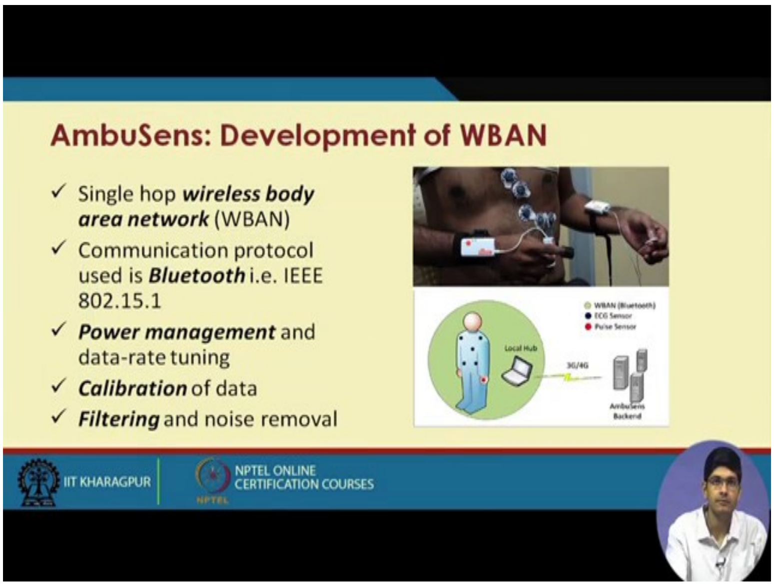
So, using the real-time monitoring we can or the AmbuSens system we can track the dynamic changes of the patient's condition over time and this can significantly reduce the latency of the medical care. The existing system traditional healthcare also requires each patient to carry his or her own medical records with him whenever he visits the healthcare facilities, but these physical records are vulnerable to physical loss wear and tear. So, the AmbuSens project also incorporates a cloud based digital record keeping system to deal with these kind of challenges.

(Refer Slide Time: 20:35)



The AmbuSens project incorporates different IoT based sensing technologies and is capable of monitoring different health parameters some of the parameters monitored are heart rate electrocardiogram, temperature, galvanic, skin response etcetera. The exact parameters which are monitored depend are often dependent upon the particular application scenario for example, if we consider the case of a patient having some cardiac disease the electrocardiogram or ECG will be of primary importance. Also in a pediatric case the temperature often plays a vital role.

(Refer Slide Time: 21:25)

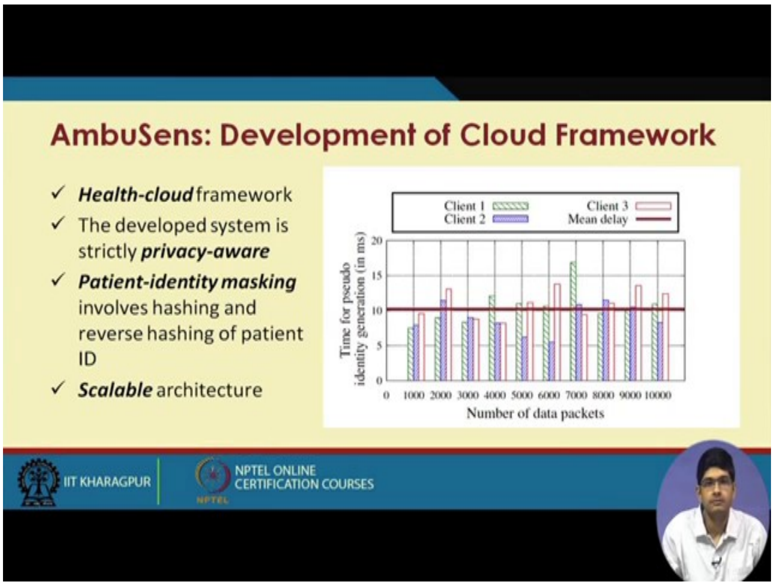


The sensing layer of the AmbuSens project consists of different wireless sensors which sample the physiological data coming from the patient and using internet of things communication technologies such as Bluetooth, Zigbee among others the data is sent to a local herb or a local data processing unit where the data is aggregated and sent further for processing.

Now, the challenges that we faced in the aggregation layer include power management data rate tuning and noise. Data rate tuning is a challenge because it is often times related to power management for example, and also data fidelity for example, when dealing with electrocardiogram or ECG data we found that minimum sampling rate of 1024 hertz what was needed to preserve the fidelity of the ECG data. Noise is a important parameter that must be taken into account at the sensing layer especially never scenario where we are dealing with the mobility of a patient often times due to the movement and the jerking of the ambulance the thinners that we are receiving corrupted in the presence of noise.

So, we implemented different kinds of filtering algorithms in the local data processing unit to obtain a clean noise free signal.

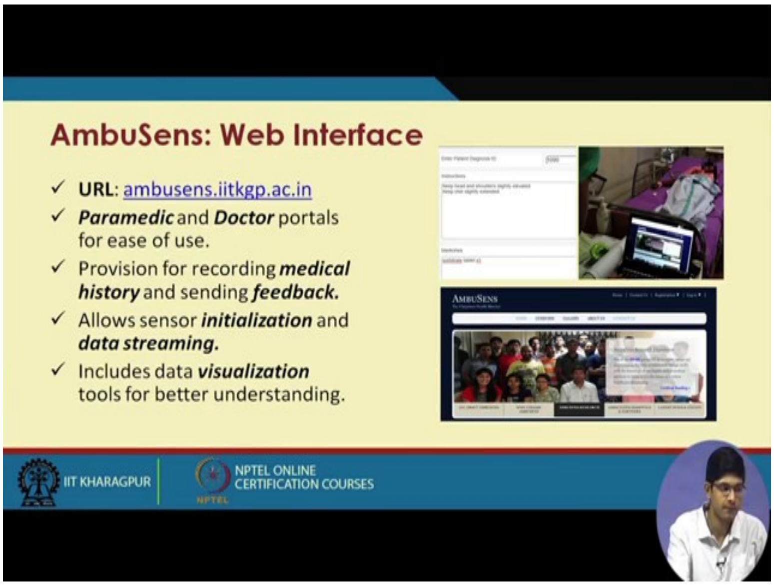
(Refer Slide Time: 23:06)



The AmbuSens project also leverages the power of cloud computing for storage and analytics, but here the challenge is that we are dealing with medical data which is often of a sensitive nature for a privacy stand point. The cloud computing and storage is often vulnerable to compromise of a patients identity. So, here we have developed a health cloud framework which is totally privacy aware.

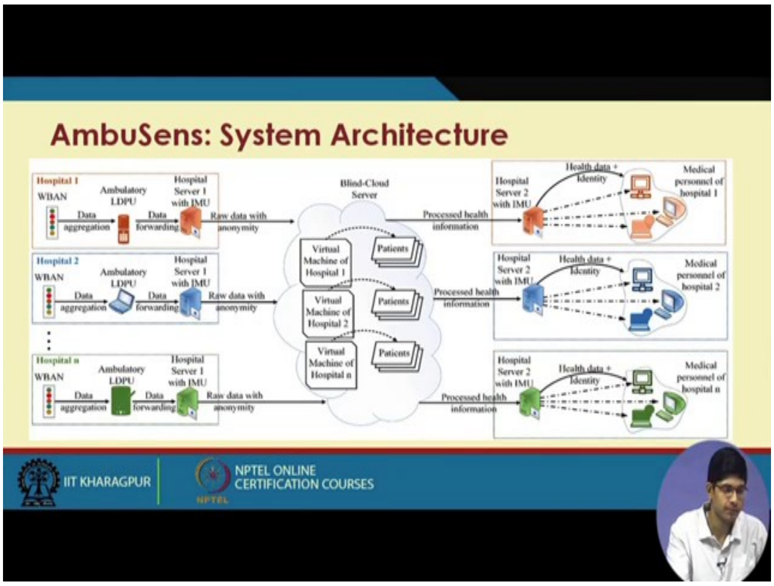
The AmbuSens system incorporates a novel identity masking module which suppresses the part of a patient's identity before sending it to the cloud so that cloud computation and analytics can be carried out on a incomplete data set clear by preserving the patients identity.

(Refer Slide Time: 24:19)



As is evident from this figure as we increase the number of clients the mean delay remains constant thus leading credence to the scalability of the system. The AmbuSens project also incorporates a web based interface for doctors and paramedics for using the different functionalities of the system. Functionalities may include features such as we have developed provisions for recording the medical data we have developed a feedback system so that doctors can give their feedback and their skills skilled expertise to the paramedics who were travelling in the ambulance, also it includes advanced data visualization graphing tools for better understanding of the data it also helps in spotting patterns and trends in the real life data streams that are coming.

(Refer Slide Time: 25:15)

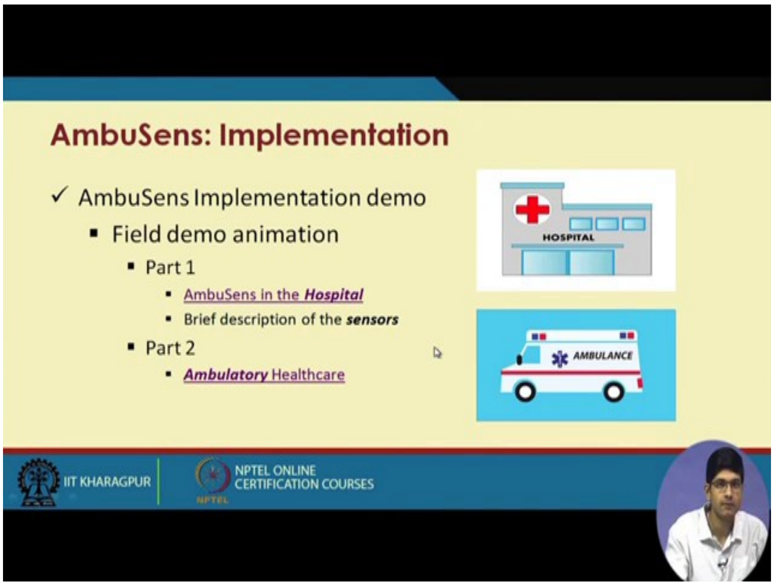


Now, as I have already explained the different modules of the AmbuSens system work together to achieve real-time monitoring. Here first we have the wireless body area networks which are formed by parallel sensing devices which capture the medical data the health parameters which indicate the condition of the patient and using communication technologies such as Bluetooth and Zigbee.

The data is sent to a local data processing unit where it is aggregated and filtering algorithms and voice removal techniques may be used and further using communication technology cellular technology such as LT or wireless land technologies such as IEEE 802.11. We forward the data to a server hospital server which contains a identity masking unit which suppresses the part of the patients identity as discussed. And the raw data is now anonymous and before it is sent to the cloud the data in the cloud apart from being anonymous with respect to a patient's identity also is stored in different virtual machines which are unique for each hospital thus extending the isolation between the data and preserving the privacy further.

The data is stored in the cloud and analytics may also be carried out and on demand that process held data is sent to a second server at the hospital where we have the reverse identity masking unit identity management unit which helps in getting back the original data set complete data set and from there the paramedics the doctors and all the caregivers who are authorized to access the data can view the data through the web interface in graphical format for analysis and prognosis.

(Refer Slide Time: 27:40)



Now we come to an implementation and demonstration of the AmbuSens system. Unfortunately due to privacy concerns we cannot actually show you the use of the AmbuSens system on a real patient instead we will prevent an animation which shows the use of at the AmbuSens system into different scenarios. Part one details the use of the system in a static hospital scenario and it also includes a brief description of the sensors. Part two includes the use of the AmbuSens system in a typical ambulatory care scenario.

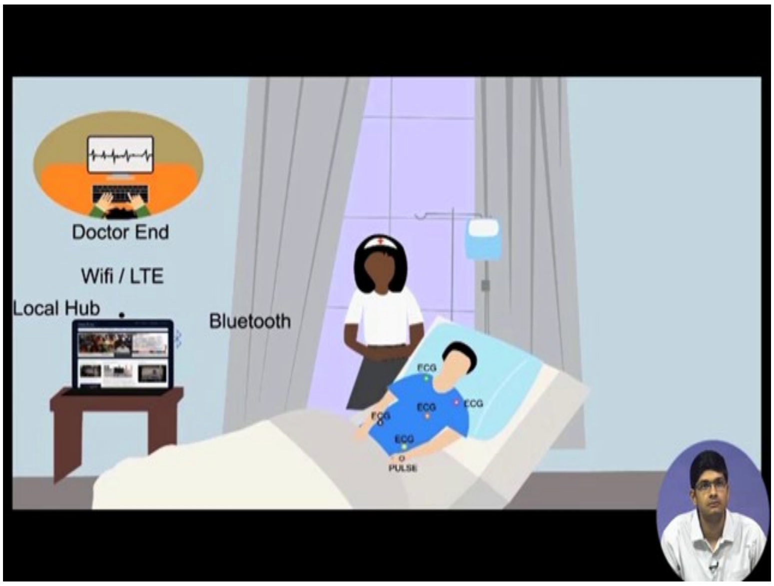
So, here we consider a typical scenario in which the developed IoT based healthcare system namely AmbuSens may be used. Here we consider a patient lying on the hospital bed with a nurse or paramedic attending him or her. Let us consider a situation when the patient needs to be monitored in real-time by doctor who is at some remote place. Now this situation may arise due to a couple of reasons a, this situation may be a rural hospital, but there is a lack of specialized doctors capable upliftment. Particular affliction which is aiming the patient it may also be the case that with a doctor who is regularly attending to the patient maybe on leave and some emergency regarding the status of the patient may require remote monitoring.

To enable remote ubiquitous monitoring you may use the AmbuSens system as follows. The nurse or paramedic who is attending to the patient is required to place the wireless sensor divisors to the patient body as shown. The wireless sensors used can be of many heterogeneous types and are application specific depending on the types of physiological parameters that we may want to monitor. For example, here in the AmbuSens system we have the provision for measuring the pulse rate, the electrocardiogram or ECG and also the temperature of the patient.

For the sake of probity here we display only two types of sensors the heart rate and a ECG sensors. The heart rate sensor in use is based on the principle of photoplethysmogram or PPG. This principle uses light emitting diodes to illuminate the skin each cardiac cycle there is a difference in the pressure of blood flow so the arteries in the subcutaneous tissue or skin which leads to a difference in light absorption. These in turn is encoded and can be used to calculate the heart rate of the patient.

Here we also measure electrocardiogram or ECG of the patient. Now electrocardiogram records that electrical activity generated by heart muscle depolarization which propagate in pulse rating electrical waves versus skin. Although the amount of electricity is in fact very small it is in microvolts it can be picked up quite reliably with ECG electrodes attached to the skin as shown in the diagram these heterogeneous sensors together make up a sensing layer or the IoT architecture.

(Refer Slide Time: 31:34)



The sensor nodes treated on the patient’s body and equipped to the Bluetooth transceiver unit which is used to send the sends data to a local hub for data acquisition and preliminary process here we have used a laptop as a local hub. So, preliminary processing includes calibration of the data in proper format for further processing and filtering to remove excess noise generated calibration includes algorithms to convert EPG reading obtained from the heart rate sensor intellectual heart rate readings etcetera. The local hub that is the laptop is capable of receiving the data through Bluetooth and then it transmits the data using either wireless LAN, Wi-Fi or cellular technologies such as 3G or LTE to the AmbuSens servers.

All of this is done while the sensors are active and data sensing is going on to achieve real-time data aggregation and processing. Local hub performs part of the activities of the aggregation and processing layer of the IoT architecture. At that remote end the doctor is capable of accessing the real-time data by logging in to the AmbuSens servers and the web interface at AmbuSens.iitkgp.ac.in using authorized credentials and using the data visualization tools which are available on the website, he or she is able to get a graphical representation of the real-time data captured from the patient.

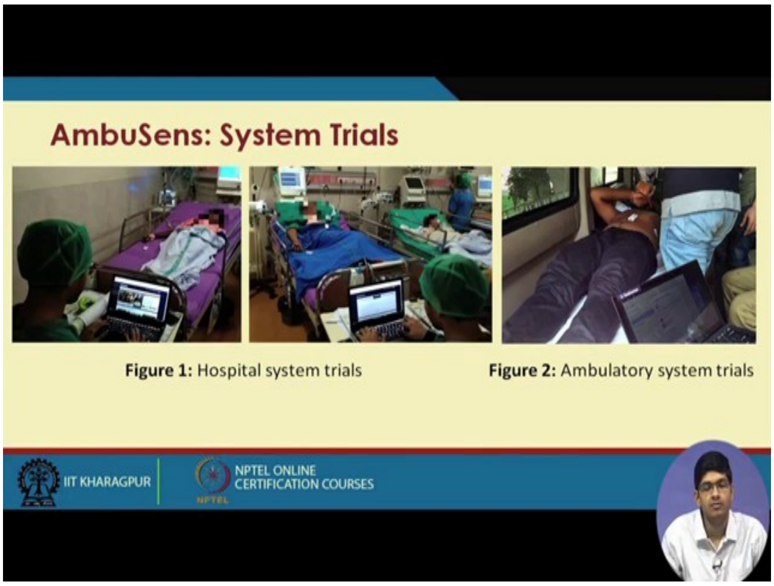
Here we consider another scenario which is particularly well suited for the application of the AmbuSens system that of mobile ambulatory health monitoring. Let us consider the case of a patient we transported by an ambulance to another far away healthcare facility. This situation is quite common especially in the case of a rural or some urban hospitals where the patient which quite often referred to a specialized clinics of the city. Inside the ambulance we see the patient lying on his stretcher with a paramedic accompany him or her typically in this scenarios the patients health condition while in transit is not monitored by doctors at either end.

The doctors at the city clinic are inform about the status of the patient when we first commences his journey, but while in transit the patient's condition may have change the significantly thus doctors are be prepared to give the best possible care to the patient this is where the ambulance system comes into the picture. As we had seen in the hospital scenario the paramedic attaches the wireless sensor devices to the patient body. The wireless nature of the sensor devises make them easily variable and makes his easy for the patient to be moved to and from the ambulance.

The sensor communicate with the local hub using Bluetooth technology. A local hub in this case has been replaced (Refer Time: 34:46) and enabled android device, the rationally behind this is to provide mobility support at ubiquitous connectivity. The mobile nature of the environment introduces more noise into the system whose require robust noise filtering mechanisms to make the stringent reliability constraint in post by medical data. This part is also handled by the local hub thus the local hub provides functionalities common to both are aggregation then the processing layer of the IoT architecture. While the ambulance is in transit real-time sensor data is streamed using the LTE connection to the AmbuSen server the doctors in the both hence that if at the referee, end the referred can login to the AmbuSens website that is AmbuSens.iitkgp.ac.in and access there is data in real-time to monitor the status of the patient into probable real-time feedback to the paramedic.

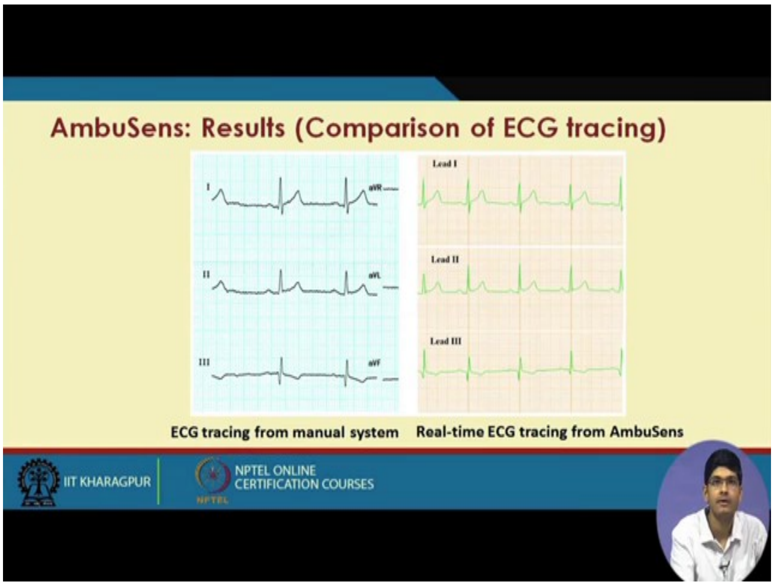
Thus we present the AmbuSen system as use case of IoT in healthcare where we use the different aspects of a internet of things such as wireless sensors heterogeneous communication technologies to solve some of the challenges present in modern healthcare. To conclude we encourage the viewers to think about what particular challenges the mobility can introduce into this system and how we may go invoke solving them.

(Refer Slide Time: 36:22)



The two scenarios of deployment shown in the animation that systems were tried out in those two scenarios - figure one shows the trials in the hospital scenario, and figure two shows the trials in the ambulatory scenario. Both trials were carried out successfully and through a number of iterations we have successfully calibrated and tested out the system, the results are shown in the next slide.

(Refer Slide Time: 36:52)



The figure on the left is that of a ECG tracing from a traditional wired ECG system and on the right you can see the real-time trace generated from the AmbuSens system comparison between the two traces shows the validity of the system.

Thus, in conclusion IoT based technologies the sensing and the communication technologies of the internet of things may be used to enhance the existing healthcare system in our country and I hope that this example inspires you to develop IoT based healthcare systems on your own.

Thank you for listening.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

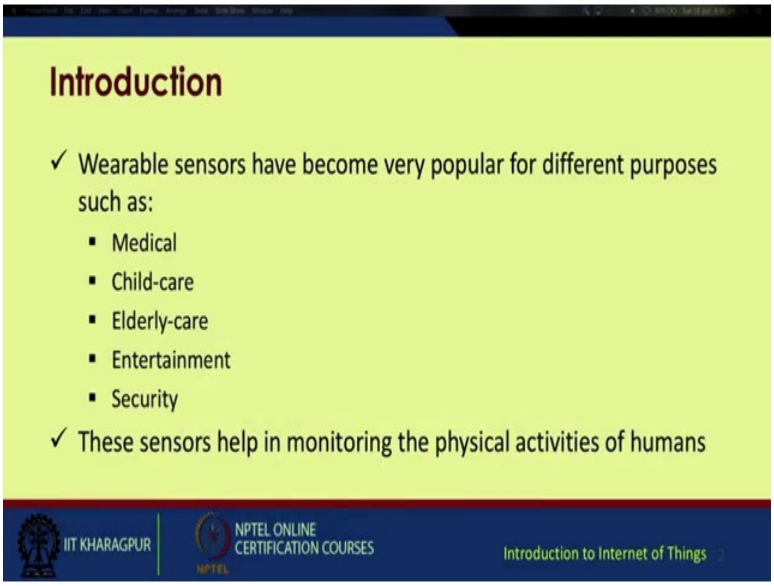
Lecture – 59
Activity Monitoring (Case Study) – I

Hello, in this lecture this again will be a two part lecture on activity monitoring, the first part will focus on the basics of activity monitoring like what we are going to do, why is it required and what is the necessity for activity monitoring in day to day life or maybe in special scenarios and finally, in the second part of this lecture which is mainly a case study, will give a demonstration has small demonstration of a simple network based data aggregator which can be used for monitoring various activities. So, the data is being generated from a smartphone and being sent to a remote server over the network. So, we have developed a small app which generates or captures the various human activities not actually activities, it captures the various sensor behaviour during human activities.

Suppose a person is walking running lying down is talking maybe person is fighting or had an accident and so on and the sensor values keep on changing the specially the smartphone sensors since we are talking about or the case study we are talking about smartphone sensors. So, we have taken the inbuilt sensors in the smartphone. So, those sensorial values are transmitted over the network to remote server, where they can be used for multitude of applications ranging from normal activity monitoring fall detection you can even use a offline non smartphone sensor like a standard accelerometer or Imo based sensors integrated to a small processer board, and the same operation can be performed for those sensors also.

So, these things this non-smartphone based activity monitors, they have been given the common name wearables. So, you must have heard about wearables, you have fitbits activity trackers it is in the form of a small watch inside it is thinner and tinier then a watch, you just charge it wear it and go about your daily activities.

(Refer Slide Time: 02:43)



So, these are a few basic ideas will be discussing in this case study. So, these wearable sensors have nowadays become very popular. This has been due to multiple reasons first and foremost they are very efficient, second they are low power consuming, third they generate reliable data so, that your activities can be accurately tracked. So, they have found many applications in various fields such as medical field childcare elderly care entertainment industry security and so on. So, these sensors help in monitoring the physical activities of human; and your physical activities not only restricts to daily activities. So, people can say if your monitoring my activities you can track what I am doing. So, I am not comfortable with sharing those kind of data over the network.

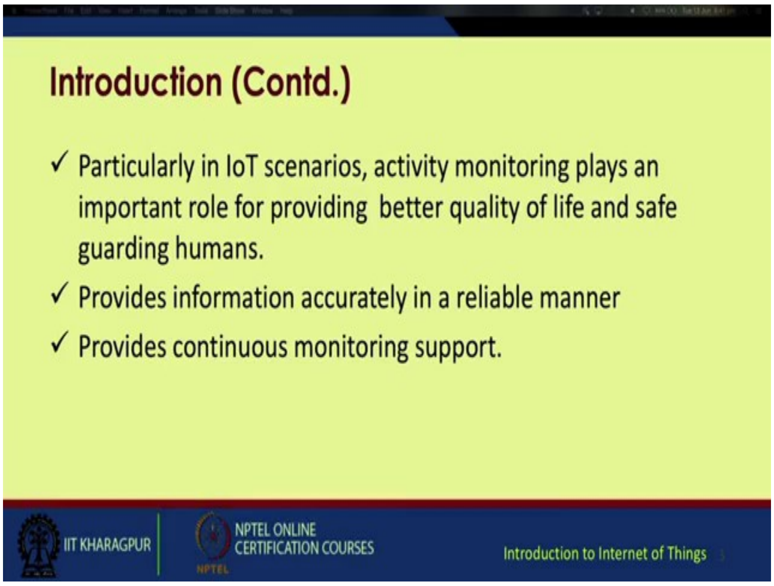
So, yes there are various issues regarding privacy regarding security of data, but we would not be dealing with those issues here. So, one by one let us just go through the basics like in medical, childcare, elderly care, entertainment security even military what are the applications what are the implications of using activity recognition. So, generally in medical field imagine a patient is hospitalized and his or her activities need to be monitored, suppose you have a very fragile patient he needs to go to the washroom to relieve himself or herself, and while doing so, the patient falls down. So, normally it may be a while before someone finds that patient in a foreign state. So, to avoid this kind of injury or this duration after falling down. So this recovery duration can be massively reduced by using activity trackers. Suppose the patients are made to wear bracelets embedded with small activity trackers, which are train to detect fall in patients or maybe they detect the changes in biomedical parameters like your pulse rate heartbeat and so on. So, these are now available in the market and collectively their called wearables, you have smart watches with activity trackers you have standalone activity trackers and so on.

So, in the medical field this can be very important for monitoring patients in child care if your child is playing on the streets if your child is going to school, you can monitor your childs activities if your child falls down or there has been accident, automatically the system will alert the parent that child has met with an injury or an accident. Then as we have covered earlier it for elderly care it is almost the same as the medical usage of wearables. So, imagine elderly people in your home wearing small activity trackers the best part is these are very small.

So, people hardly notice there even there. So, an additionally they are not very power hungry. So, once in a while you charge it may be in three days four days you charge it and it will keep on going. So, in elderly care you are you can use these activity monitoring applications. In the entertainment industry, you must have seen various documentary documentaries or you must have seen those action movies where the protagonist performs multiple and dangerous stunts. So, you must have realized most of these are something which is known as CGI. So, in CGI actually you stand in front of a green screen wearing various activity monitors in front of cameras, which are used to track your activities and you have certain highlighted points or markers on your body and these will be used for generating what activity you are performaning and so, that this can be reliably translated in terms of a movie scene with changing backgrounds maybe you see some dinosaurs running around, you after your CGI scripting and editing has been done maybe you are jumping of a bridge you are jumping of a plane and so on.

So, this is from the entertainment industry in security also you can have activity monitors monitoring where you are going what exactly you are doing maybe you have no person zone, and if someone is entering that zone or maybe have activity sensors installed which you do not want in our area you do not want anyone to access, and suddenly in the middle of the night some of the sensors go off. So, you hit upon this idea that since no one is supposed to be in that area and suddenly many activity sensors are turning on. So, there may be a case of breach of that security. So, this is maybe one of the potential applications of activity monitors in the domain of security.

(Refer Slide Time: 08:45)



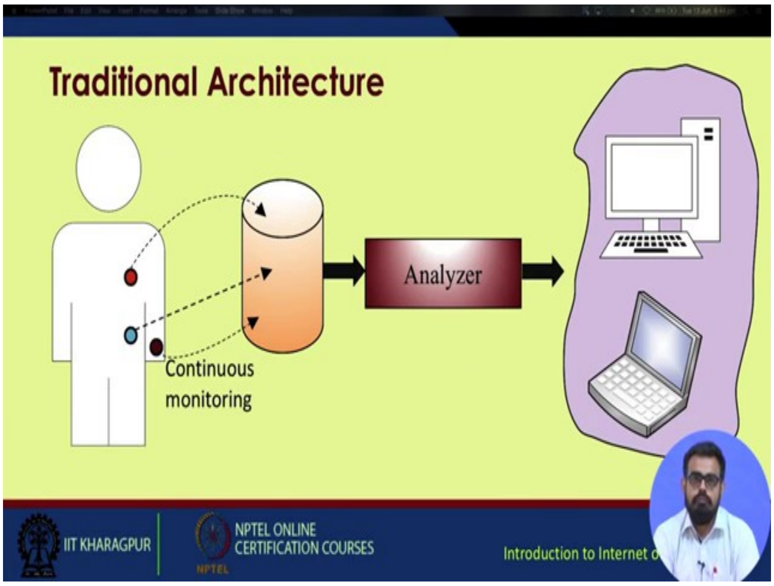
So, now coming back to the IoT based scenarios, this activity monitor monitoring plays a very important role and since mainly if you keep the security aspects the entertainment aspects aside normal medical and human implications in day to day life they provide for a better quality of life, they provide and they promise for a better quality of life and they safeguard the humans against various accidents. By promising and providing quicker response quicker emergency action and other system.

Now suppose while driving a person is wearing an activity monitor which normally under emergency normally alerts some emergency numbers as well as his family members. So, the person meets with an accident on the road, and there is a sudden change in the persons activity since let us suppose the person is only wearing an accelerometer on his wrist, and within normal limits the accelerometer is giving two units of reading and the impact of with the impact of the accident these two units will be translated to 100 units.

So, that would be a massive jump in the persons daily activities so; that means, the person has received a big physical shock. So, that the sensor is giving such an abnormal reading. So, in this way you can train your system both on the device as well as offline or online on the network, to generate abnormal activities sometimes it may be due to sensor malfunction sometimes it may be due to electrical disturbance, but sometimes it maybe even due to some serious life threatening situations. So, once this abnormal activity has been registered maybe some emergency numbers are alerted, family members are alerted and they are notified of the persons location the present location or the last location from which the alert was generated, and immediately rescue teams reach that person and eventually the person will survive.

May there are high chances that the person may survive. So, another thing is to provide information accurately and in a very reliable manner, and you need to provide a continuous monitoring support while considering activity monitor.

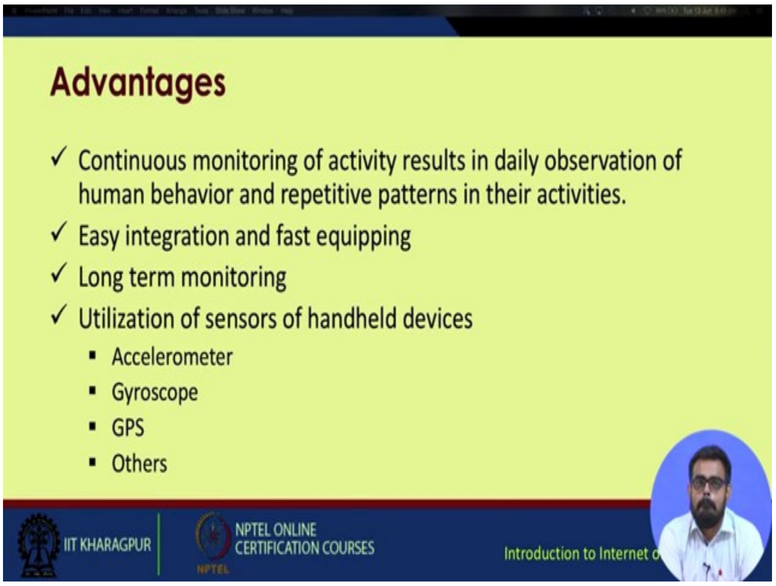
(Refer Slide Time: 11:26)



So, typical architectures deal with suppose you have this person and he is equipped with multiple wearables, one is tracking the heartbeat, one is tracking the body temperature, one is tracking the activity on the wrist and all this data is being forwarded maybe to a remote router or a network server, and then an analyzer analyses the activities and instead of transmitting the raw data, the analyzer transmits the analyzed activities to various connected stations that may be a home computer to which the family members are keeping track of view, that maybe a laptop or a mobile computer or even a cloud or maybe your medical doctors or consultants are keeping track of your activities.

So, this is a online base model, maybe for offline based models you can have all these things on a single wrist band in a small minute size, and it is doing all the processing offline that is within the device itself. So, there may be certain disadvantages of these and the applications may be restricted, but yes suppose you are going for jogging and you can using these offline models like every calculation and everything is being done on the device itself, you can keep track of your heart rate and it will give you an analysis whether you need to slow down or need to speeded up during your jogging and there are multiple such applications of activity monitoring.

(Refer Slide Time: 13:19)



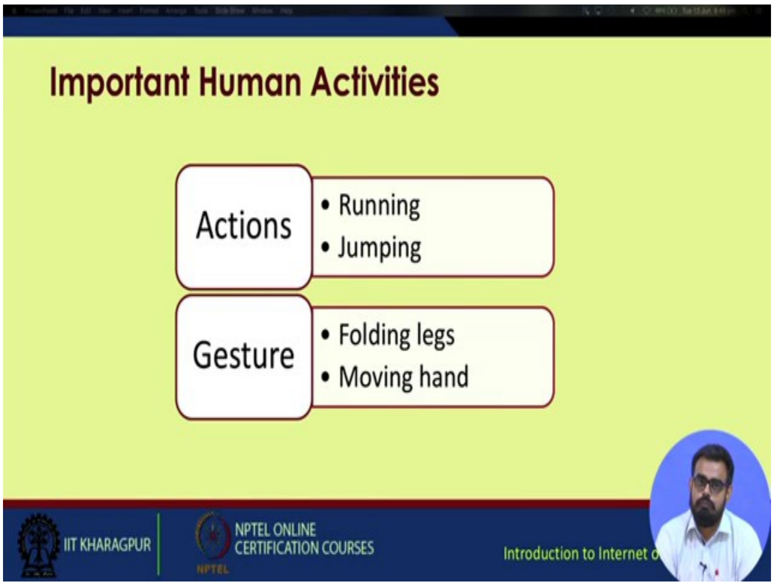
So, they inherently have certain advantages first is your continuous monitoring of activity will result in daily observation of human behavior, and repetitive patterns in the activities.

So, prior to generalizing some activities, your walking pattern, your running pattern the way you sit way you stand the your basic body language, varies for every person. So, that may vary due to height that may vary due to weight that may vary due to some previous injury some present injury and there are multiple reasons, while there may be variations. So, you need continuous monitoring and continuous training of the system to generate reliable results and this will also generate repetitive pattern. Suppose if you are going for normal activities like running, walking, jogging maybe driving sitting lying. So, they have clear cut markers they can be easily applied to, but what if you have some special activities you need to take care of like when you are lifting your left leg when you are lifting your right leg, you need to distinguish between these kind of minute activities you need to find in your system, in this can be only done through collection of data over a long period of time from individual subjects.

Now, another advantage is the easy integration of these sensors and the fast equip equipping time of persons with these sensors. Then you have long term monitoring available since these are very low power consuming you can keep on monitoring the activities for days at an end, then using normal sensors and basic handle devices you can build up the system which can monitor activities, you can opt for either smartphones or you can go for accelerometers attached to a basic processor and maybe a Wi-Fi radio or you can go for gyroscopes, which gives the orientation readings you have GPS and you can have multiple sensors, you can keep on increasing the sensors, but at the end the more the sensors you are increasing the more power hungry your device becomes, the more costly your device becomes and more volume of data it will generate.

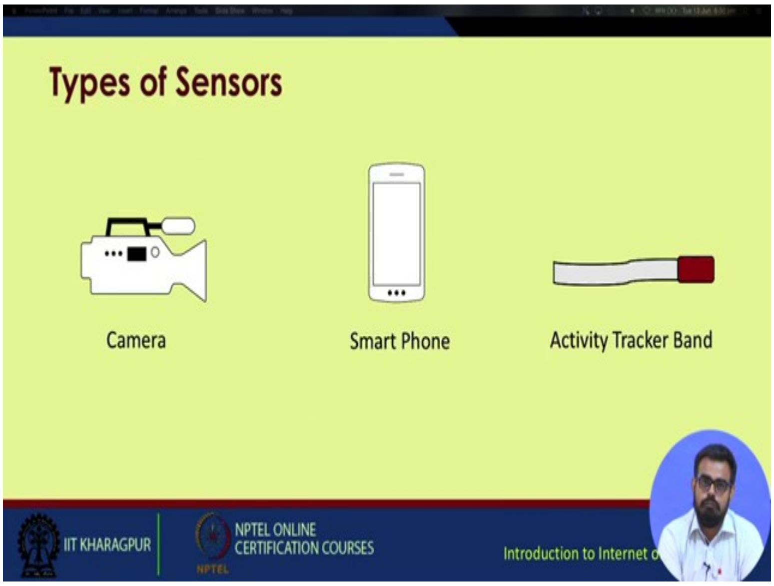
So, these are some of the plus and minus points of using activity monitoring, using sensors. So, mainly you need to restrict the number of sensors you go on including on a variable so, that it is lightweight, it is portable and it is less power hungry.

(Refer Slide Time: 16:27)



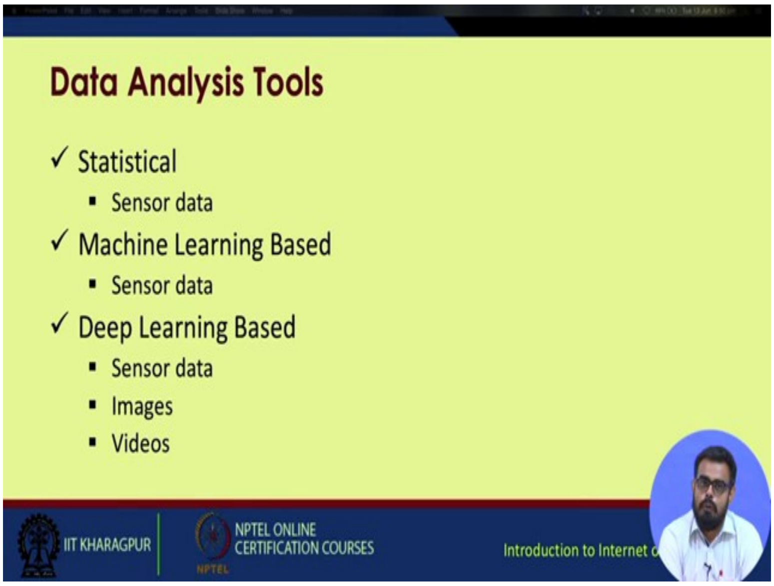
So, some of the basic human activities which these market available devices do are they can distinguish, actions they can distinguish gestures like for actions they can distinguish between running jumping or whether a person is lying down or sitting, and what gestures you can have if a person is holding his or her legs, if a person is moving his or her hands and suppose if a person is dancing right. So, that would be considered as an action, but there will be gestures involved also. So, maybe a person is dancing peacefully or a person is dancing aggressively, you can detect that using various gestures you can detect you can maybe predict the intent of a person using the gestures the person is providing maybe a person is threatening, someone maybe a person is trying to please someone and so on.

(Refer Slide Time: 17:31)



So, some basic sensors you have you can either go for video or image based monitoring of activities, which is very processing intensive then you can go for smartphone based activity monitors, you can involve a lot of sensors inbuilt sensors, but your phone has to generate a lot of data and then again you have this normal activity tracker band where the sensors unlimited and power is quite restricted.

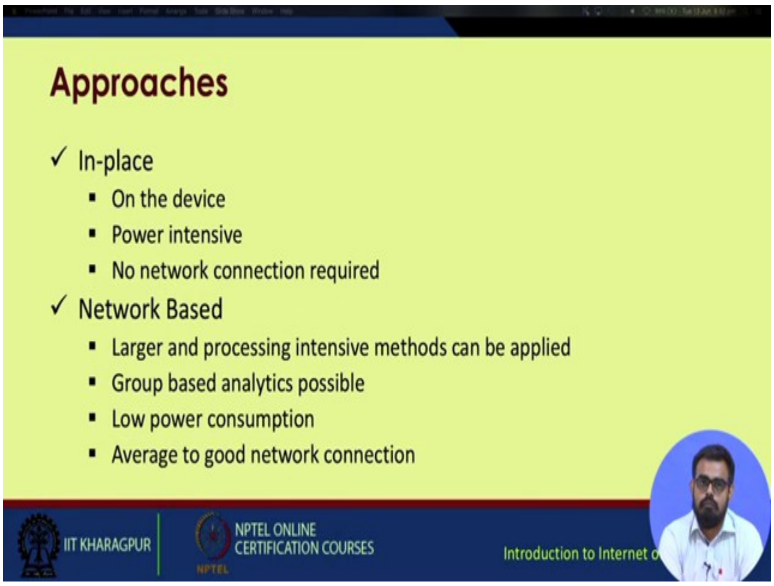
(Refer Slide Time: 18:06)



So, once your data is collected from the sensors be at the camera, be at the smartphone sensors, be at normal standalone sensors, what next? You have to find some means or methods to analyze these data. Generally these data are going to be very long there will be errors or let us say in statistical terms there will be outlets, that may be due to errors in the sensor reading that may be due to fluctuation in the sensor itself that may be due to some accidental minor accidental bumping of the sensor, suppose you are about to wear your activity tracker band and suddenly it falls off on the ground.

The person is standing still the person is fine, but the sensor falls off. So, that will record a major shock other alert in the activity monitoring system. So, these kinds of falls predictions can be avoided and we will name them as out layers, that is beyond the normal statistical behaviour of the data. So, you have statistical analysis of the data being generated, generally they work on sensor data then you have machine learning based analysis again they work on sensor data, maybe machine learning, with image processing you can use for analyzing video and image data then you have this deep learning based approaches you can use normal sensor data you can use image data you can also go for video based data.

(Refer Slide Time: 19:52)



So, somewhere sometime in the previous slides I have already discussed it, but mainly your activity monitoring can be divided into two parts one is in place the other is network base. So, I am calling the activity monitoring or the processing of data on the device itself as an in place approach. So, your monitoring is done on the device, since you are monitoring your diagnosing the activities on the device itself will need a processor, the processor has to process the sensor data and has to generate some alert. So, it is definitely going to be power hungry or power intensive, and generally no network connection is required, but yes you can obviously, opt for network connections. So, even if you go for network based in place devices, there will be an unnecessary wastage of additional power.

Next is your network based system. So, these are mainly aimed at processing larger and processing intensive methods such as deep learning tasks, computer vision based task, machine learning based task and so on. Group based analytics is possible suppose you and your group of 20 friends are out on a hike, maybe on the hillside or somewhere of terrain. So, suddenly one or two members start lagging behind. So, since you are not aware in that rough terrains since you are yourself very tired, but you are not aware about your friend's position. So, your activity tracker will tell your group that you are group is moving at this average velocity whereas, two units or two persons from this group are lagging behind. So, maybe they are facing some hardships or they are maybe facing some medical condition and need to be looked into.

So, we call this group based analytics. So, in this one network based approach you can go for group based analytics then; obviously, most of the processing and data is off loaded to a server and only you have a wireless radio and a sensor on your body. So, this will be low power consuming and additionally you will required an average to good network connection maintain with the server to which you are sending your data for activity monitoring. So, those are different approaches. So, I hope for this case study the basic importance of activity monitoring has been established, in the next part will give a demonstration of how we are using smartphone base sensors and connecting it to a network and visualizing it ok.

Thank you.

Introduction to Internet of Things
Prof. Sudip Misra
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 60
Activity Monitoring (Case Study) – II

Hello in this second part of the case study on activity monitoring, we will be going through a brief demonstration of a Smartphone based activity monitoring system. So, it is a very basic set up; that means, we have a Smartphone with us.

(Refer Slide Time: 00:38)

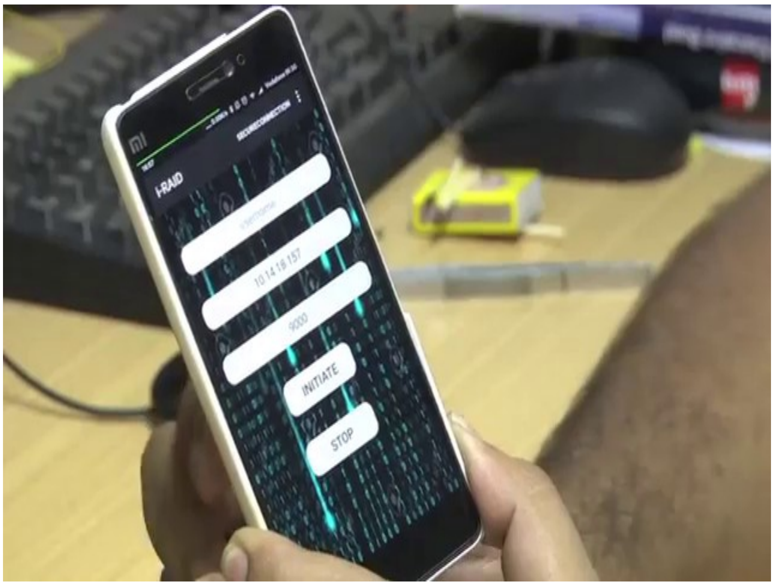
We have a remote server and we have a network. Now nowadays Smartphone's are as good as computers, laptops, PCs. So, and in fact, in some cases they are even more powerful than traditional PCs. So, what we are planning on doing is since everyone carries a Smartphone nowadays, almost everyone is using a Smartphone nowadays. So, we are going to use the inbuilt sensors and we are going to try to transmit the data from the Smartphone sensors over the network to a remote server, on which we can visualize the incoming data. So, for this part we have not explored it that much, but judging from the preliminary successes, we predict this has a huge potential and if properly worked upon this can be easily integrated with standard or traditional IoT based technologies; even in smart homes, smart offices, smart buildings transportation and everything. So, your decision making what we are proposing, you do the decision making at the server end we just transmitted data from the Smartphone over the network to the remote server.

Now, before beginning I would like to just brush up on a few things. So, I hope you all know that your smart phones are built in with certain sensors, more specifically you have your accelerometers which are in every Smartphone higher end Smartphone's will also have compass and a gyroscope. So, compass or magnetometer it will give you magnetic readings with respect to the true north, and your gyroscope will give you the orientation of your Smartphone. So, for example, your accelerometer will give you the readings of accelerations. So, suppose in case of certain jerks like this Smartphone is traveling with you. So, in case of certain jerks this accelerometer will generate higher impulse response.

In case of Gyroscope if your Smartphone's orientation changes even if there is a tilt or angle or any such other change, the gyroscope will record this and your magnetometer which will be responsible for locating the direction, you are moving with respect to the knot.

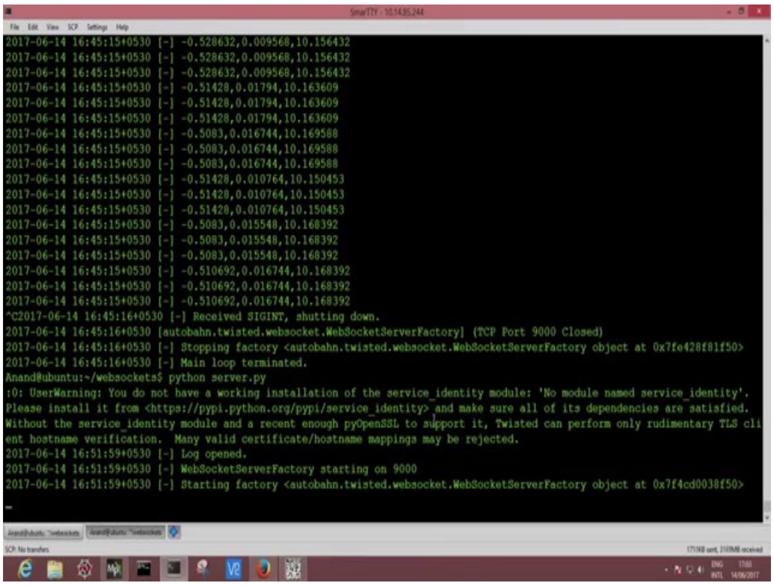
And additionally almost all Smartphone's are equipped with GPS. So, you have four very basic sensors found in almost all Smartphone's, your accelerometer gyroscope magnetometer and the GPS. So using a combination of these four sensors and maybe the internal clock of the sensors, internal clock of your Smartphone and the network attaching capability. That means, since your Smartphone has already been enabled with a cellular connection or a Wi-Fi connection. So, you can choose either any of these two connections to transmit your data over the network to a remote location. So, this was about the Smartphone's, we are not going into the details how we are transmitting the data which network we are choosing for this for our demonstration purpose we are choosing a local Wi-Fi network over which the server is also connected and the server is remotely located, I will be using my desktop to access that server remotely and I will be trying to log in to my remote server via an android app so that the data can be transmitted directly.

(Refer Slide Time: 04:48)



So, I have my android app I have connected it to the Wi-Fi network, I open this app you just named it I-RAID. So, it has got three fields one is username, one is the IP address of the server and one is the port. So, if you remember that those lectures on IoT with raspberry pi. So, we were also using 2 basic things one was the IP address another was the port. So, over here also we are using these 2 the IP of the server AND the port, onto which your data will be uploaded and we have got two buttons one is initiate and one is stop.

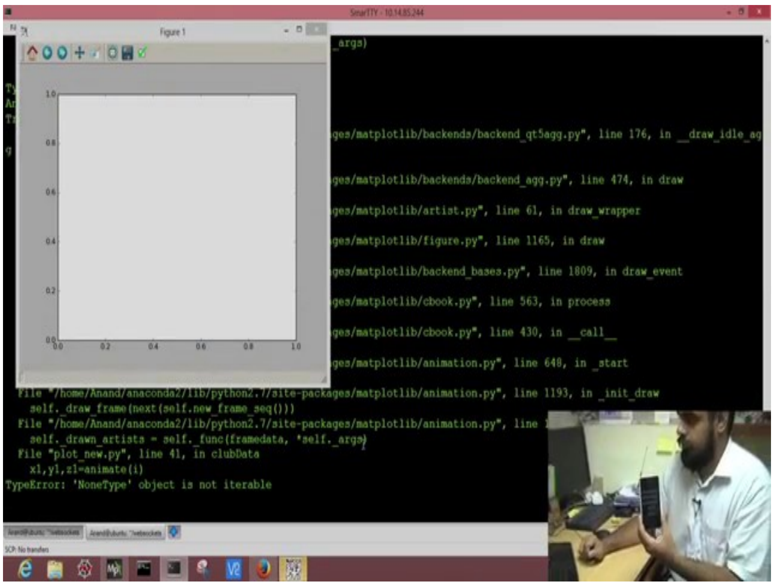
(Refer Slide Time: 05:40)



So, over at the server end I will start my python server. So, this web server was made on a library function python library function for web sockets, it is known as auto ban. And using this auto ban and the twisted framework we created this web socket server, and similarly on this android phone the android programming for this application was done using the same manner. So, I give my server IP address as and the port name is same I will provide some username right. So, whenever I initiate my connection first you look the server is actually expecting connections.

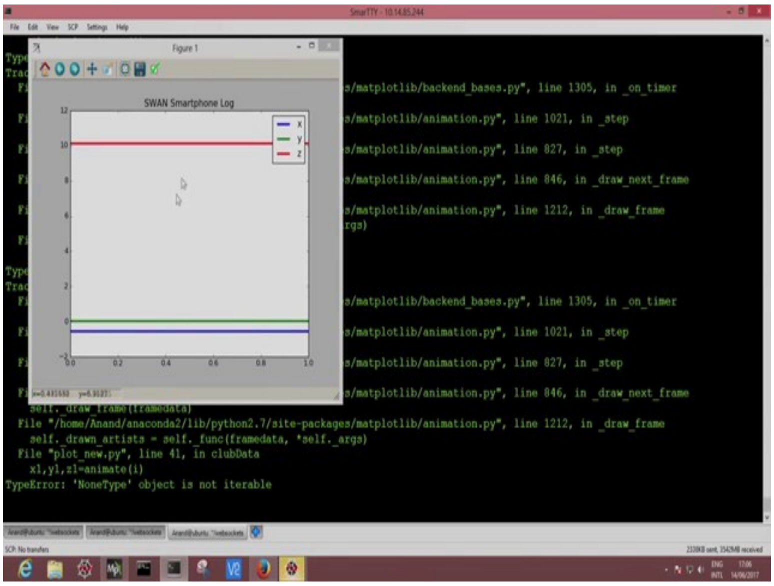
So, whenever I initiate my connection on the Smartphone text message pops up connected, and if you focus on the server end you will see that data is being logged onto the server. So, it has got few fields first is the date field on which the data is being collected, next is the time then third fields we have kept intentionally blank, and for this demonstration purpose we are only logging the accelerometer values. So, if you see I give it jerky moments, the values abruptly change on the server end additionally we open another link to the server and we open a plotting function. So, on one thread the data is being uploaded over the network from the Smartphone, remotely located Smartphone on the other thread we are running a plotting functions.

(Refer Slide Time: 07:44)



So, if you see on the screen now a plotting window pops up. So, since nothing is being plotted here, I might need to change some parameters. So, now, my data is being continuously logged on to the server. So, this is my plotting function and in the plot program again you see these three lines these denote the accelerometer xy and z readings.

(Refer Slide Time: 08:54)



So, if you see if I move my Smartphone these lines go up and down. So, this we have not tried filtering this data you are trying to plot it as it is coming into the server, there has not been any delay element added to it nothing, just there all sensor values are being plotted.

So, one thing you can derive from this is suppose your Smartphone is kept on a level area. So, you see your x axis y axis are more or less on the same plane, nearby each other and the z, z axis gives a reading of ten. So, this basically signifies it is at certain distance from the ground right it is not at the zeroth position or the same as x and y axis. So, whenever I change my maybe I tilt my phone if you see on the screen the blue line goes up; that means, the x axis of the Smartphone changes right. Now whenever I tilt up the phone in this manner you see my z axis goes down. So, it is much more nearer to the ground whereas, my y axis goes up right. So, y-axis reading has changed. So, basic primary application which can be derived from this is maybe this can be used as a level tester to check whether your levels are correct or not, whether you are maybe you are supposed to put everything for parallel to the ground, but you needs some kind of level testing device which can tell you the measurements.

So, this may be one potential application other potential applications may include using these sensors and combining them with various machine learning algorithms. So, for that you need a prior or historical data on which your various machine learning algorithms will be trained. So, for supervised learning, on the basis of that you can go for activity detection also this is only just monitoring of activities we are not giving out any kind of intelligence whether this phone is or not whether a person holding this phone is sitting down or standing upright or lying down.

So, those kinds of things can be additionally added to this framework to make it more robust more reliable and much more functional. So, one is basic activity monitoring another application can be which can be very useful is fall detection; like we discussed in the previous lecture for medical patient monitoring you need fall detection approaches you need emergency alert approaches and so on. So, maybe using this you can detect a fall and after a fall has been detected various emergency services can be alerted you can even provide a feedback from the server after a fall has been detected, the server will ask the phone user whether you have actually fallen or not. So, that may be miscommunication from the sensor or that may have been due to an accidental jerk or sudden bump. So, if the user is in a condition to respond then it is fine. So, user says no if the user is not in the condition to respond. So, maybe something has gone wrong and emergency services hospitals relatives can be alerted.

So, these are some of the basic implications and applications which can be developed using this framework in this approach. So, it is actually limited by the by the users imagination what else can be done. So, I hope this has been useful to you.

Thank you.

THIS BOOK IS NOT FOR SALE
NOR COMMERCIAL USE

PH: (044) 2257 5905(08)

nptel.ac.in

swayam.gov.in