

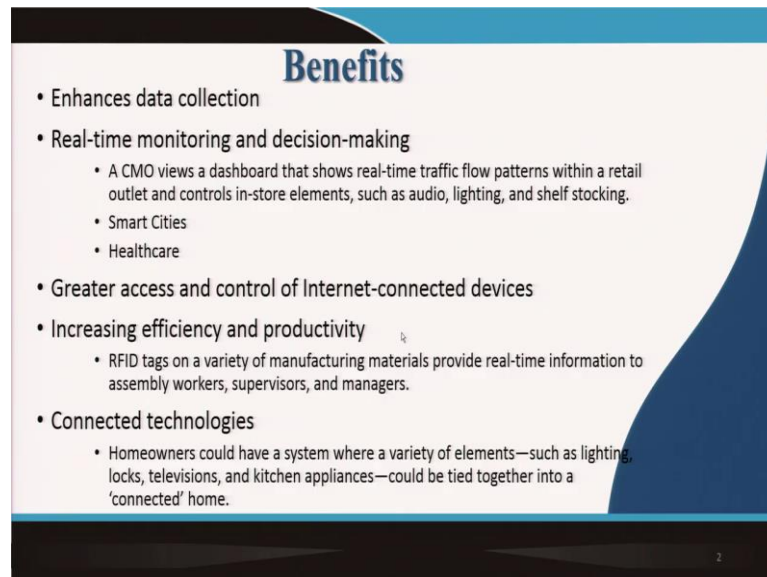
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module – 09
Emerging Technologies
Lecture – 44
Internet of Things Part – III

Hello and welcome back to the fifth lecture on ‘Emerging Technologies’! So, we are continuing with ‘Internet of Things’; this is the third part. In the previous two lectures, we had spoken about what internet of things is all about, various applications of internet of things.

And we had also discussed technologies or rather the evolution of technologies with respect to the internet of things. So, today we will talk about the advantages and the disadvantages of internet of things.

(Refer Slide Time: 00:55)



Benefits

- Enhances data collection
- Real-time monitoring and decision-making
 - A CMO views a dashboard that shows real-time traffic flow patterns within a retail outlet and controls in-store elements, such as audio, lighting, and shelf stocking.
 - Smart Cities
 - Healthcare
- Greater access and control of Internet-connected devices
- Increasing efficiency and productivity
 - RFID tags on a variety of manufacturing materials provide real-time information to assembly workers, supervisors, and managers.
- Connected technologies
 - Homeowners could have a system where a variety of elements—such as lighting, locks, televisions, and kitchen appliances—could be tied together into a ‘connected’ home.

So, moving ahead to talk about the benefits, we will begin with the benefits the first benefit of internet of things is that it enhances data collection. So, we have seen that earlier prior to internet of things, there was a lot of problem with respect to data collection, because data was not available to that extent there was data, but it was not available to that extent.

We did not have so many technologies around us, we did not have so many applications around us, that would be sending out data continuously. But with the arrival of internet of things and with sensors which are plugged into certain devices or applications, which collect data on the fly constantly; data collection has become much easier than before.

Consider the example of healthcare technologies, wrist bands or say you know chips that are plugged into human body. And these chips continuously collect healthcare data regard respect to different parameters of human health and this data is being collected continuously 24-7. So, imagine the amount of data that is getting generated and that is getting collected and stored.

So, with the arrival of internet of things data collection has become much less challenging than it used to be before. If we consider the example of home automation system, there are so many gadgets at home and if these gadgets are actually you know a sensor is implemented one or more sensors are implemented, imagine the amount of data that gets collected on a daily basis.

So, arrival of internet of things has actually facilitated data collection in a big way. Moving on, real time monitoring and decision making. So, since the data is getting collected on the fly huge amount of data getting collected and stored lot of analysis or you know patterns can be found in the data.

You know real time monitoring of certain entities, say for example, in healthcare real time monitoring of a patient can be done, the health status of the patient and decision making can be made immediately. So, let us take some examples, a C M O a chief marketing officer in a retail store views a dashboard that shows real time traffic flow patterns within a retail outlet.

And controls so with the help of that dashboard and the data that is the real time data that is getting you know reflected in the dashboard, the C M O can actually control in store elements such as audio, lighting, shelf stocking based on a traffic pattern within the store and this happens on a real time basis.

Smart cities has a huge application you have seen the previous day; an example of how the traffic system has a you know in a smart city is enhanced by internet of things. So,

for example, if there is an accident at a certain point in time, the traffic the smart city system with the help of IOT will be able to monitor or alert a driver.

And the driver will be able to take a different alternative route. Also you know it is real time data analysis with respect to traffic in smart cities helps driverless cars, they can take automatic decisions; they can take real time decisions with the help of data that is coming in. Healthcare, in healthcare real time monitoring has a huge role to play.

So, for example, when data is collected in healthcare systems, you know if data of patients is getting collected on the fly constantly what can happen is, in case it is observed that the blood pressure of a patient has suddenly shot up or the sugar level has shot up.

So, the health care provider can take measures to monitor and take immediate action, such as hospitalization of the patient or prescribing a certain drug or several other measures to actually smoothen the healthcare service provider to the patient or also at the same time you know improve the quality of health care service, maybe prevent a certain disaster in terms of the health of the patient.

So, in all of these examples we see, that so in all of these examples we see that real time monitoring and decision making is enhanced to a large extent and is facilitated by internet of things. Third benefit is with respect to greater access and control of internet connected devices.

So, you know a real time application of this is seen in the case of smart homes. Wherein, even if the residents of the home are not within the home premises, they are outside at work or elsewhere. And they realize that you know, they have forgotten to switch off the lights or you know the water system the tap was turned on while they left the home.

They can from their from wherever they are they can control the entire home automation system to maybe turn off the light or turn off the water tap and so on. So, you really have lot of you know enhanced access and control of internet connected devices through internet of things.

Then we move ahead to increasing efficiency and productivity. This is a given, this is obvious that by implementing internet of things efficiency improvement and productivity

improvement takes a huge leap. So, for example, radio frequency identification tags on a variety of manufacturing materials provide real time information to assembly workers, supervisors and managers.

Based on which, they can avoid you know delays, bottlenecks and maybe accidents. Finally, connected technologies so homeowners could have a system where a variety of elements, such as lighting, locks, television, kitchen appliances all you know home elements could be tied together into a connected home.

So, this gives the residents a seamless connectivity across different devices through connected technologies and they can enjoy the leisure of a connected home within their own premises. So, here we have mentioned the benefits of internet of things and we have discussed all of them with examples.

(Refer Slide Time: 08:23)



Challenges in IoT

- Data Management: Storage and processing of zettabytes of data
- Data Ownership
- Data mining sophistication
 - In 2015 McKinsey Global Institute estimated that the United States needs 140,000 to 190,000 more workers with analytical skills and 1.5 million managers and analysts with analytical skills to make business decisions based on the analysis of big data.
- Privacy and Security
- Legal
- Chaos
- Internet Access

The slide also features a small video inset in the bottom right corner showing a woman with glasses and a pink top speaking.

So, moving on let us spend some time on the challenges and the challenges are not a deterrent here, because the challenges are to be overcome if we have to actually realize the benefit of internet of things. So, some of the challenges very obvious and very important challenges related to IOT are, with respect to data management.

So, we have seen that IOT facilitates a continuous connection collection of data and storage of data. So, beyond a point IOT does not remain limited to you know, a small

setup. As huge amount of data gets get collected every day on the fly, storage and processing of zeta bytes of data becomes a huge challenge.

So, ordinary traditional methods of storage and processing will not help. Advanced and more sophisticated technologies are required. So, that is a major challenge with respect to data management within the context of IOT s. Data ownership again you know a continuing on the same lines, since data gets generated.

You know, on the fly from multiple devices, say from human bodies, from social media, from home automation systems, smart cities there arises a problem of data ownership. So, who actually owns the data? If my healthcare health data is getting constantly you know transferred by means of IOT to certain hospitals or healthcare providers, who is the owner? Am I the owner of my data? Is the hospital the owner of the data or is the network manager or the I OT provider the owner of the data?

So, data ownership becomes a challenge and if there is data ownership challenge, then there could be issues you know other serious issues such as who manages the privacy of the data; who takes care of the security of the data; so on so on and so forth. So, data management and ownership both together could pose a challenge to the you know advancement and improvement of internet of things, if not handled in an appropriate manner.

Moving on, data mining sophistication - so, this is a statistic that was obtained which said that in 2015 McKinsey Global Institute estimated that in the U S, there is a need of 140,000 to 190,000 more workers with analytical skills; and around 1.5 million managers and analysts again with an analytical skills to make business decisions based on the analysis of big data. So, if so much amount of data is getting collected through internet of things, who actually would process the data?

So, this report the McKinsey report suggest that, there is a need of a huge you know talent of workers, who are actually huge you know some or pool of workers who actually have the talent or the skill to analyze big data. And big data technology is way different from the processing and storage of traditional technologies.

So, that much amount of skill is required going ahead. So, that might be a challenge, if we do not have that sufficient pool or resource of workers or you know skilled workers

who are skilled in the analysis and management of big data. So, that could be another challenge; now moving on to the more grave challenges of privacy and security.

Let us spend some time here. We also have three other challenges which we will take up subsequently, challenges legal challenges, chaos related challenges and internet access. The last one here, internet access is very obvious because internet of things entirely depends on internet connectivity.

So, a nation where internet connectivity is not up to the mark, there might be a huge challenge in the deployment and implementation of internet of things; so, going back to the privacy and security issue. Privacy challenges of internet of things - so, for a moment let us take a step back and talk, discuss the definition of privacy.

(Refer Slide Time: 12:47)

Privacy Challenges of IoT

"The right to be left alone and the right to be free of unreasonable personal intrusions, surveillance or interference from other individuals or organizations".

The slide features five images illustrating IoT privacy challenges: 1. A person wearing a wristband. 2. A map with a red pushpin. 3. A calculator and a document. 4. A smart home interior with IoT devices. 5. A hand holding a smartphone. A red text box at the bottom reads "Tradeoff between privacy and QoS". A small video inset in the bottom right shows a woman speaking.

So, privacy is the right to be left alone and the right to be free of unreasonable personal intrusions, surveillance or interference from other individuals or organizations. So, as the definition suggests let us talk about these five pictures or graphics that we see here. The first one says that you know, human being is wearing a certain wrist band through which is health care data gets transferred constantly.

The second one talks about your location so if you have chips inbuilt in your body or you know connected to you in some form, your locational data constantly can get transferred

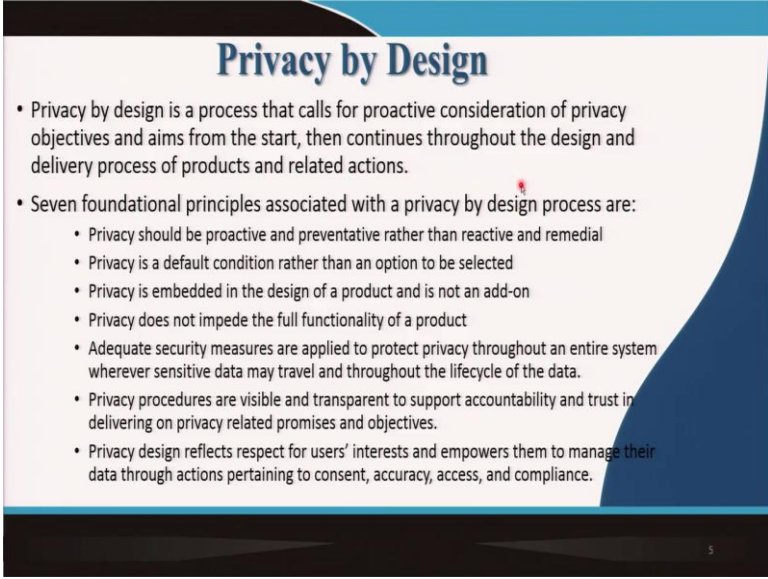
and can get monitored. Thirdly, with chips and with IOT implemented in your smart homes your financial information can be at stake so that could be another problem.

The last two here talk about home automation, wherein all your gadgets, all your household devices which are connected to the internet will be constantly sending out information, so a lot of your privacy could be at stake here. So, there is a huge you know maybe trade off or we can see a paradox here, as to which is more important, privacy or superior quality of service?

Because service providers, IOT service providers would want to gather more and more private information about you, in order to give you a better quality of service in every aspect. But, that also poses a huge risk of privacy, because as more of your data is getting transferred and transmitted over the internet; there is a huge challenge related to your privacy getting compromised.

So, what would you prefer? There that that is why it is mentioned that there is a trade off for there has to be a balance between the two, privacy and the quality of service that you receive.

(Refer Slide Time: 15:11)



Privacy by Design

- Privacy by design is a process that calls for proactive consideration of privacy objectives and aims from the start, then continues throughout the design and delivery process of products and related actions.
- Seven foundational principles associated with a privacy by design process are:
 - Privacy should be proactive and preventative rather than reactive and remedial
 - Privacy is a default condition rather than an option to be selected
 - Privacy is embedded in the design of a product and is not an add-on
 - Privacy does not impede the full functionality of a product
 - Adequate security measures are applied to protect privacy throughout an entire system wherever sensitive data may travel and throughout the lifecycle of the data.
 - Privacy procedures are visible and transparent to support accountability and trust in delivering on privacy related promises and objectives.
 - Privacy design reflects respect for users' interests and empowers them to manage their data through actions pertaining to consent, accuracy, access, and compliance.

Now, some of the measures which could be implemented at design level of IOT systems to take care of the privacy challenge, because privacy as you understand is a huge

challenge and there is an uproar across the entire world with respect to protection of privacy.

So, if privacy could be handled during the design level itself, you know measures could be taken to protect privacy breach or privacy of data being violated. Privacy by design is a process that calls for proactive consideration of privacy objectives and aims from the start, then continues throughout the design and delivery process of products and related actions.

So, from the beginning to the end privacy is given a lot of consideration while designing the IOT system. So, it is more of a proactive measure, rather than a reactive or remedial measure. So, there are 7 foundational principles associated with privacy by design process, we will quickly enumerate them.

So, privacy should be proactive and preventative, rather than reactive and remedial; we have just discussed this. Privacy is a default condition rather than an option to be selected. So, the option to select whether a customer would want to have additional privacy or not, should not be left to the customer all the time; the privacy option should be a default condition.

And if the customer wants less amount of privacy, that should that option should be left to the discretion of the customer rather than a privacy being left to the discretion or being left to the discretion of the customer. Thirdly, privacy is embedded in the design of the product and is not an add-on; so, we have just discussed this point as well, privacy.

So, fourthly privacy does not impede the full functionality of a product. So, this means that you know if you want to explore or exploit the end to end functionality of a product privacy should not be an impediment; and if privacy is an impediment many people would not be able to explore the complete functionality of the product.

Fifth adequate security measures are applied to protect privacy throughout an entire system, wherever sensitive data may travel and throughout the life cycle of data. So, along with privacy and in tandem with privacy comes the issue of security. So, adequate security measure should be implemented throughout the entire IOT system. Then, we talk about privacy procedures should be visible and transparent.

So, this is very important because if you want to have you know if you want your customers to trust your IOT system, privacy procedures should be visible to them and they should be transparent. So, what I mean by this is you know if your, I if your smart your wrist watch or your wrist band has certain privacy procedures, those procedures should be visible to the customer rather than being hidden somewhere.

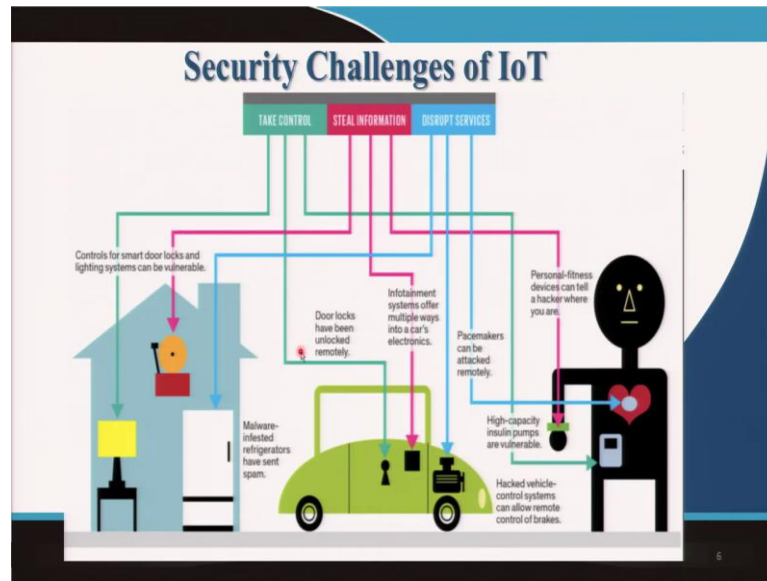
So, instead of being translucent or opaque or being hidden somewhere, they should be obvious and visible directly to the customer. So, that they can have you know more you know your system can have more accountability and would be able to engender human trust. So, privacy procedures being transparent and visible are of up utmost importance.

And lastly privacy design reflects respect for users interest and empowers them to manage their data, through actions pertaining to consent accuracy access and compliance. So, this actually means in short, you know if I were to explain this in brief, your customers should have the right to be able to have control over their privacy.

So, you should be you should take their consent before you want to collect their data, you should take their consent if you want to access and transfer their data and so on. So, if your customer does not you know is not willing you would rather not collect that data, because that may actually disrupt the entire concept of privacy by design.

So, these seven procedures, would in would you know holistically ensure that privacy is considered in the design of your entire IOT system and would facilitate, the you know seamless operation of your entire IOT system without privacy being an impediment.

(Refer Slide Time: 19:51)



Moving on, so we said that, in along with privacy security is also another major challenge so this diagram summarizes the security issues with respect to internet of things. So, if there are sensors inbuilt in different devices. So, here is a home automation system, a car and here there is a human body.

So, in if in all of these devices there are some sensors implemented, though you know any hacker or a malicious entity sitting outside could take control could steal information or could disrupt services. So, let us take some examples. If in a home automation system, a third party or a hacker with a malicious intention breaks into your system and takes control.

So, they cannot only enter your system they can also steal a lot of your, you know household you know property they can go and damage your entire system and they can wreak havoc into your house. So, taking control here creates a huge problem.

Again, if the malicious entity has the intention of stealing data they can again break into your house, they can break into your car and they can steal a lot of your confidential information. So, that is again a problem. The last one is the worst of all. So, if the malicious entity actually wants to harm you physically, they can also do that.

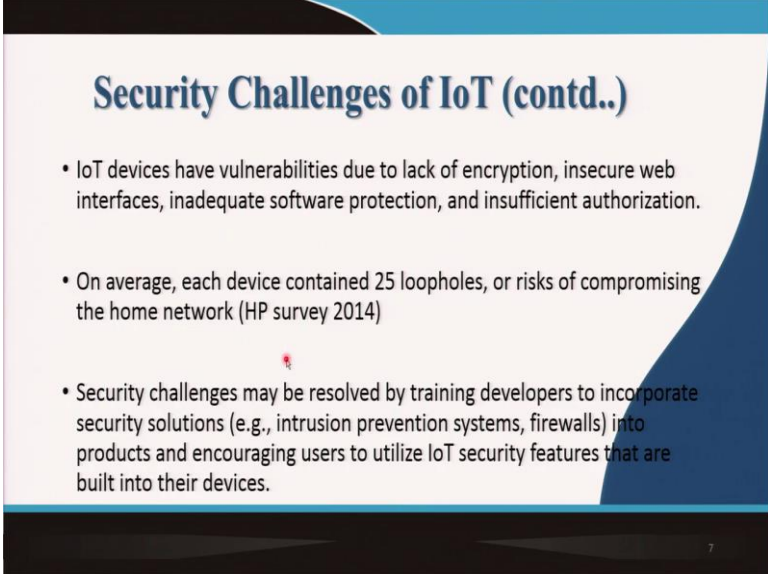
Because in case you know you have a you have a car which is connected with sensors and if the third party or the malicious attacker wants to harm you, they can break into

your system and they can disrupt the control of your vehicle. So, your; you may; you may lose control over your brakes, you may lose control over your vehicle and your life may be in danger.

The situation becomes even more grim, in case of, you know, in case you are using sensors in, you know, in your heart where your pacemaker is controlled remotely or say in insulin pumps. So, if a hacker wants to you know wants to actually you know has an extremely malicious intent, the hacker may actually get into your body and can disrupt the functionality of the sensor here and that could actually have a very very detrimental effect on your health.

So, security challenges though may seem benign, can have an immense you know can create an immense has the potential of creating a huge amount of problem, if they are into your smart systems in your body, in your car, in your home and if they try to you know take control. So, here we see security poses a huge challenge.

(Refer Slide Time: 22:57)



Security Challenges of IoT (contd.)

- IoT devices have vulnerabilities due to lack of encryption, insecure web interfaces, inadequate software protection, and insufficient authorization.
- On average, each device contained 25 loopholes, or risks of compromising the home network (HP survey 2014)
- Security challenges may be resolved by training developers to incorporate security solutions (e.g., intrusion prevention systems, firewalls) into products and encouraging users to utilize IoT security features that are built into their devices.


Now, moving on security challenges become even more grim because IOT devices have vulnerabilities. Due to lack of encryption, insecure web interfaces, inadequate software protection and insufficient authorization. So, security measures are not adequately implemented in many IOT systems.

Because of which there is a huge problem. On average each device contain you know there was an survey conducted by H P in 2014 and they surveyed a home network home automation system. They found that on average each device contained 25 loopholes, which could be compromised by a by a malicious entity.

So, security challenges may be resolved, by training developers to incorporate security solutions such as intrusion prevention systems or firewalls into products and encouraging users to utilize IOT security features that are built into their devices.

So, a lot of awareness and a lot of training you know needs to happen, if you actually have to take care of the security challenges related to I O T. You not only have to train the you know the developers have to be trained at the same time users have to be trained to a large extent, trained and made aware of the challenges posed by security and of how they could be controlled.

(Refer Slide Time: 24:28)



Legal Challenges of IoT

- **Data Ownership and liability issues** : Multiple stakeholders, MGI and M2M communication generated in an IoT environment pose ownership and liability issues.
- **Intellectual Property rights**: When an original data is created by virtue of the interaction of various devices in an IoT environment, which may include, *inter alia*, a new process of arriving at desired results, who claims the IP Rights in such content/data/process?

So, moving on we have discussed quite a bit about the privacy and security challenges, the now talking a little bit about the legal challenges. So, legal challenges there could be a lot of legal challenges related to IOT lets discuss a few of them, challenges due to data ownership and liability issues.

So, we have just discussed data ownership could be a problem since there are multiple stakeholders to an IOT system and there are also a lot of machine generated information

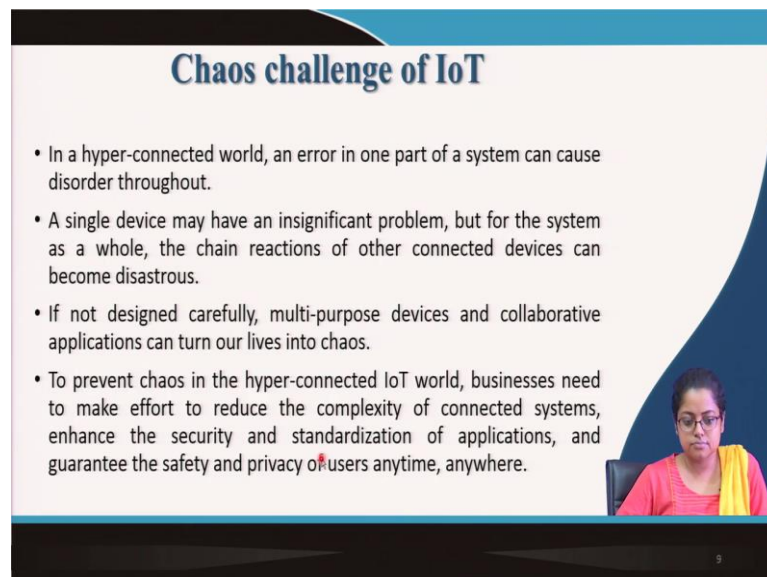
and a lot of machine to machine communication generated in an IOT environment. So, here there could be a problem related to the ownership and who takes the liability in case you know there is a conflict.

So, data ownership and liability could create legal issues in turn in an IOT system. Intellectual property rights they are also very important. Because when an original data is created by virtue of interaction of various devices in an IOT environment, which may include among other things a new process of arrival at a arriving at a desired result, who claims the I P rights in such content data or process.

So, for example, if a new process has been created, with you know because of now in build building in new a sensors or putting a new sensors in an IOT system. A new process gets created or a new content gets created or a new data gets generated.

So, who claims the intellectual property of that? So, that also becomes a challenge because there are again multiple stakeholders involved in the entire IOT system. So, these are some examples of legal challenges there could be a lot more, but these are the primary ones that we wanted to highlight in this course.

(Refer Slide Time: 26:24)



Chaos challenge of IoT

- In a hyper-connected world, an error in one part of a system can cause disorder throughout.
- A single device may have an insignificant problem, but for the system as a whole, the chain reactions of other connected devices can become disastrous.
- If not designed carefully, multi-purpose devices and collaborative applications can turn our lives into chaos.
- To prevent chaos in the hyper-connected IoT world, businesses need to make effort to reduce the complexity of connected systems, enhance the security and standardization of applications, and guarantee the safety and privacy of users anytime, anywhere.

And finally, the chaos challenge. So, everything is connected right, you realize that by now. That in an IOT system whether it is in a home, whether it is in the traffic system, whether it is in a human body, things are connected to one another. So, in a hyper

connected world an error in one part of the system can cause a ripple effect and can cause disorder throughout. So, single device may have an insignificant problem.

But if that device is a part of the entire system, there is a chain reaction and the entire system you know the connected devices may fall apart, so that can create a huge disaster. If not designed carefully, multipurpose devices and collaborative applications can turn our lives into chaos. Because you know that if every device around you is connected to the internet and some of them start malfunctioning then, God help us!

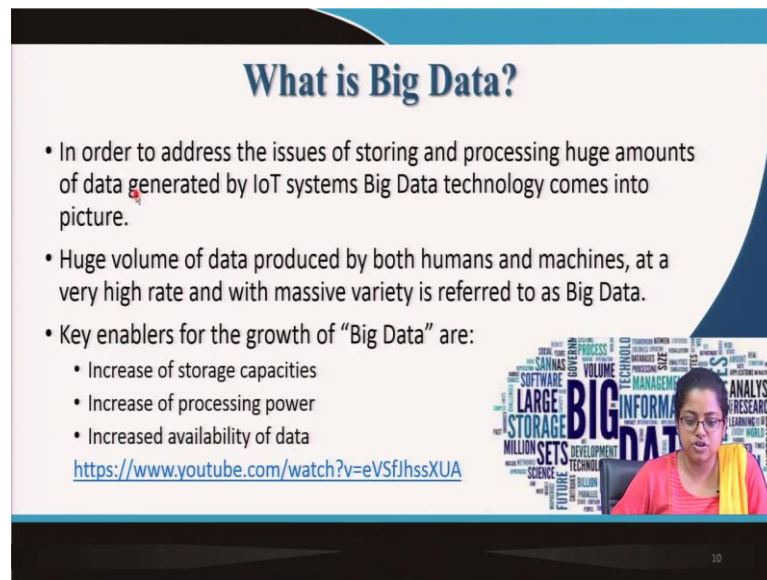
So, you saw in the example in the previous you know session, where we had seen how in a house you know every activity of the residence is directed or guided in some way by internet of things. So, if certain things malfunction then there can be a huge problem for the entire household.

So, this chaos challenge has to be controlled or prevented by you know trying to reduce the complexity of connected systems, by enhancing security, privacy, standardization of applications very important. That is why there are IOT standards and that would actually guarantee the safety and privacy of users anytime and anywhere.

So, standardization and taking care to reduce complexity security and enhancing security and privacy are of utmost importance, if you want to manage the chaos with respect to failing internet of things or with respect to errors in internet of things. So, these are some of the major challenges.

So, we have discussed the challenges as well as ways and means to overcome them. So, 'big data' is another big data technology, is another way of overcoming, the technology management or the management of data as we have seen here the management of data in IOT system. So, the storing and the processing of zeta bytes of data is facilitated by another evolving technology known as 'big data'. So, we will take up 'big data' in the next session.

(Refer Slide Time: 29:07)



What is Big Data?

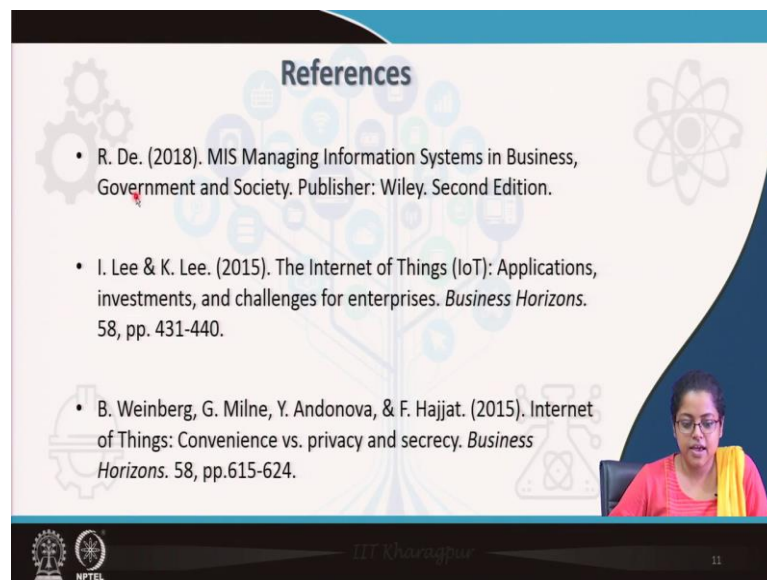
- In order to address the issues of storing and processing huge amounts of data generated by IoT systems Big Data technology comes into picture.
- Huge volume of data produced by both humans and machines, at a very high rate and with massive variety is referred to as Big Data.
- Key enablers for the growth of “Big Data” are:
 - Increase of storage capacities
 - Increase of processing power
 - Increased availability of data

<https://www.youtube.com/watch?v=eVSfJhssXUA>

10

We will not touch upon it today, we will take it up in the next session and see how it can, you know, resolve some of the data related challenge of challenges of internet of things.

(Refer Slide Time: 29:20)



References

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.
- I. Lee & K. Lee. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*. 58, pp. 431-440.
- B. Weinberg, G. Milne, Y. Andonova, & F. Hajjat. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*. 58, pp.615-624.

11

These are my references; thank you! And we will see you in the next lecture where we will talk about big data, block chain and some other emerging technologies.

Thank you!