

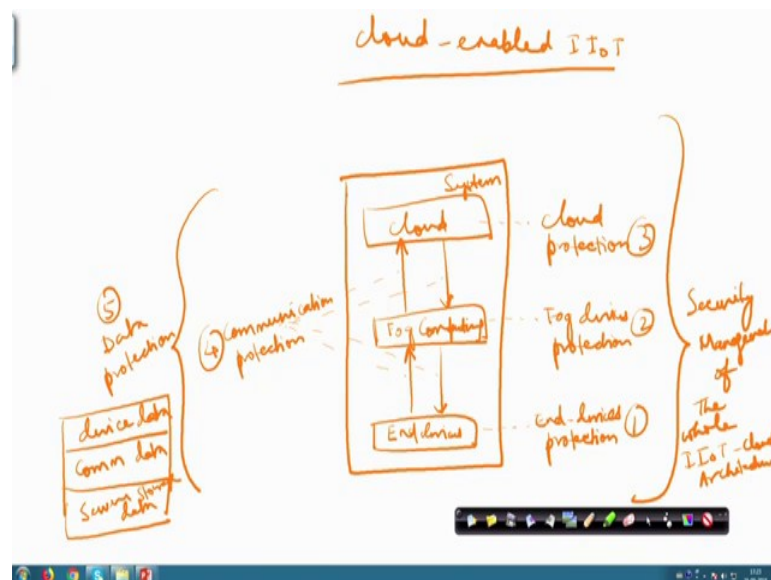
Introduction to Industry 4.0 and Industrial Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 48
Advanced Technologies: Security in IIoT - Part 2

So, in the previous lecture on Security for IIoT we discussed about the security vulnerabilities in IIoT which is in addition to what already exists for IoT, we have seen that there is an integration of IT with OT in IIoT. So, consequently one needs to consider the security issues with IT and OT and their convergence separately. So, we have looked at all of these; now let us look at the few other issues.

So, before we do so I would like to go through a very high level schematic of the actual communication taking place in an IIoT scenario and this we have done in different perspectives in the previous lectures, but in order to keep things in the perspective of security let us revisit the whole thing from a different angle. Let us look at what actually happens with respect to communication in an IIoT setting.

(Refer Slide Time: 01:37)



So, let us think about what actually happens, if we are talking about some cloud enabled IIoT system, so let us look at the cloud enabled IIoT system. So, at the very bottom or let us say that when we are talking about the system as a whole at the very bottom we are talking about different end devices.

Thereafter let us say that it is completely you know up to date with technology we have fog as well as cloud implementations, let us see that thereafter we have another layer of processing which is the fog computing layer, which actually does some processing close to the edge, so basically close to these devices from which the data are being retrieved.

And so we have two way communication between these two layer and as we have seen in the lectures on fog computing and cloud, that the rest of the data which can wait for the processing of would be sent to another layer which is basically the cloud right so this is the cloud layer and so we have bidirectional communication between all of these different layers; the end devices layer, the fog layer and the cloud layer.

So, holistically we have let us say that this particular box representing our system, this is our IIoT cloud fog enabled IIoT system. So, if you look at the security aspects we need security for everything. So, we need security for end devices, protection this is quite obvious, we need security for the protection of fog devices.

We need security for cloud; fog devices protection and this is cloud protection, cloud security and so on. And we have bidirectional communication everywhere we have these different communication links between all of these 3 different layers in the system as a whole.

So, these are all communication links, so we need protection for this communication system protection. So, we need communication protection and so let us number these. Let us say that this is number 1, this will be our number 2, this will be our number 3, this will be our number 4 and then what is happening is that from this system as a whole we are retrieving the data. So, the data is being retrieved and has to be protected. So, this we need as data protection.

So, data protection and so if we look at the data protection, then basically the data has to be protected at again the respective levels. So it can be your device data, so device data protection; communication data, so communication data protection; and then we have the server storage data, so server storage data protection.

So, these are respective components we have seen that these are mainly the 5 components where protection is required. Now holistically the whole thing has to be managed with respect to security. So, this is security management. So, we need a suitable

architecture for security management. So, security management of the whole IIoT cloud architecture.

So, this is holistically what we need to do in terms of security management of a cloud fog enabled IIoT system. So, this is the holistic perspective that we have to keep when we discuss about the rest of the topics in this particular lecture. So, let us proceed further and see what we can do about this security protection.

(Refer Slide Time: 07:03)

Security requirements for IIoT

- End-to-end security is the primary requirement of IIoT
- Both horizontal and vertical security are important
- Security of the whole system depends:
 - Security of deployed devices
 - Communication security
 - Data protection
 - Security management

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

The slide includes a diagram showing two vertical stacks of layers representing devices, labeled 'Dev 1' and 'Dev 2'. A vertical double-headed arrow on the left is labeled 'vertical security', and a horizontal double-headed arrow between the stacks is labeled 'horizontal security'.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 2

So, if we are talking about security in terms of the requirements for security in the IIoT context. We need to have end to end security between the end devices, so from the origin point of the data till the point of consumption or point of storage or whatever.

So, from the source to the receiver to the intended destination etc., end to end security has to be ensured otherwise if you do not have a system which has ensured end to end security the system as a whole is not going to work for all practical purposes. Next important thing is that holistic end to end security is fine, but think about it little bit deeper. So, when you talk about different devices these are the different devices that internally are composed of different layers.

So, you have one device following a particular stack you have one device following a particular stack comprising of different layers likewise you have different other devices having different layers and so on and you are trying to put them all together. So, it is

something like this that you have one stack. So, this is let us say device 1, this is another stack let us say this is device 2 and this thing can continue like this all right.

So, we need to ensure horizontal security; that means, so basically what is going to happen is communication between these different layers are going to happen. So, we have to ensure horizontal security as well as we need to also ensure this one which is the vertical security; both are important. So, security of the whole system comprising of horizontal as well as vertical security ensuring end to end security is what we have to strive to achieve.

So, security of the deployed devices is required when you are thinking about the system as a whole communication security is important, data security is important, security management is important right. So, we are talking about all these different types of security issues and taking care of these component wise layer wise and so on for the system as a whole IIoT clouds, fog enabled IIoT system and its security.

(Refer Slide Time: 09:53)

Security Framework for IIoT

- Every industrial application of IoT must have a security framework with its own requirements and solutions
- The framework should address:
 - Different security issues in IIoT
 - Trustworthy IIoT System
 - Major security building blocks of IIoT
 - Techniques for securing each independent block and secure integration

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

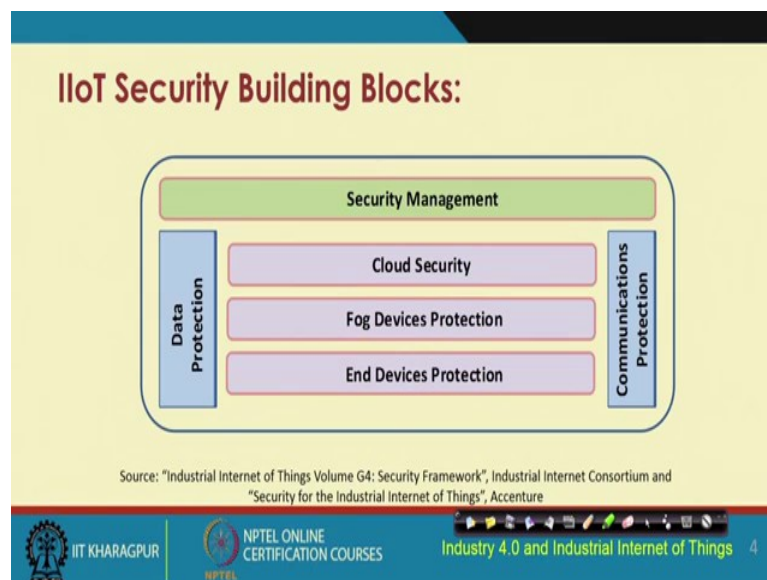
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 3

So, when you are talking about IIoT industrial applications of IoT we have to ensure that there are certain commonalities, there are certain commonalities across all IIoT applications which are fine. So, you can come up with a common security framework, but then there are specificities across different application domains even within an application domain also there are sometimes custom requirements that will have to be fulfilled for different industries.

So, all of these security requirements will have to be understood and then you have to come up with a security framework catering to the requirements which are general plus the custom requirements. So, the framework that we come up with for security has to address different issues in IIoT, has to ensure trustworthiness of the system, has to ensure that each of the individual building blocks have taken care of the different vulnerabilities and the security aspects.

And will have to ensure that the communication itself, the communication that takes place itself across the different independent and different other building blocks those are also secured. So, you need to have techniques for securing each of these individual blocks plus their integration and the communication between them.

(Refer Slide Time: 11:31)



So, IIoT security building blocks would be like this, you need to have end devices security, fog devices security, cloud security, you need to ensure that the data that is coming in from this whole system that is secured and protected. The communication medium through which these different devices communicate that is also protected and secured and you need to have a holistic security management framework cutting across all these verticals and horizontals.

(Refer Slide Time: 12:08)

End Devices Protection - Challenges

- Devices: sensors, actuators, machines and many small embedded devices
- Resource constrained
- Many devices are mobile
- Heterogeneous
- No support for standard cryptographic protocols

Source: "Security for the Industrial Internet of Things", Accenture

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 5

So, when we are talking about end devices protection of end devices we are talking about essentially sensors, actuators, their communication; the sensors and actuators they are hosts; that means, the machines where they are deployed, the embedded systems that are running them and so on. So, we need to consider the protection of all of these different components, additionally we also have to keep in mind what I was telling you in the previous lecture that we are talking about IIoT means that we are talking about a highly resource constraint environment.

So, resource constraint, energy constraint, processing constraint the network resource itself is constraint, bandwidth constraint, low data rate, low energy. So, we have a highly constraint kind of environment and we have to ensure the protection of the different devices, the different devices in isolation, the different devices in communication and the different devices that comprise the system as a whole.

Heterogeneity also we have talked about earlier the real challenge in IIoT is that we are not talking about homogeneous devices following homogeneous protocols homogeneous standards and so on. We are not talking about that IIoT essentially is featured to run different heterogeneous protocols, heterogeneous devices working intended and so on.

So, we need to take care of this kind of challenge to deal with heterogeneity. So, and there is no standard cryptographic protocols that are there to run for IIoT. I mean people are working on different protocols, they are trying to come up with lightweight protocols

that are going to work in this kind of constraint environments, but cryptography itself is heavyweight.

So, original cryptography itself is heavyweight coming up with lightweight protocols, cryptographic protocols is a huge challenge and so there are lots of research work one would find which are trying to cater to cryptographic protocols and their design for IoT and IIoT.

(Refer Slide Time: 14:10)



So, in terms of the requirements when we are talking about the end devices we have to ensure physical security of these devices, we have to ensure that the end devices have their identity and this identity will have to be protected, we have to ensure the protection of the data the and also the access control. We have to ensure that legitimate access control based on what actually the organizational policies are going to support so legitimate access control is has to be ensured.

So, it should not happen that a particular device gets accessed by someone in certain level of the automation hierarchy who should not actually have access to that device or it's data. So, not only within the organization, but also outside the organization also nobody should get illegitimate access to the devices and the data. So, all these 4 components can be summarized in this manner.

So, we have to ensure for end device protection that there is suitable authentication mechanism in place, which will give an assurance that a claimed characteristic of the entity is correct and suitable authorization is also in place in order to ensure that suitable rights are granted as per the requirements and as per what is desirable.

(Refer Slide Time: 15:46)

End Devices Protection – Solutions

- Lightweight cryptographic protocols
 - Energy efficient authentication
 - Lightweight symmetric key cryptography
- IDS and behavior analysis at upper layer devices
 - Malicious behavior detection
 - Abnormal data traffic detection
 - Mitigation using proper actuation unit and signals

Source: Pacheco et al., 2017 and "Lightweight Cryptography for the Internet of Things", Sony Corporation

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industri

So, there are different solutions for end devices protection we need lightweight cryptographic protocols there are many that have been researched, there are a lot of research papers that basically come up with lightweight cryptographic protocols for IIoT. Energy efficient authentication mechanisms, lightweight symmetric key cryptography; symmetric key as you probably already know, here actually we are talking the same key being used at both the ends right, so the symmetric key.

And so lightweight symmetric key cryptographic mechanisms should be used and also intrusion detection; intrusion detection coming up with intrusion detection system, intrusion prevention systems based on behavioral analysis at different layers of the device basically analyzing the malicious behavior, detecting malicious behavior based on the data and it's analysis, abnormal data traffic detection, mitigation using proper actuation unit and signal. So, all of these things will have to be done in order to protect the end devices.

(Refer Slide Time: 17:03)

Fog Devices Protection

- Devices deployed near to end-devices capable of notable computing and storage
- Requirements are same as end devices
- Standard cryptographic protocols for:
 - Authentication between fog devices
 - Authentication between fog devices and cloud
- Lightweight cryptography for security between for authenticating end devices

Source: Pacheco et al., 2017

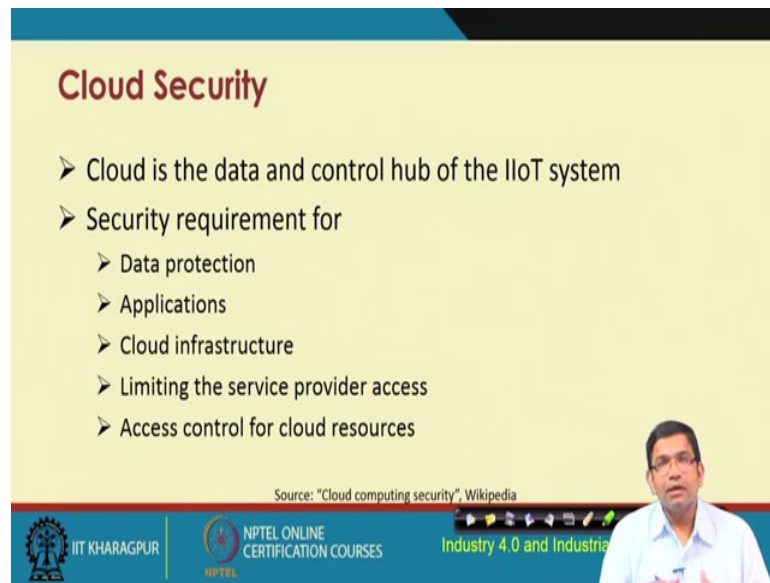
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial

The slide features a yellow background with a blue header and footer. A small video feed of a man in a white shirt is visible in the bottom right corner of the slide area.

So, in terms of protection of the fog devices; fog devices are deployed near to the end devices and these are also constraint, it is better than the end devices in terms of computing storage etc., but still it is more constraint than what actually exists at the server form or the cloud end. So, these fog devices because they are also like semi-constraint in terms of resources storage computing etc., will have to ensure that we have some suitable protection mechanisms in place for protecting these fog devices.

So, plus we have to come up with some cryptographic protocols that are going to do authentication, authorization and authentication of the fog devices and authentication between the fog devices and the cloud. So, basically the essence over here is to ensure that we come up with lightweight cryptographic and other security information system security methods for use in this kind of constraint environments.

(Refer Slide Time: 18:18)



Cloud Security

- Cloud is the data and control hub of the IIoT system
- Security requirement for
 - Data protection
 - Applications
 - Cloud infrastructure
 - Limiting the service provider access
 - Access control for cloud resources

Source: "Cloud computing security", Wikipedia

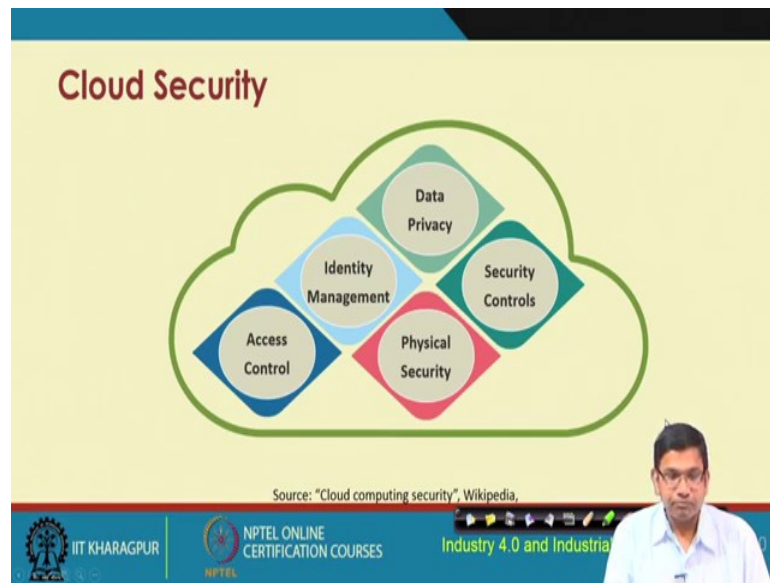
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial

The slide features a yellow background with a blue header and footer. A small video inset in the bottom right corner shows a man in a white shirt speaking. The footer contains logos for IIT Khharagpur and NPTEL, along with the text 'Industry 4.0 and Industrial'.

Cloud actually is the huge resource; so cloud security is of huge concern because it's typically a third party kind of service cloud, but at the same time cloud security and ensuring cloud security is of a lesser challenge than the fog security or the end device security.

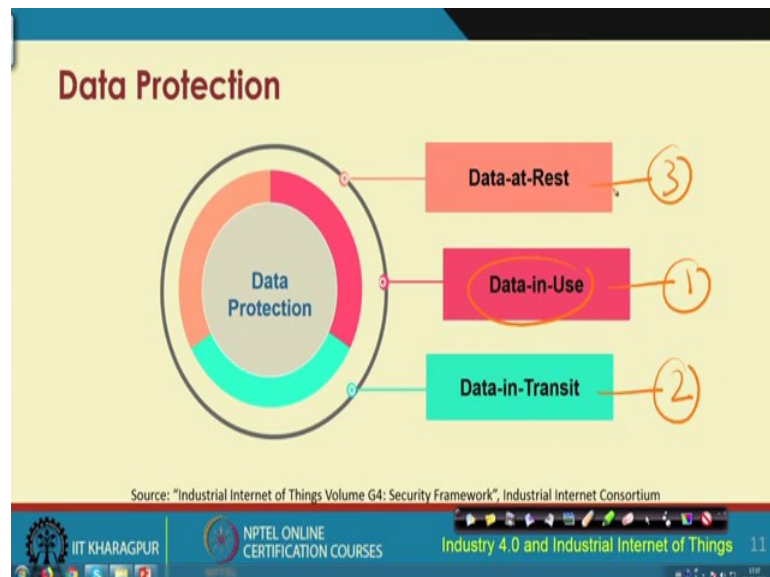
So, for cloud level you need to ensure data protection at the cloud, applications that are running on the cloud and using the data from the cloud they will have to be secured the cloud infrastructure itself has to be secured and protected and also there has to be some policies for limiting the service provider access and also there has to be access control for the cloud resources. So, all of these different aspects of security and the requirements of security for cloud are very important and has to be considered holistically.

(Refer Slide Time: 19:18)



So, for cloud security then we have all these different issues that will have to be taken into consideration, the physical security, data privacy, security controls, identity management and access control. So, holistically all of these different issues will have to be taken into consideration for ensuring cloud security.

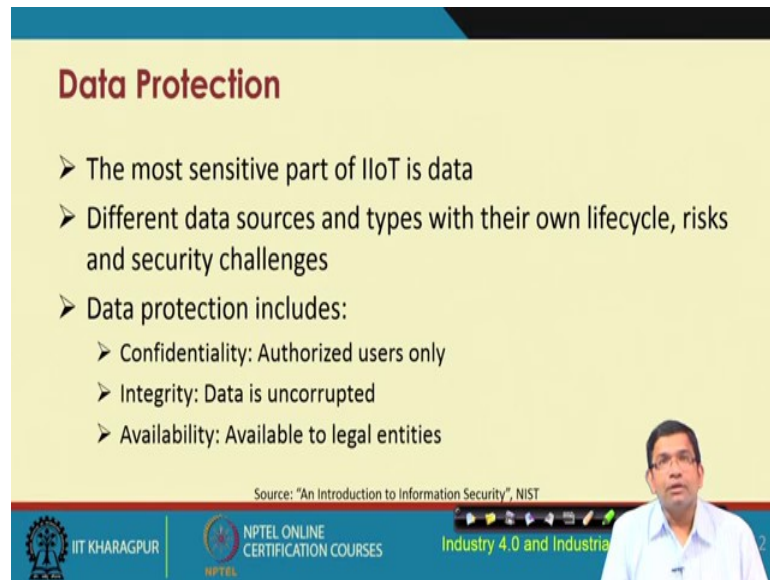
(Refer Slide Time: 19:36)



So, for data protection; there are different types of data, some data are in use, this is one kind of data then we have some data which are basically in transit and some data which are in rest. So, typically stored in the servers for future use so data at rest data in use the

data that are currently being used and data in transit are basically coming to the channel and still they are not being used. So, all these different types of data will have to be protected with suitable levels of protection.

(Refer Slide Time: 20:17)



Data Protection

- The most sensitive part of IIoT is data
- Different data sources and types with their own lifecycle, risks and security challenges
- Data protection includes:
 - Confidentiality: Authorized users only
 - Integrity: Data is uncorrupted
 - Availability: Available to legal entities

Source: "An Introduction to Information Security", NIST

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial IoT

The slide features a yellow background with a blue header and footer. A small video feed of a man in a white shirt is visible in the bottom right corner. The footer contains logos for IIT Khargapur and NPTEL, along with the text 'NPTEL ONLINE CERTIFICATION COURSES' and 'Industry 4.0 and Industrial IoT'.

So, data protection is the most sensitive part of IIoT and so basically when we are talking about IIoT; IIoT it's all about collecting data and analyzing the data right. So, IIoT is this data and it is the most sensitive part of IIoT systems and you have to ensure suitable levels of protection of IOT data.

Different data sources and types with their own lifecycle risks and security challenges will have to be understood, will have to be analyzed and suitable mechanisms consequently will have to be brought in place. Data protection includes three different things -- confidentiality which has to ensure authorization of only the legitimate user's, integrity which basically talks about ensuring that the data is uncorrupted and it has not been tampered with, and availability which has to ensure that the legal entities are available.

(Refer Slide Time: 21:35)

Communications Protection

- Secure exchange of information between IIoT devices
- Different security risk: sensor data, commands, actuation signals, log reports, configuration messages, etc.
- IIoT traffic and data formats are different from core network
- Protection involves:
 - Communication with devices at the same layer
 - Communication with devices at upper or lower layer

Source: Pacheco et al., 2017

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Automation

The slide features a video inset of a man in a white shirt speaking in the bottom right corner. The footer contains logos for IIT Khargapur and NPTEL, along with the course title 'Industry 4.0 and Industrial Automation'.

So, availability of the data whenever it is required to the legally entitled entities is very essential. So, these are the three different layers of data protection confidentiality, integrity and availability. Communication protection securing the exchange of information between the IIoT devices. IIoT: it's all about connectivity, so when whenever we are talking about connectivity. So, basically earlier I told you that IIoT code to IIoT is data, but the data has to come only if these devices are all interconnected right.

So, at the backbone is what we have is the communication channel the backbone network etc. So, that channel itself has to be secured so communications security and protection is very important. So, the different security risks that exist would be with securing the sensor data, securing the commands, securing the actuators and the signals that are sent for actuation, log reports and their security configuration messages and their security and so on.

So, all of these are different security risks and their security will have to be ensured adequately. IIoT traffic and data formats are different from the core network, so protection involves communication with the devices at the same layer which is basically the horizontal security that I talked about earlier and communication with devices at upper or lower layer which is the vertical security that also I explained earlier.

(Refer Slide Time: 22:56)

Communications Protection Techniques

- Network access control
- Security gateways
- Network firewalls
- Cryptographic protocols with:
 - Strong mutual authentication
 - Authorization mechanism
 - Data ciphering

Source: Pacheco et al., 2017

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial

So, for communication protection, communication security you need to have suitable network access control you need to have security gateways, network firewalls and also different cryptographic protocols for authentication, authorization and data coding encoding.

(Refer Slide Time: 23:19)

Security Management

- Deals with configurations, periodic updates and managing the security controls
- An active unit, functions from establishment to end of entire IIoT system
- Prevention, detection, analysis and mitigation of security risks
- Performs security monitoring, policy management and updates over time as per standards

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

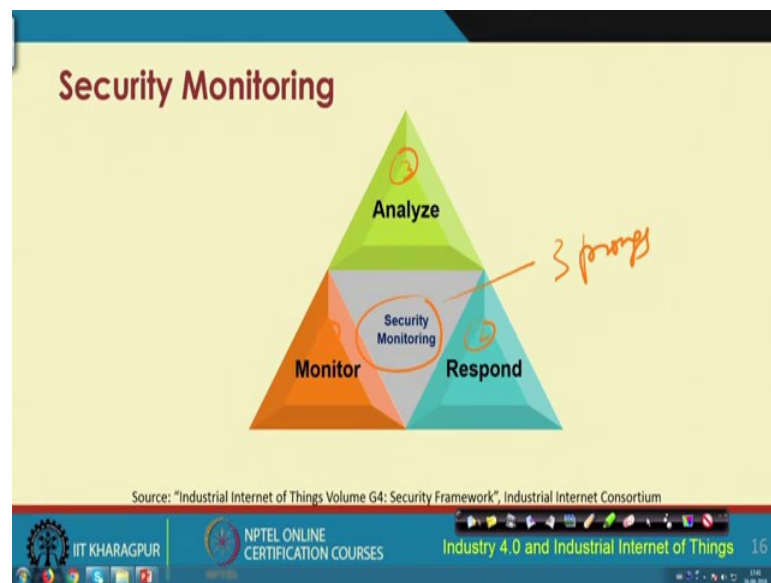
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial

For security management we are talking about the system as a whole, we are talking about dealing with issues of configurations, periodic updates and managing the security

controls. Security management is an active important function and this has to ensure that the whole system the IIoT system is secured.

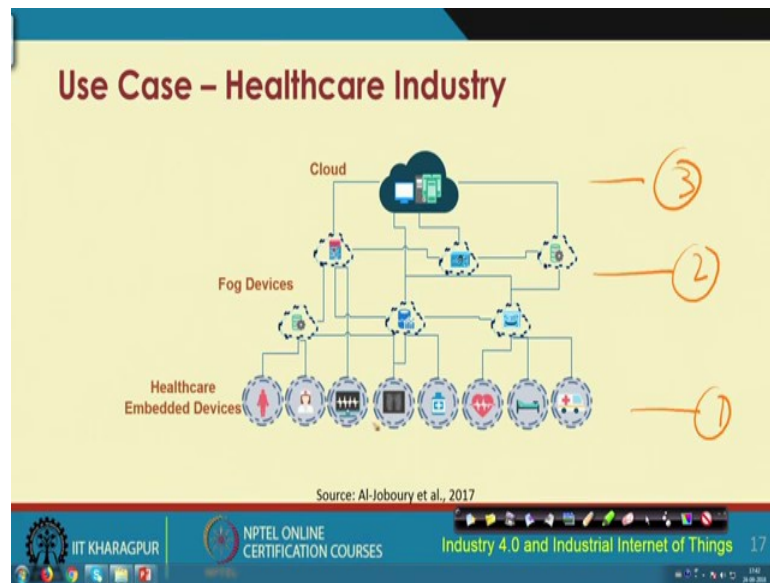
So, the management of this whole system is what concerns the security management of IIoT. Prevention detection analysis and mitigation of security risks are very important when you are talking about security management of any system and definitely for IIoT systems.

(Refer Slide Time: 24:02)



So, for security monitoring these are the three different prongs of the same problem, one is the monitoring, response and analysis. These are the 3 different prongs of security monitoring; monitoring, response based on what is being observed, and the analysis of the data. So, this is the security monitoring and its three different prongs.

(Refer Slide Time: 24:35)



Now, let us look at this particular diagram which talks about a fog cloud enabled IIoT system for healthcare industry this is an architecture that I have taken from the source given below. So, look at the different layers over here so we have the healthcare embedded devices in this particular layer: this is layer 1, then you have the fog devices layer and the cloud layer.

So, holistically so these are basically the healthcare embedded devices such as SpO₂, devices such as the different healthcare monitors, devices such as the glucose monitoring system, devices such as the blood pressure monitor like that all these different devices and their connectivity. So, these devices are basically in an IIoT scenario these devices do not work in isolation, they are all connected.

So, ensuring the security of all of these devices and their interaction between them is important and second is the fog devices layer here also the security mechanisms adequately will have to be ensured and finally, at the cloud layer also the data are being stored and adequate security mechanisms and adequate access control through the cloud will also have to be ensured.

So, access control and data protection at through the cloud at the cloud, through the fog at the fog and also through the healthcare embedded devices and at these devices -- these are all these different things that will have to be taken into consideration and analyzed.

(Refer Slide Time: 26:22)

Security in Healthcare IoT

- Devices security:
 - Protection of healthcare embedded devices
 - Protection of fog devices - gateways, processing units, data hubs
 - Cloud security
- Communications Security:
 - Healthcare devices - Fog devices (Lightweight cryptography)
 - Fog devices - Fog devices (Cryptography, Firewalls, Security gateways)
 - Fog devices - cloud (Cryptography, Security applications)

Source: Pacheco et al., 2017

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 18

So, whenever we are talking about security in healthcare IoT we have to talk about the devices, their security, their protection, devices would include not only the sensors actuators and so on but also in the gateways the processing units, the data hubs and also the cloud to where most of this data are stored. The second is the communication security which is basically talking about security of these connected devices, these connected devices themselves, connected devices to the fog, connected fog to cloud.

So, the communication everywhere will have to be secured suitably using lightweight cryptographic methods, we using gateways secured gateways, using secured, using firewalls and different secure security applications. So, using all of these holistically communication security will have to be ensured.

(Refer Slide Time: 27:22)

Security in Healthcare IoT (Contd.)

- Data Protection:
 - Device data protection (Password, Signatures, Digital certificates)
 - Communication data (data ciphering and hashing)
 - Data at cloud (Access control lists, Signatures, Digital certificates)
- Security Management:
 - Global security handling at cloud
 - SDN-based security management and monitoring

Source: Pacheco et al., 2017 and Flauzac et al., 2017

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 19

Device data protection using suitable password mechanism, signatures, digital certificates, communication data protection using suitable use of data ciphering and hashing and data protection at the cloud using suitable access control mechanisms, digital signatures, digital certificates and so on. Security management holistically global security handling at the cloud and SDN based security management and monitoring.

SDN is something that I have already discussed in detail in two different lectures I am not going to mention or elaborate it further over here, but I think this is quite understandable, SDN based security management and monitoring is basically what is desirable because most of these systems are going to be in the future SDN enabled and their security is also of importance.

(Refer Slide Time: 28:16)

Regulatory Standards for IIoT Security

- A security standard helps in achieving a common level of security in industries
- Standards help manufacturers and vendors to offer services at different level of security
- For IIoT, security standards should include requirements of IT and OT
- Till date, there is no security standards specific to IIoT

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 20

Regulatory standards for IIoT security is important not only all these technological issues, not only these technical issues, device level, fog level and cloud level and the communication level and so on. But also we are talking about ensuring that the regulatory standards that are in place the security of those.

So basically for IIoT we are talking about security standards, conforming to the requirements of IT and OT. Information technology and operation technology and there is unfortunately no security standards that is in place to ensure the security of IT and OT; that means, catering to the requirements of IIoT.

(Refer Slide Time: 29:03)

Standards Related to IIoT Security

IT Security

- ISO/IEC 154083: Common Criteria for Information Technology Security Evaluation
- ISO series of standards for privacy, framework and regulations
- ISO 27017, NIST SP 800-144, ENISA standard: Cloud security standards
- Common criteria and Federal Information Processing Standard (FIPS)

OT Security

- IEC 62443: Industrial automation and control systems security
- NIST SP 800-82: Security in Industrial Control Systems
- NERC-CIP: Critical infrastructure protection
- IEEE 1686: Standard for Intelligent Electronic Devices Cyber Security Capabilities
- NISTIR 7628: Guidelines for Smart Grid Cyber Security

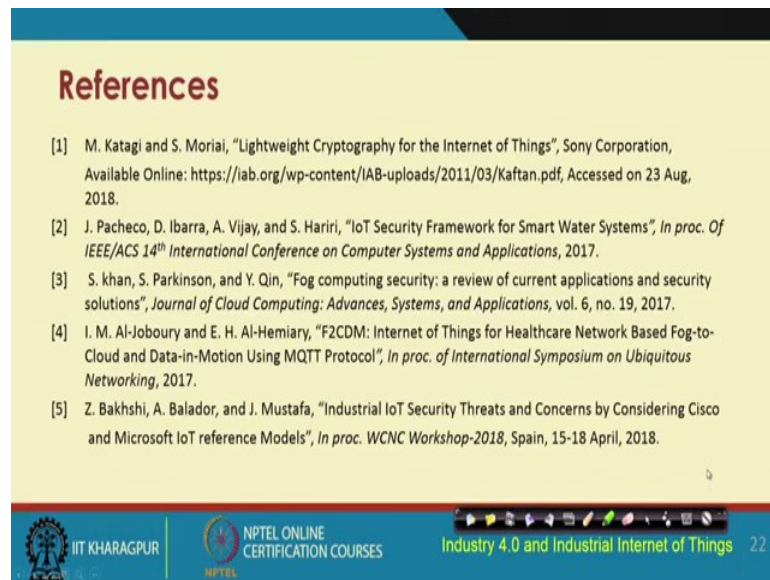
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 21

So, if you are talking about separately IT security, there are some regulatory standards that are there ISO/IEC 154083, this is a common criteria for information technology security evaluation, like this there are few other related standards for security of IT, for OT also separately there is this standard IEC 62443 which is a an industrial automation and control system security standard like this NIST also has its own and so on.

There are a few different other standards for OT which are in place, but in IIoT once again we are talking about IT and OT security requirements working together. So, you have to have a separate set of regulatory requirements for security of IT-OT convergence to be there. So, one is to come up with those regulatory framework for ensuring IIoT security.

(Refer Slide Time: 30:05)



References

- [1] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things", Sony Corporation, Available Online: <https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf>, Accessed on 23 Aug, 2018.
- [2] J. Pacheco, D. Ibarra, A. Vijay, and S. Hariri, "IoT Security Framework for Smart Water Systems", *In proc. Of IEEE/ACS 14th International Conference on Computer Systems and Applications*, 2017.
- [3] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions", *Journal of Cloud Computing: Advances, Systems, and Applications*, vol. 6, no. 19, 2017.
- [4] I. M. Al-Joboury and E. H. Al-Hemiary, "F2CDM: Internet of Things for Healthcare Network Based Fog-to-Cloud and Data-in-Motion Using MQTT Protocol", *In proc. of International Symposium on Ubiquitous Networking*, 2017.
- [5] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models", *In proc. WCNC Workshop-2018, Spain, 15-18 April, 2018*.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 22

With this we come to an end of security concerns and their issues and their discussion surrounding. These are some of these different references that you can go through if you are interested to dig further into these issues of security in the context of IIoT.

Thank you.