Introduction to Industry 4.0 and Industrial Internet of things

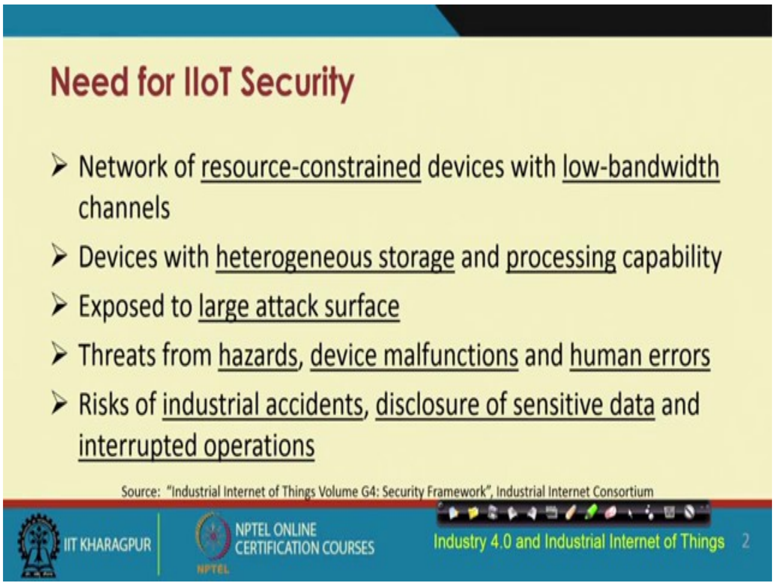
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 47
Advanced Technologies: Security in IIoT - Part 1

In this particular lecture, we are going to focus on the security aspects of IIoT. So, this particular lecture will give a highlight of the different security issues, the vulnerabilities that exist due to the incorporation of IoT in the industrial sector, manufacturing plants and so on, and why these vulnerabilities arise and what are the main issues and so on. And at a very high level; what are the ways forward the discussions about those. So, this is what we are going to discuss in this particular lecture and the next.

So, when we think about IIoT. So, IIoT is industrial IoT as we have seen this in detail in the last several lectures. So, industrial IoT, when we talk about it is basically an integration of IoT to cater to the requirements of the industrial sector. So, every industrial sector has its own separate requirements. So, catering to those specific requirements for these different industry verticals is what IIoT should concern.

(Refer Slide Time: 01:41)



Need for IIoT Security

- Network of resource-constrained devices with low-bandwidth channels
- Devices with heterogeneous storage and processing capability
- Exposed to large attack surface
- Threats from hazards, device malfunctions and human errors
- Risks of industrial accidents, disclosure of sensitive data and interrupted operations

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
2

So, let us look at some of these different issues. So, when we talk about IoT as I was telling you that IoT is basically a resource constraint environment internet of things. So, this is what we have been telling time and again in the last several lectures that IoT.

Forget about IIoT, but IoT in general is a highly resource constraint environment with devices which operate in low bandwidth and in resource constraint environment such as devices having very low energy, the devices having very low computational power, the everything like even the storage the buffer etc.; everything is highly constraint. So, we have such a constraint environment.

Now you know when we talk about security, as most of us already know that security basically there are lot of different security solutions that are available right. So, security for IoT particularly in general is something that has been well researched. There are so many different security solutions considering different aspects of security and so on. System security, information security; lot of works are available, lot of different algorithms have been proposed. All these algorithms like you know RSA, Diffie-Hellman and many others right, even the digital certificates and so on; digital signatures and so on; all of these different works on security.

These have been proposed primarily for resourceful environments right; so, where there is no resource constraints. Now, when we talk about wireless networks in general. Wireless networks if we are talking about the traditional wireless networks like cellular networks and Wi-Fi etc.; these have some additional vulnerabilities over the wired counterparts, but still these are not highly resource constraint networks. So, the devices are not highly resource constraint. But when you are talking about IoT devices, these devices are operating in highly resource constraint environments right. So, all these sorts of constraints that I told you just now, so those constraints are applicable for these IoT resource constraint devices.

So, one thing is that IoT devices are primarily, but not necessarily wireless devices right. So, they operate in wireless environment. Secondly, they are resource constrained. And when we talk about IIoT, basically what we are talking about is the incorporation of these IoT systems into the manufacturing sector or the industrial sector. Now, the industrial sector has its own different characteristics, which basically adds to the list of vulnerabilities that were already existing with IoT. So, additional vulnerabilities because of this implementation of IoT in the industrial sector, there are some additional vulnerabilities that are going to be existing.

So, how you are going to deal with all of these different types of vulnerabilities; what are the different types of attacks and what are going to be the different solutions is what concerns security in IIoT. So, going back, as I told you that we are talking about a resource constraint environment, devices are highly resource constraint, energy constraint, processing power constraint, buffer constraint and resource constraint with respect to all kinds of computational resources that we can think off. Plus these IoT devices operate in low bandwidth channels; typically, low bandwidth wireless channels and all these different types of communication wireless communication, wire communication applicable for IoT these are the ones that we have already seen.

And we have always already seen that these different ones which are characterized with their own different features, they pose if you think little deeper, they will pose their own different vulnerabilities which will have to be addressed. Otherwise there could be attacks, security attacks that would be possible; so, that is number one.

Second thing is that we are talking about in the IoT world, not a homogeneous kind of environment, heterogeneous devices; devices following different standards, devices which have been developed through proprietary means using proprietary technology by different vendors, devices having different configurations with respect to storage, with respect to processing capability and so on.

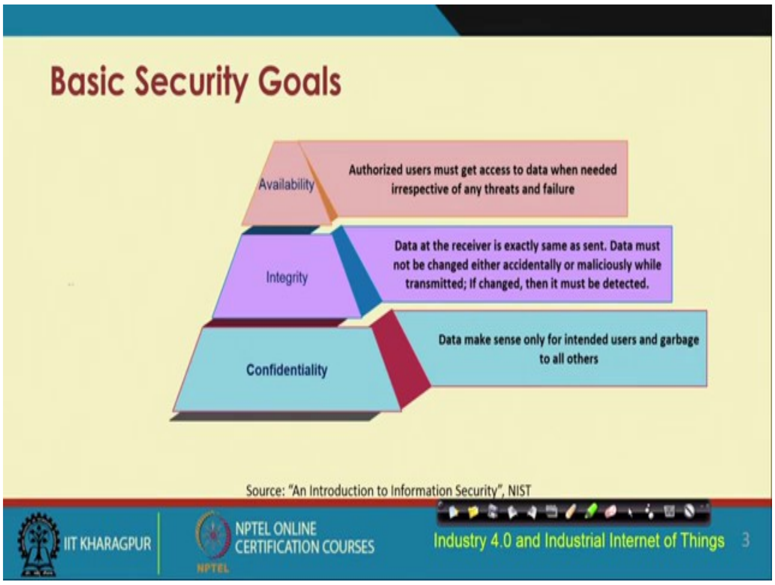
So, these are highly heterogeneous devices, following different own proprietary standards, following different heterogeneous network protocols and other protocols and so on. So, you see that we have a highly complex heterogeneous environment which also adds to the different vulnerabilities that might already exist with IIoT.

Third is that because of all these vulnerabilities, wireless nature and so on and so forth, these systems are exposed to large attack surfaces. So, large attack surface means that there are so many different types of attacks that are possible because of the diverse nature of vulnerabilities that exist in these IoT systems integrated with the industrial systems and so on. So, there are different types of threats.

Additionally in IIoT systems, threats due to different types of industrial hazards; due to the hazards, due to the machineries and so on. Device malfunctions, malfunction of the networks, and human errors. Human is very important in the manufacturing sector, in the industrial sector. So, human errors, there are risks of industrial accidents, disclosure of sensitive data, interrupted operations and so on.

So, as you can see that in a typical IIoT environment, we are not just talking about IoT. We are not just talking about devices, networks and so on. We are not just talking about connectivity, we are also talking about the industrial machinery and their operations and the additional risks or vulnerabilities that come up due to the integration of these low power resource constraint devices in these industrial plants.

(Refer Slide Time: 08:43)



Basic Security Goals

Authorized users must get access to data when needed irrespective of any threats and failure

Data at the receiver is exactly same as sent. Data must not be changed either accidentally or maliciously while transmitted; if changed, then it must be detected.

Data make sense only for intended users and garbage to all others

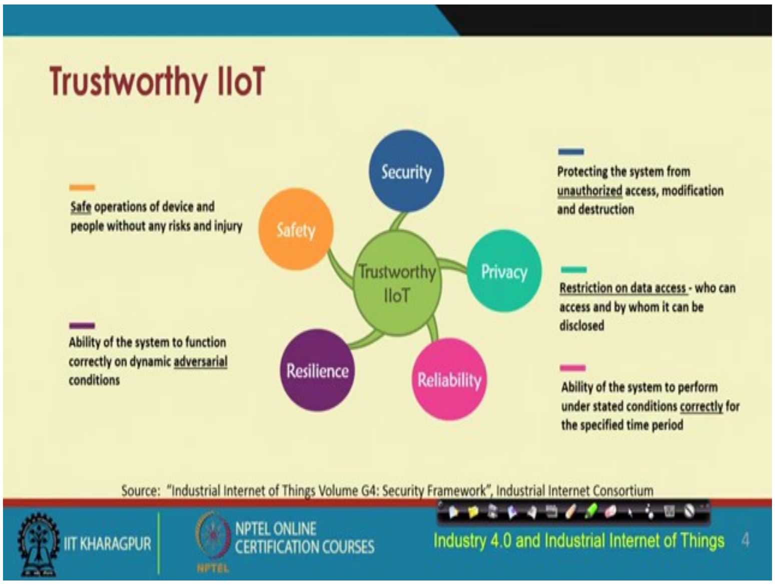
Source: "An Introduction to Information Security", NIST

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

So, the basic security goals with respect to IIoT are 1. Availability. So, availability means that only the authorized users must guest access to the data, but they must get access to the data whenever it is required; irrespective of whether there is any threat or there is any failure of any kind.

Integrity is the 2nd goal of IIoT security. Integrity basically talks about that from the point; the data was sent, till the point that the data was received by the receiver. The contents of the data, the nature of the data, the data as a whole has not changed. So, basically the data that are sent are exactly received in the same way at the receiver; so, that is integrity. 3rd is the confidentiality. Confidentiality basically ensures that only the intended users will get access to the data. So, only the intended users will be able to derive value out of the data and for all others, the data will either not be made available or if it is made available by any chance, then the data will not be of any use to the others.

(Refer Slide Time: 10:20)



Trustworthy IIoT

Safe operations of device and people without any risks and injury

Ability of the system to function correctly on dynamic adversarial conditions

Protecting the system from unauthorized access, modification and destruction

Restriction on data access - who can access and by whom it can be disclosed

Ability of the system to perform under stated conditions correctly for the specified time period

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 4

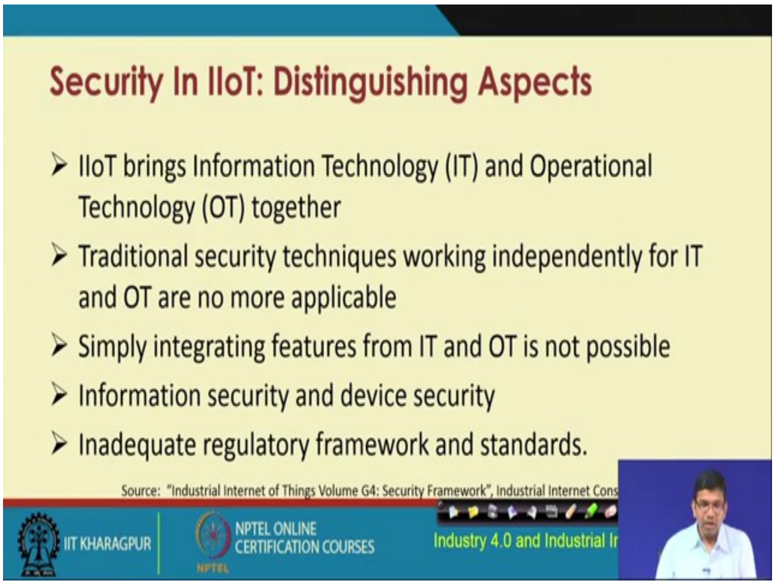
Now, IIoT systems must be trustworthy. Trustworthiness when we talk about has different facets. Trustworthiness with respect to security is what I have been talking about in the last few minutes. Trustworthiness with respect to privacy; that means, only the data will be made available to the ones that are the genuine recipients of it; the privacy of the data should be restricted; the access to the data should be restricted and so on. Only the intended recipients should be able to get access to it; others should not be able to. The privacy of the data should be maintained.

Reliability is very important. So, basically reliability ensures that the system has the ability to perform the under stated conditions correctly for the specified duration of time. Resilience is very important which basically ensures that the system is able to function correctly on dynamic adversarial conditions; if the nature of the adversaries changes, then also the system would be able to function correctly.

And safety; safety particularly is an important characteristics of the industrial IoT. Safety basically ensures that the machinery that are being used, the devices that are being used are not going to pose any risks or are going to not hurt or give injury to the users.

So, safe operations of the device of the machinery and the people without posing any risks and injury that is the safety component of the trustworthiness.

(Refer Slide Time: 12:14)



Security In IIoT: Distinguishing Aspects

- IIoT brings Information Technology (IT) and Operational Technology (OT) together
- Traditional security techniques working independently for IT and OT are no more applicable
- Simply integrating features from IT and OT is not possible
- Information security and device security
- Inadequate regulatory framework and standards.

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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Ir

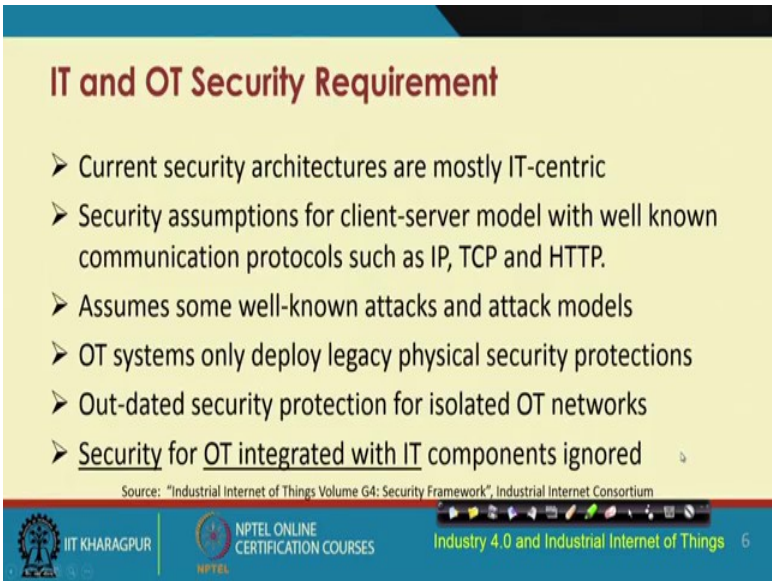
So, security in IIoT, there are certain distinguishing characteristics over the traditional IoT. So, when we talk about IIoT, as we discussed in a previous lecture we are typically at a very high level talking about the integration of information technology with operational technology. So, this operational technology component comes characteristic of industrial sector. So, this operational technology along with the traditional information technology from the traditional IoT, the integration of both of these is the distinguishing characteristic of IIoT.

Traditional security techniques working independently for IT and working independently of OT in the traditional manufacturing plants are no more applicable. So, we are not talking about independent operation of IT, we are not talking about independent operation of OT. It is an environment where IT and OT work hand in hand and that is where we have to consider the features the requirements and so on of both IT and OT and we have to come up with security mechanisms to for that converged set of for the converse set of requirements.

So, simply integrating features from IT and OT is also not possible and is not desirable. So, information security and device security will have to be considered together in order to come up with that IT or OT converged set of requirements for catering to the requirements of security in IIoT as a whole. In addition, we also have to take into consideration the regulatory framework, the regulatory standards that are existing because the regulatory issues are also a very important alongside to be considered for security.

Regulatory standards are very important because if you do not consider the proper regulatory standards, there might be some vulnerabilities that might come, some attacks might sneak in because of those non compliance of these systems with the regulatory standard. So, these are some of these distinguishing aspects of security in our IIoT.

(Refer Slide Time: 14:36)



IT and OT Security Requirement

- Current security architectures are mostly IT-centric
- Security assumptions for client-server model with well known communication protocols such as IP, TCP and HTTP.
- Assumes some well-known attacks and attack models
- OT systems only deploy legacy physical security protections
- Out-dated security protection for isolated OT networks
- Security for OT integrated with IT components ignored

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

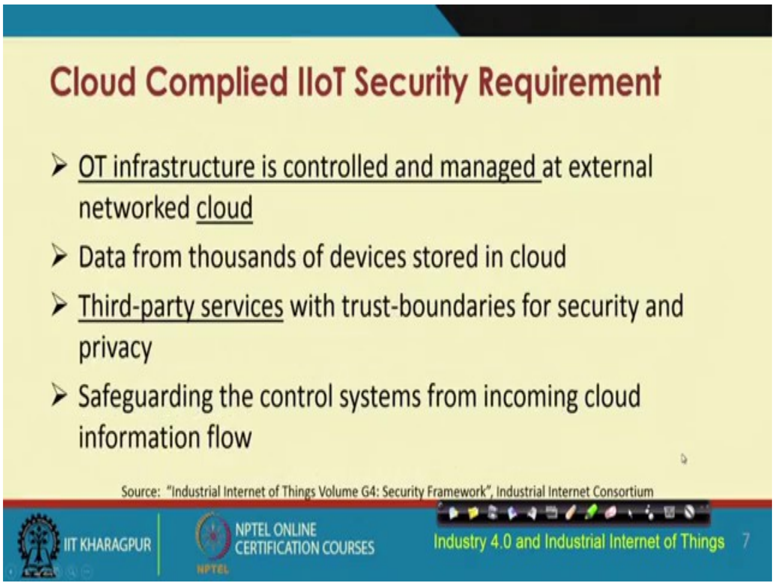
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 6

So, I have been talking a lot about IT and OT security requirement. We have seen that both sorts of requirements will have to be considered. Security for OT integrated with IT components is something that is required to be considered, but is often ignored. So, whenever people talk about IIoT, they simply think about IoT security not IT and OT security integrated as a whole. So, this is the most important requirement that will have to be considered, when we are talking about IIoT security.

So, the current security architectures that are available particularly for catering to IoT requirements are mostly IT centric. Security assumptions for client-server model with well known communication protocols such as IP, TCP, HTTP are no longer valid for IIoT, when we are talking about this IT-OT convergence. So, the well-known attacks and attack models that are there for traditional networks, for traditional wireless networks are also not sufficient to be considered for this kind of IT-OT converged environment.

So, you need to also find out the different other attack possibilities that might exist due to this particular integration of IT with OT. OT systems only deploy legacy physical security protections and IT ones will only cater to the requirements of the traditional IT centric equipments. So, the outdated security prediction are there for most of the isolated OT networks in the most of the industries. So, we need to come up with an integrated solution for catering to the requirements of both IT and OT.

(Refer Slide Time: 16:35)



Cloud Complied IIoT Security Requirement

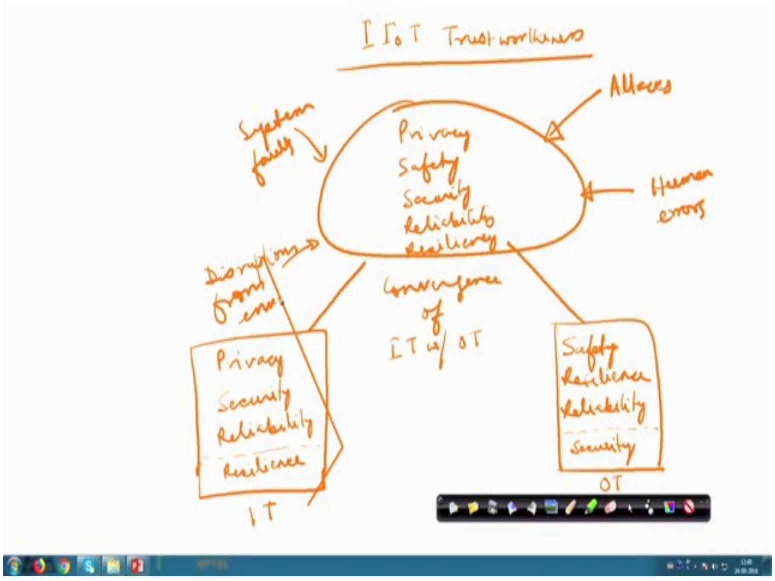
- OT infrastructure is controlled and managed at external networked cloud
- Data from thousands of devices stored in cloud
- Third-party services with trust-boundaries for security and privacy
- Safeguarding the control systems from incoming cloud information flow

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 7

So, having said that let us first try to understand as a whole, what I have just mentioned. So, let us look at this trust issue in IIoT.

(Refer Slide Time: 16:50)



So, IIoT trustworthiness. This is very important. So, let us try to begin into this particular issue in little bit more detail. So, I have been talking a lot about the IT issues. So, we are talking about IT and OT convergence. So, this is let us say OT. So, whenever you are talking about IoT, then IT issues are important. But in industrial IoT, you have to also take into consideration the OT issues.

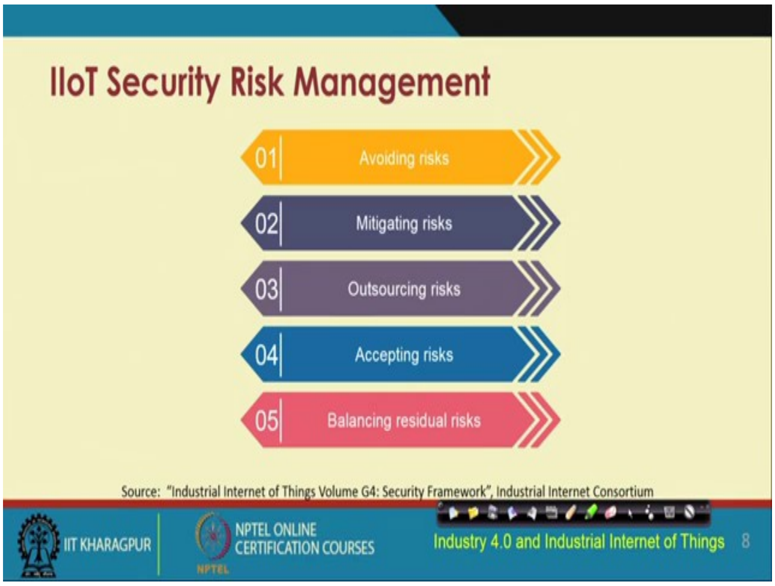
So, IT trustworthiness will take into consideration issues of privacy, issues of security, issues of reliability and to some extent resilience. On the other hand, if you are talking about OT trustworthiness, the main issues of concern are safety, device safety, machine safety and so on. Resilience is more important over here, and reliability; to some extent security is also important.

So, these are the issues of concern if we are talking about isolated IT systems and their trustworthiness and these are the issues of concern if we are talking about isolated OT systems and their trustworthiness. So, what is required in an IIoT scenario, we have to converge these two. So, the convergence of IT with OT has to happen.

So, for this basically we need to come up with an integrated set of requirements which will consider privacy, which will consider safety, which will consider security, which will consider reliability and resilience everything together. So, we have to come up with a trust model catering to all these requirements. So, as to make the system robust from different types of attacks; any kind of human or external machinery errors, different system faults and disruptions from environment. So, these are different considerations. So, now, we have also seen that cloud integrated IIoT solutions are very popular nowadays.

So, when you are talking about cloud; cloud is typically a third party service. Now whenever you are talking about a third party service, you also need to consider, you have to extend your existing trust boundaries to include the security and privacy issues that are existing with those third party services and you also have to safeguard the control systems in your IIoT from the incoming cloud information flow. Because it should not happen that there is some sneaking in that happens through the cloud due to some cloud vulnerability and there is some attack on the industrial machinery that is supposed to operate properly.

(Refer Slide Time: 21:19)



IIoT Security Risk Management

01 Avoiding risks

02 Mitigating risks

03 Outsourcing risks

04 Accepting risks

05 Balancing residual risks

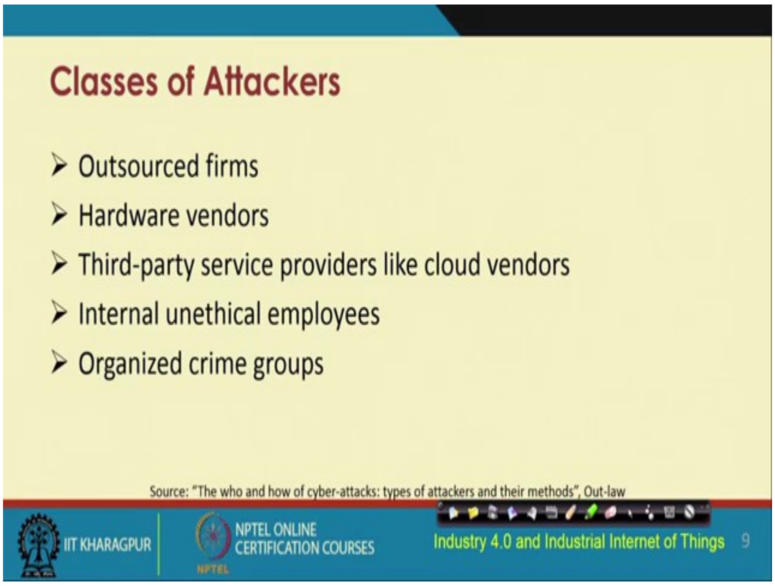
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 8

So, IIoT security risks will have to be managed. So, for this many management there are these different considerations that will have to be made. Number 1 is it is required to avoid the risks; second is IT is required to mitigate the risks that will be still existing. First of all you avoid; second is whatever comes in you will have to mitigate and sometimes for risk management it is required to outsource the risks; outsourced to a third party and may be typically with at some cost right.

So, you have to pay some money to the third body in the form of insurance or something like that and that is how you basically outsource the risk to some third party. Then the fourth one is that accepting the risks. So, you know after doing all of these things, there will still be some risks that will be there and one has to accept those risks and not just accepting the risks, but those residual risks that will be there, somehow you will have to moderate those risk; you have to balance out those residual risks. So, this is this overall 5 step security risk management that is applicable for IIoT.

(Refer Slide Time: 22:32)



Classes of Attackers

- Outsourced firms
- Hardware vendors
- Third-party service providers like cloud vendors
- Internal unethical employees
- Organized crime groups

Source: "The who and how of cyber-attacks: types of attackers and their methods", Out-law

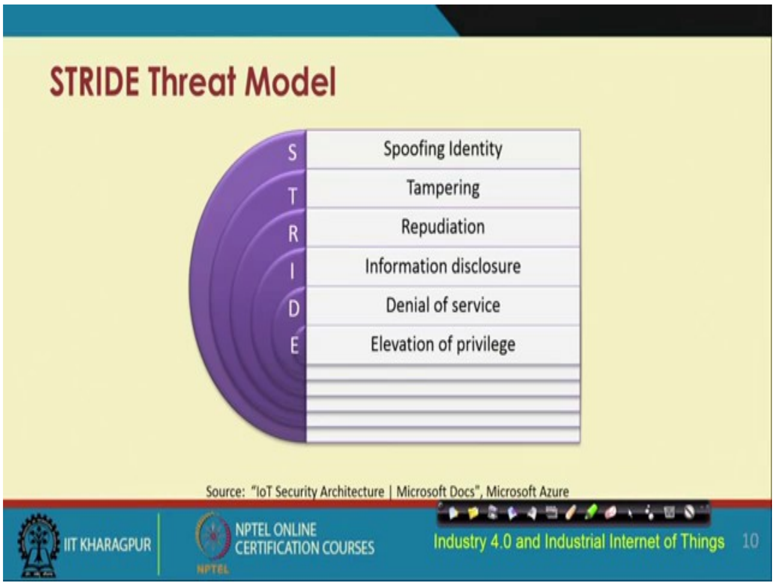
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Internet of Things
9

So, there are different types of attacks that are possible; different types of attackers that would be possible. IIoT basically scenarios, will involve outsourced third parties. So, those outsourced firms will be vulnerable points through which different attacks might be launched. So, outsourced firms might also pose as attackers directly or indirectly due to the vulnerabilities that might be existing in them or the vulnerabilities that arise due to the integration of those third party services to the services that are being offered in the mainstream.

Second is the hardware vendors. So, there are different hardware that are procured and are being used in IIoT. Those individual isolated systems might also have different vulnerabilities which might be points for entry for the attackers. Third-party service providers like cloud vendors would also be the attackers and internal unethical employees.

So, basically employees from within the organization who practices or adopts unethical practices, they might also be the attackers. So, these are basically the attackers from within the organization. And the last one is the organized crime groups, who intentionally want to launch different types of attacks on these IIoT systems.

(Refer Slide Time: 24:12)



STRIDE Threat Model

S	Spoofing Identity
T	Tampering
R	Repudiation
I	Information disclosure
D	Denial of service
E	Elevation of privilege

Source: "IoT Security Architecture | Microsoft Docs", Microsoft Azure

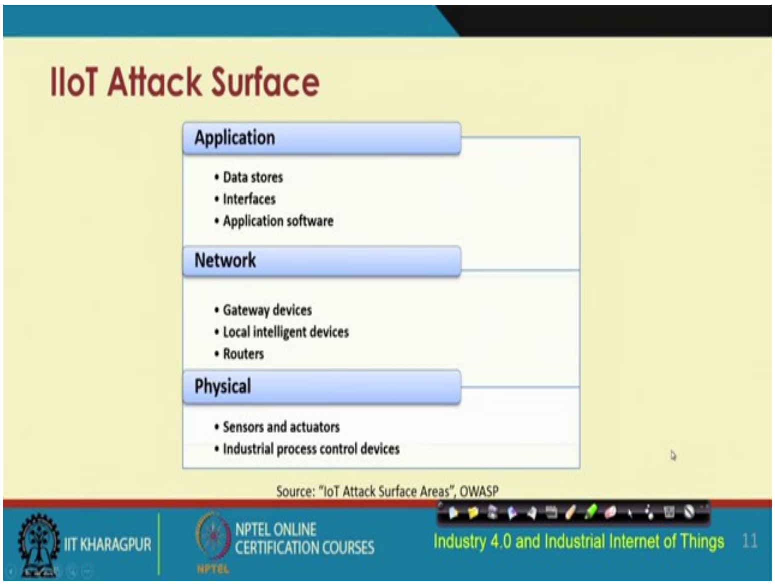
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Internet of Things
10

So, this is threat model and these different aspects of the threat model. So, STRIDE is the threat model. So, S stands for spoofing identity. So, basically somebody will be trying to act like a genuine user and we will try to spoof in. So, that is the spoofing identity. So, identity of a genuine user will be somehow hacked and will be somebody will be trying to pose as a legitimate user that is the spoofing identity.

Second is tampering; tampering means tampering with the system, tampering with the data to hurt the integrity of the data, to hurt the integrity of the system. Repudiation means like basically that you send the data and later on, you deny that you have sent the data. So, you know preventing from reputation is very important. So, you send the data, but later on you pose like as if you have not done anything, you have not sent the data, so, that is repudiation.

Information disclosure is well understood and denial of service; denial of service means like you send so many requests to a computational resource that after some time that resource is over flooded with the limited capacity it has and that is how basically the future requests that are sent to that particular computational facility, those are going to be denied. That is the denial of service. So, denial of service is a very popular form of attack and elevation of privilege is basically one tries to go beyond the privileges that have been given and try to get access to those different points of elevation.

(Refer Slide Time: 26:05)



IIoT Attack Surface

Application

- Data stores
- Interfaces
- Application software

Network

- Gateway devices
- Local intelligent devices
- Routers

Physical

- Sensors and actuators
- Industrial process control devices

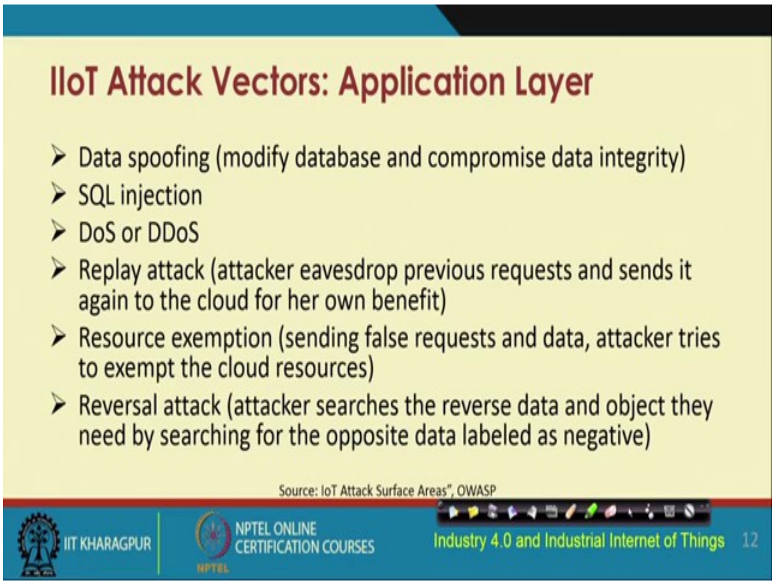
Source: "IoT Attack Surface Areas", OWASP

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 11

So, I was talking at the outset about the IIoT attack surface. IIoT attack surface is quite big, there are different points of vulnerability, points of attack and so on. At the application level data stores, interfaces, application software are there which are like different points of attack. At the network level the different gateway devices, routers, intelligent devices which are local to the network, those are different points of attack through the network and at the physical level the sensors, the actuators, the industrial process control devices, those are the different points of attacks.

So, IIoT attack surface is quite big. There are different diverse points of attack on the IIoT system due to the integration of so many different concepts, so many different technologies and particularly because they are heterogeneous and are quite diverse.

(Refer Slide Time: 27:06)



IIoT Attack Vectors: Application Layer

- Data spoofing (modify database and compromise data integrity)
- SQL injection
- DoS or DDoS
- Replay attack (attacker eavesdrop previous requests and sends it again to the cloud for her own benefit)
- Resource exemption (sending false requests and data, attacker tries to exempt the cloud resources)
- Reversal attack (attacker searches the reverse data and object they need by searching for the opposite data labeled as negative)

Source: IoT Attack Surface Areas", OWASP

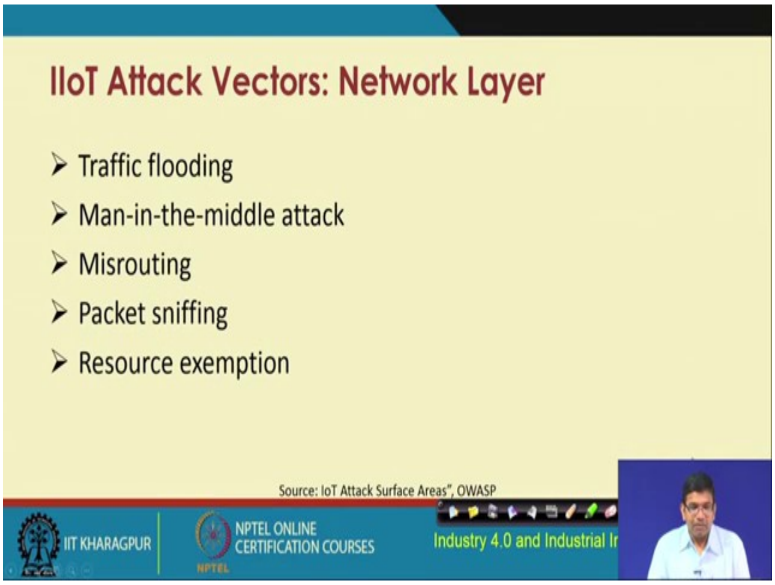
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 12

So, at the application layer, these attack vectors could be launching data spoofing attack; wherein basically the existing database the data that is resident in the database they are going to be modified, the integrity of the data is going to be hard and so on. So, that is that data spoofing attack. SQL injection attack basically is something like you sent different SQL queries to the database and thereby you try to get in through those queries to the data that normally should not be made accessible to you. So, intelligently you try to design your SQL queries in such a way that you get access to data beyond what you are supposed to get.

DoS or DDoS; Denial of Service and Distributed Denial of Service attacks. So, DoS attack, I have already told you and distributed denial of service attack is particularly relevant for IoT scenarios, where the machines themselves, the devices themselves are distributed and not centralized in one location. Replay attack basically here the attacker eavesdrop the previous requests and sends it again to the cloud for her own benefit.

Resource exemption attack here basically false requests are sent and the attacker tries to exempt the cloud resources. So, that is the resource exemption attack. Then, reversal attack; here, the attacker searches the reverse data and object they need by searching for the opposite data that is labeled as negative. So, basically through those negative data, the attacker tries to get in and get access to the legitimate data.

(Refer Slide Time: 28:55)



IIoT Attack Vectors: Network Layer

- Traffic flooding
- Man-in-the-middle attack
- Misrouting
- Packet sniffing
- Resource exemption

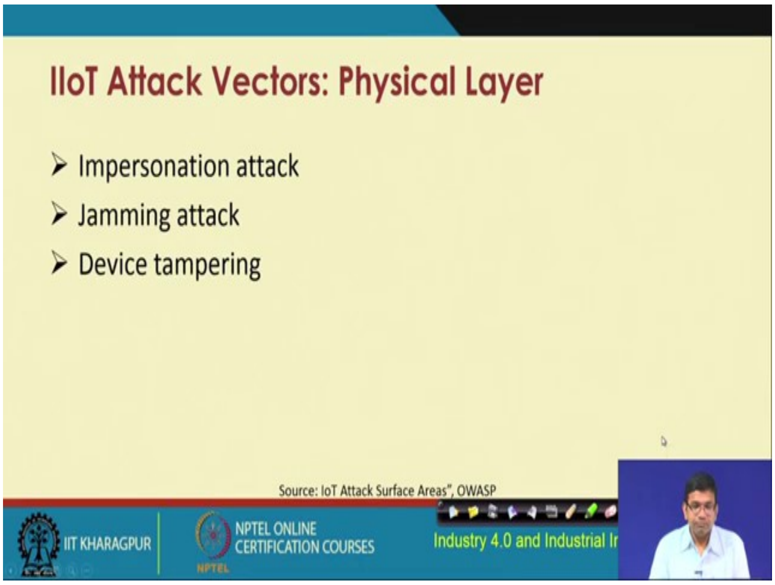
Source: IoT Attack Surface Areas", OWASP

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial I

At the network layer, we are talking about traffic flooding, man-in-the-middle attack. So, basically man-in-the-middle attack means within the channel you know the entity is going to get in and get access to or going to sniff in the packets that passing through that particular channel that is the man-in-the-middle attack. Then, misrouting; so, the data are supposed to be sent through some legitimate route; but basically what happens is they are sent through some other route through which they are not supposed to be sent originally.

Packet sniffing; basically staying in between and trying to sniff the packets that are traveling in a communication channel. So, that is the packet sniffing attack and similarly resource exemption attack at the network layer is also possible and resource exemption attack I have already mentioned in the previous slide.

(Refer Slide Time: 29:47)



IIoT Attack Vectors: Physical Layer

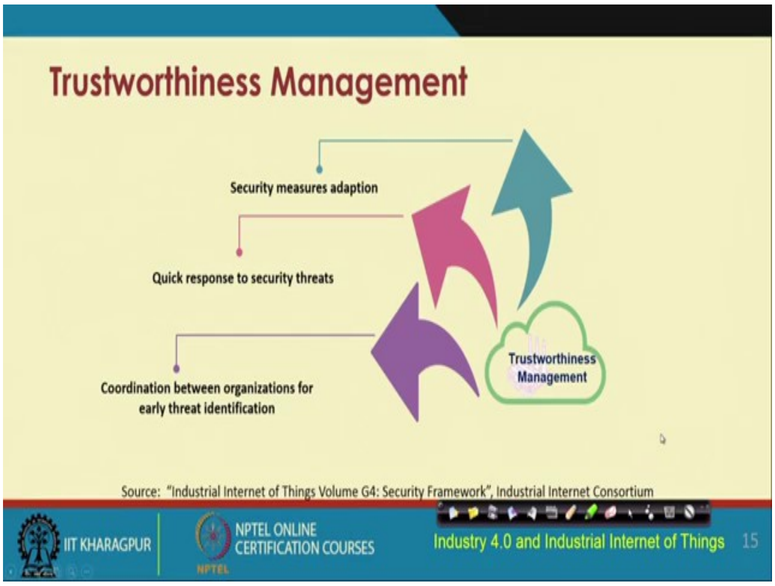
- Impersonation attack
- Jamming attack
- Device tampering

Source: IoT Attack Surface Areas", OWASP

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Ir

At the physical layer, impersonation attack, jamming attack, device tampering attack are all these different possibilities. I would like to mention to you about this jamming attack; jamming attack is particularly very prevalent and relevant and is of serious concern in IIoT not just IIoT even in IoT also. Because in IoT or IIoT we are typically talking about this resource constraint, highly constraint network environment and so on. Where, a high power jammer sending strong signals could be able to cripple the functioning of the system and the network.

(Refer Slide Time: 30:30)



Trustworthiness Management

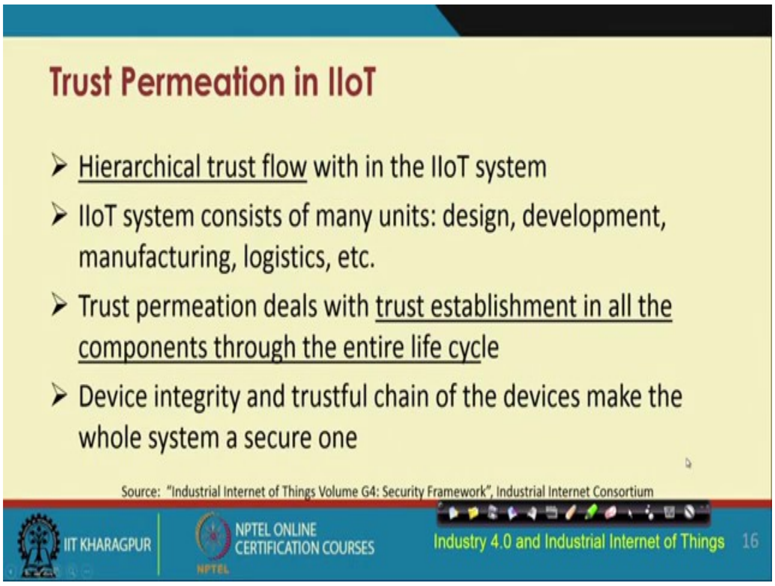
Security measures adaption
Quick response to security threats
Coordination between organizations for early threat identification
Trustworthiness Management

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
15

So, trustworthiness is very important and you have to manage the trust worthiness. For trustworthiness management, you have to consider 3 different things. Number 1 is security measures for adaption rather; then, the quick response to the security threats and the coordination between the organizations for early threat identification. These are the three different measures that will have to be taken in order to manage trustworthiness in IIoT.

(Refer Slide Time: 31:00)



Trust Permeation in IIoT

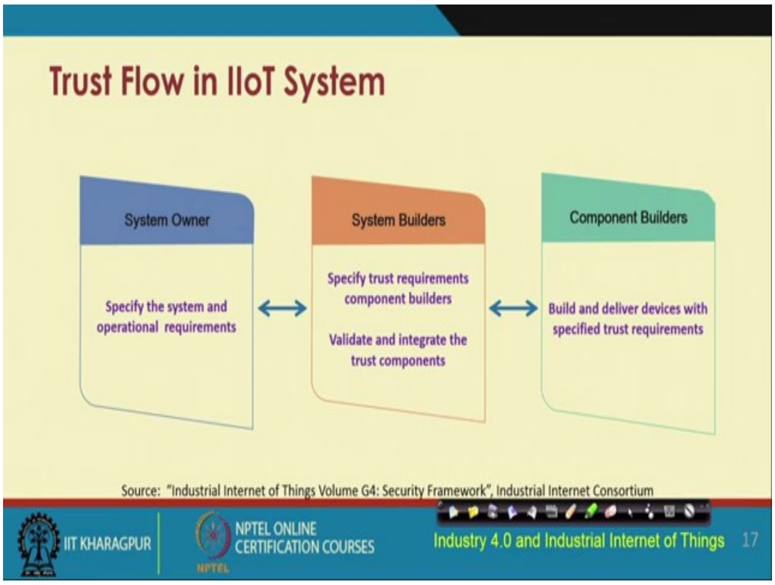
- Hierarchical trust flow with in the IIoT system
- IIoT system consists of many units: design, development, manufacturing, logistics, etc.
- Trust permeation deals with trust establishment in all the components through the entire life cycle
- Device integrity and trustful chain of the devices make the whole system a secure one

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
16

So, trust permeation in IIoT is important. We are talking about hierarchical systems in IIoT. So, in a hierarchical system, you also need to ensure that in all these different levels of hierarchy that the trust flows through these different layers of hierarchy. So, this is the hierarchical flow of trust that is important in a layered, hierarchical layered IIoT system. IoT system basically consists of many units; design, development, manufacturing logistics and so on. So, trust permeation basically deals with trust establishment in all the components through the entire lifecycle.

(Refer Slide Time: 31:43)



Trust Flow in IIoT System

System Owner

Specify the system and operational requirements

↔

System Builders

Specify trust requirements component builders

Validate and integrate the trust components

↔

Component Builders

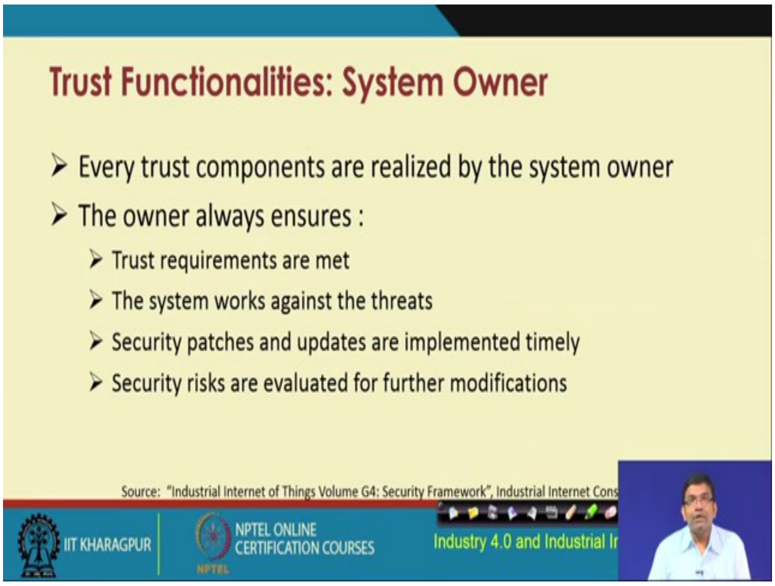
Build and deliver devices with specified trust requirements

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 17

So, in IIoT system, trust flow happens between the system owner who basically specify the system and operational requirements; through the system builders who specify the trust requirements for the component builders, and validate and integrate those trust components to the component builders who actually build and deliver the devices with the specified trust requirements. So, it’s a 3 component trust flow model that is relevant for IIoT. So, trust flow flowing through the system owner, through the system builders to the component builders. So, this is a very important consideration for trust flow in IIoT.

(Refer Slide Time: 32:31)



Trust Functionalities: System Owner

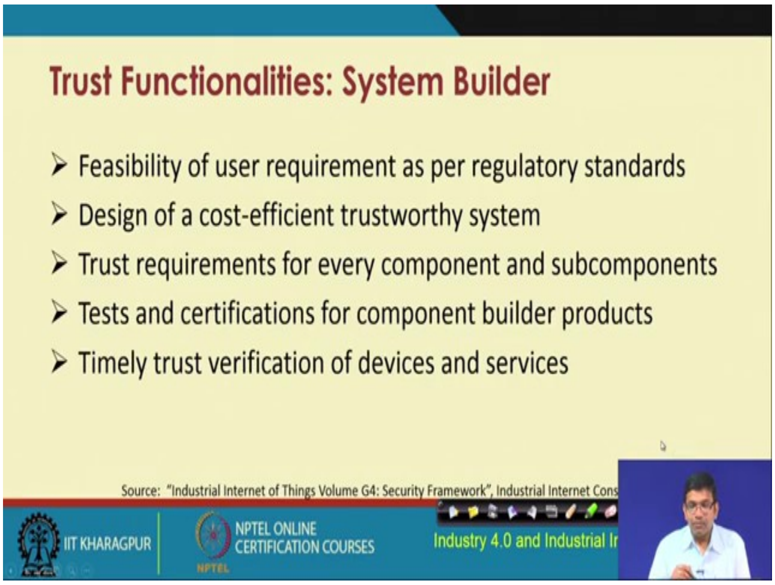
- Every trust components are realized by the system owner
- The owner always ensures :
  - Trust requirements are met
  - The system works against the threats
  - Security patches and updates are implemented timely
  - Security risks are evaluated for further modifications

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

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

So, trust functionalities at the system owner level; every trust component has to be realized by the system owner. The owner always ensures that the requirements of trust are made. The system works against different types of identified threats and the security patches and updates are implemented in a timely fashion and are also installed in the relevant parts of the system and so on. And also the security risks are evaluated for further modifications of the system coming up with different additional patches to be implemented, to be installed in the system and so on.

(Refer Slide Time: 33:11)



Trust Functionalities: System Builder

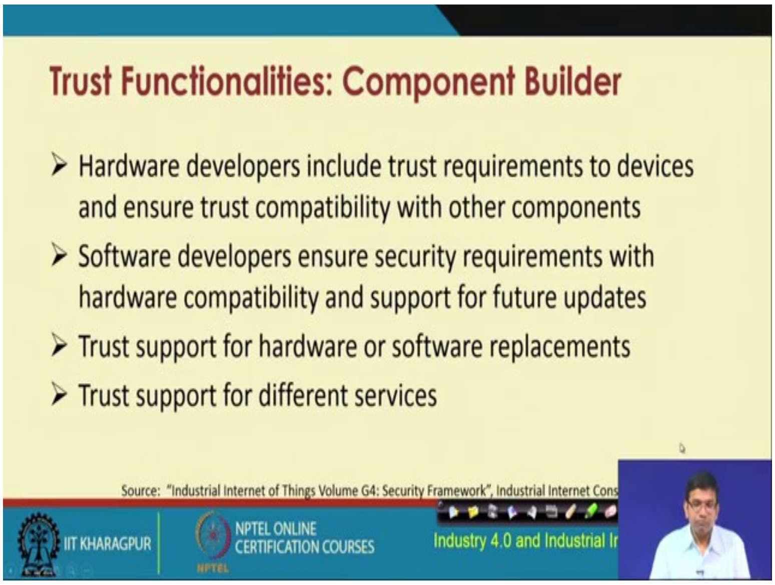
- Feasibility of user requirement as per regulatory standards
- Design of a cost-efficient trustworthy system
- Trust requirements for every component and subcomponents
- Tests and certifications for component builder products
- Timely trust verification of devices and services

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

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Ir

So, then comes the system builder; after the system owner, the system builder who is more concerned about building a cost efficient trustworthy the system. The trust requirements for every component and sub component has to be considered by the system builder and timely trust verification of the devices and services will have to be provided.

(Refer Slide Time: 33:31)



Trust Functionalities: Component Builder

- Hardware developers include trust requirements to devices and ensure trust compatibility with other components
- Software developers ensure security requirements with hardware compatibility and support for future updates
- Trust support for hardware or software replacements
- Trust support for different services

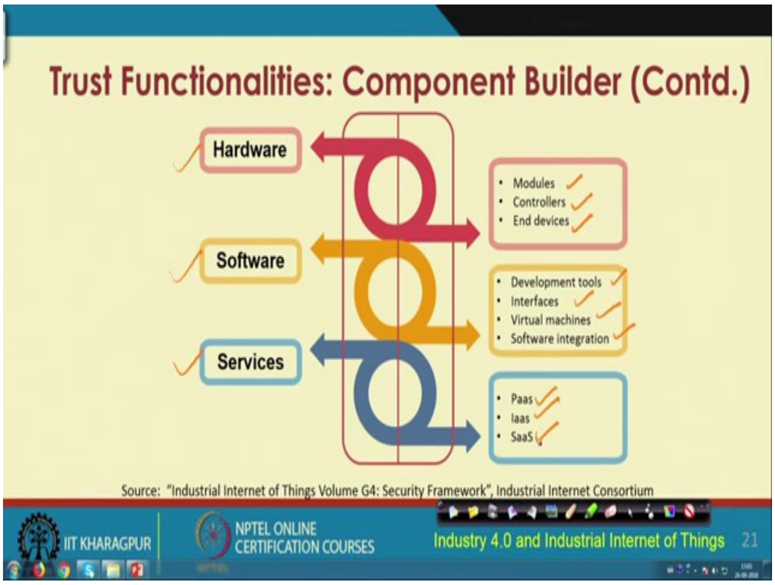
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Cons

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES
Industry 4.0 and Industrial Ir

For the component builder; component builders deal with hardware developers and they will have to ensure that the hardware that are being used are trustworthy enough and the devices, the hardware, they are compatible with the trust requirements of the different ones with whom they are going to work. The software developers will also additionally have to ensure that the security requirements with hardware compatibility and support for future updates are provided.

And the trust support for both hardware or software replacements will have to be provided by the component builder. The component builder will also have to provide trust support for different services.

(Refer Slide Time: 34:14)



Trust Functionalities: Component Builder (Contd.)

- Modules ✓
- Controllers ✓
- End devices ✓

- Development tools ✓
- Interfaces ✓
- Virtual machines ✓
- Software integration ✓

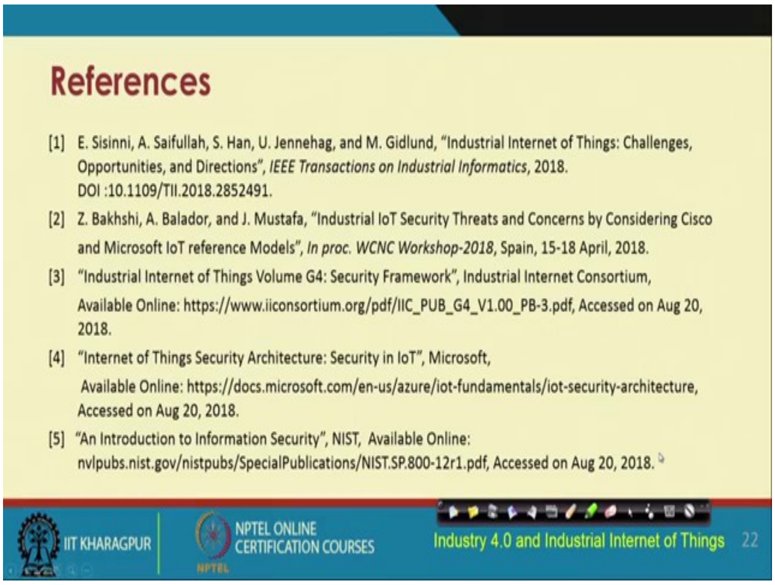
- Paas ✓
- Iaas ✓
- SaaS ✓

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

For the component builder these are the different trust functionalities; at the hardware level trust functionalities, at the software level and the services level. At the hardware level the issues of concern are the different modules, the controllers and the in devices that are being used and their corresponding trust issues and so on.

At the software level development tools, interfaces, virtual machines, software integration are of concern and their corresponding trust issues are of concern and at the services level different cloud service models for example like the platform as a service, infrastructure as a service and software as a service and their corresponding trust and not only trustworthy, trust functionalities are of prime concerned.

(Refer Slide Time: 34:03)



References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions", *IEEE Transactions on Industrial Informatics*, 2018. DOI :10.1109/TII.2018.2852491.

[2] 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.

[3] "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium, Available Online: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf, Accessed on Aug 20, 2018.

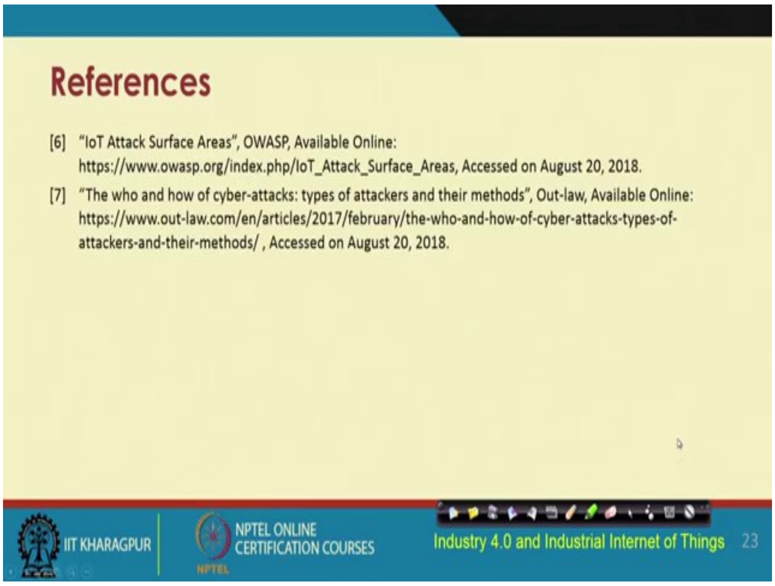
[4] "Internet of Things Security Architecture: Security in IoT", Microsoft, Available Online: https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture, Accessed on Aug 20, 2018.

[5] "An Introduction to Information Security", NIST, Available Online: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, Accessed on Aug 20, 2018.

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

So, with this we come to an end of the introduction of security for IIoT. These are some of different references that have been provided to you, for your further reading.

(Refer Slide Time: 35:15)



References

[6] "IoT Attack Surface Areas", OWASP, Available Online: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas, Accessed on August 20, 2018.

[7] "The who and how of cyber-attacks: types of attackers and their methods", Out-law, Available Online: https://www.out-law.com/en/articles/2017/february/the-who-and-how-of-cyber-attacks-types-of-attackers-and-their-methods/ , Accessed on August 20, 2018.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things 23

So, with this we come to an end.

Thank you.