

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 – 16
Industry 4.0: Cybersecurity

In this lecture, we will talk about Cybersecurity, which is a very important topic. In fact, a topic, which is of utmost concern in IoT, in general and IIoT, as well for the industries. In the context of Industry 4.0 whatever we have talked about so far, all these things would be meaningful, if people are not much concerned about the security of their systems, the physical systems, the cyber physical systems, and also the security of the data. The overall data that is collected and transmitted through the system has to be secured, the privacy of the data has to be maintained, it has to be the data, that is received from one person, it has to be trustworthy and so on. So, like this there are different allied issues as well when it comes to Cybersecurity.

Security, privacy, trust these are all interlinked entities and these are of utmost concern in the context of any system, and definitely for any internet-based system and low-powered resource constraint systems IoT, IIoT, and so on. So, that is why in the context of Industry 4.0 we need to understand the basic concepts of Cybersecurity, what are the different elements of it, and some of the different types of threats that are there in terms of securing the cyber physical systems in the industries. So, we will look at each of these in detail now.

(Refer Slide Time: 02:11)

The slide is titled "What is Cybersecurity?" in a bold, dark red font. Below the title, there are three bullet points: the first is "In computing, security consists of" followed by two sub-bullets, "Cybersecurity" and "Physical security"; the second is "Protection of internet-connected systems from cyber-attacks is known as cybersecurity." The slide has a yellow background with a blue header and footer. The footer contains logos for IIT KHARAGPUR, NPTEL ONLINE CERTIFICATION COURSES, and the text "Industry 4.0 and Industrial Internet of Things". A source attribution "Source: Techtarget.com: Cybersecurity" is visible in the bottom right of the slide area.

So, what is Cybersecurity? It is basically the security of the cyber infrastructure that is there. Basically in computing what is there is we are talking about not only the cyberspace in computing, we talk about the computing infrastructure, which includes hardware, software etc. Not only the security of the cyber infrastructure, but also the physical security, the physical security of the computing machines, the non-computing machines, and so on. So, other all kinds of machines the physical security of the machines on which the cyber infrastructure operate.

So, we are concerned about two things, one is the Cybersecurity and the physical security these are the two different things that we are primarily concerned about in the context of security.

So, protecting against what? Protecting against different attacks. Attacks will be performed by entities, which want to harm the infrastructure. In the context of industrial IoT, the fundamental premise is that the machines the systems are all interconnected. So, if they are all interconnected we have an internetwork, and we are talking about the potential of different intruders getting into the system and trying to launch some kind of attack to harm the system, the way it is operating, the different data that are being transmitted, stealing the data, overall harming the network, the hardware, the software and the physical machines themselves. So, these are all the different aspects of Cybersecurity in an internet connected world.

(Refer Slide Time: 04:20)

What is Cybersecurity?

- This protection involves protection of
 - hardware
 - software
 - data
- Enterprises use cybersecurity and physical security simultaneously against unofficial access to data centres.

Source: Techtarget.c

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

So, when we are talking about Cybersecurity we need to talk about how to protect the hardware, software and the data. So, what happens is that in the case of a cyber physical system enterprises use Cybersecurity and physical security simultaneously against unofficial access to data centers.

(Refer Slide Time: 04:59)

Protect against what?

- Unofficial change in the data
- Unofficial deletion of the data
- Uncertified access

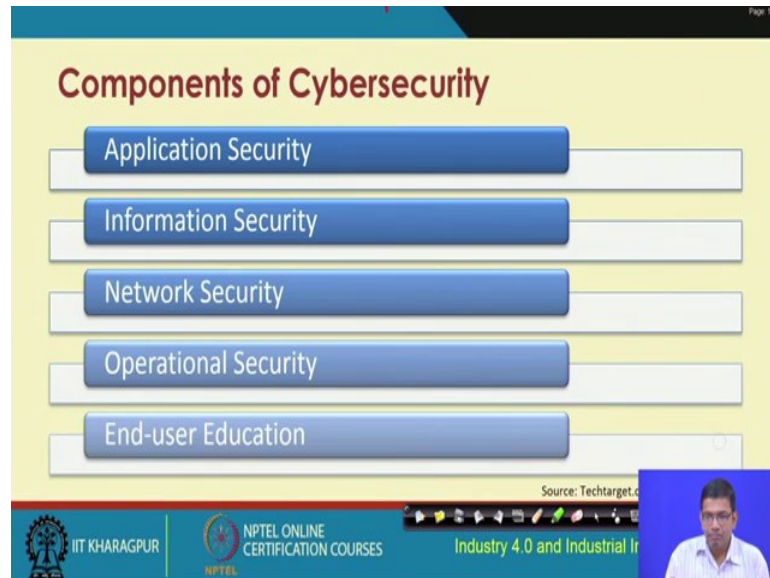
Source: Techtarget.c

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

So, what should we protect and it is protection against what? So, protection against unauthorized, unofficial change in the data; unauthorized on unofficial deletion of the

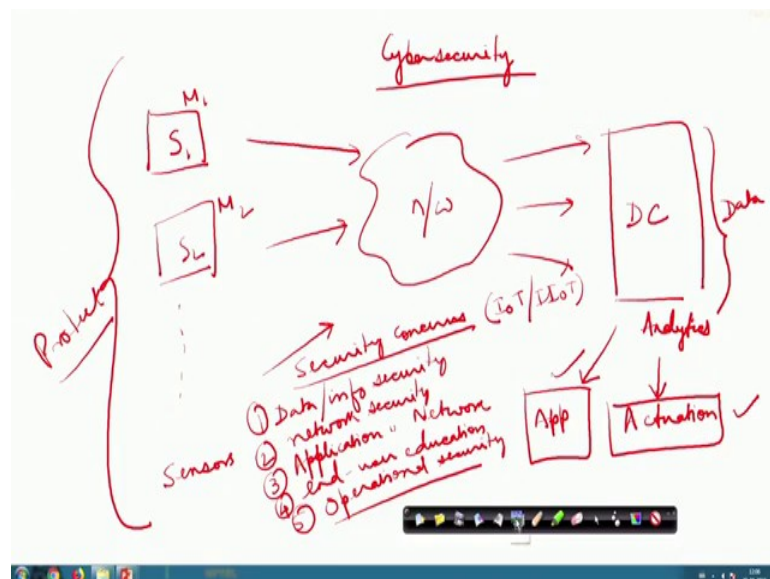
data and uncertified access. So, these are the 3 different things against which the protections will have to be made.

(Refer Slide Time: 05:27)



Let us now get into understanding and going back into the understanding about how in general the IIoT systems or IoT systems in general work. And this is something that we have already discussed in significant detailed in the past.

(Refer Slide Time: 05:32)



So, what we have? We have different physical systems on which there is some kind of sensor that is deployed. So, we have a machine 1, which has some sensor. Let us say, a

machine 2, which has some other sensor and likewise, we have different machines, which have one or more sensors. Here I have drawn a single sensor per machine, but it is also possible that a machine would have multiple different sensors.

So, these sensors what they do? We have seen this before, through some kind of a network, these machines are going to send the data to some other infrastructure. This is where we will have some data center or, some server or, something like that, which will get access to the data, which will acquire the data, and we will run different analytics on it. This is typically what is done. And based on the analytics we have also seen that some kind of actuation may be required to be implemented. So, this is typically how any IoT system and IIoT system, at a very high level, is going to work.

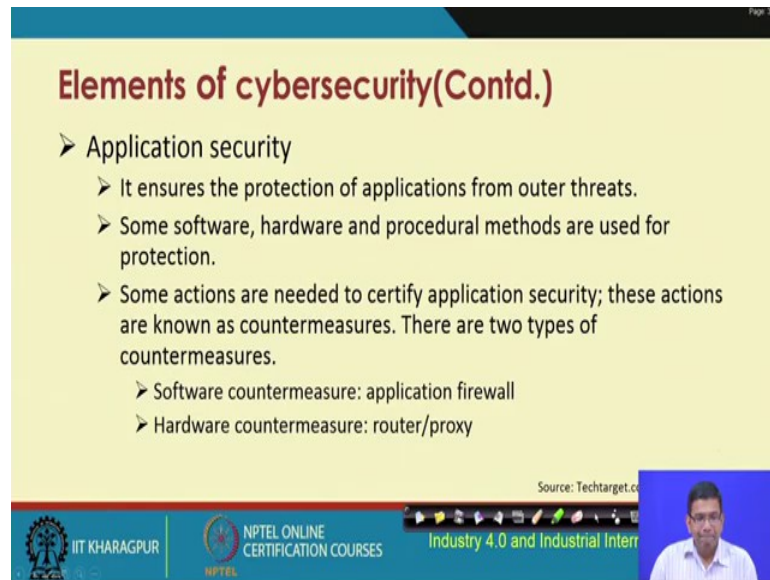
So, what are the different layers over here? We have sensors, which will sense the environment in the physical environment, in which they operate, collect the data pass it, through some network. Then this data is being sent through the network, will have to be analyzed and some actuation may be required over here. And actuation may be there or, even what might so happen is the data would be the analysis of the data, in some kind of application software.

So, now we know if we are talking about Cybersecurity. These are the things that we need to keep in mind. We have to holistically, we need to protect we need to protect this system from unauthorized, unintended access and potential harm to the system. So, how do we do it? One thing is that the data that is received from these sensors, we can we have to protect it. So, we have what? We have data or information security. Then we have to do what, this is number 1. Number 2 would be the finally, the data will have to be sent through the network. So, we need to have network or inter-network security we also need to ensure that these applications that are running on the system like these ones these also will we will need to be protected. So, we are talking about application security.

There are few other types of security concerns that will have to be there. So, the users, the end users, who are using the system or are different actors taking part in the system they will also need to be educated enough to use the system properly, and that there are some potential issues with security of the system of the infrastructure of the data and so on. We are talking about, end user education for security. Finally, overall the operations that are being carried on security of the operation, so operational security. So, we have

these as the different security concerns in the context of IoT or IIoT. These are the main components of Cybersecurity, application security, information security, data security, information or data security, network security, operational security, and end-user education.

(Refer Slide Time: 11:48)



The slide is titled "Elements of cybersecurity(Contd.)" and is part of an NPTEL online certification course. It contains a bulleted list of information about application security. The list includes: application security, its purpose (protecting applications from threats), methods used (software, hardware, procedural), and countermeasures (software like application firewalls and hardware like routers/proxies). The slide also features logos for IIT Kharagpur and NPTEL, and a small video inset of the presenter.

Elements of cybersecurity(Contd.)

- Application security
 - It ensures the protection of applications from outer threats.
 - Some software, hardware and procedural methods are used for protection.
 - Some actions are needed to certify application security; these actions are known as countermeasures. There are two types of countermeasures.
 - Software countermeasure: application firewall
 - Hardware countermeasure: router/proxy

Source: Techtarget.co

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

Application security basically ensures that you are protecting the different applications from outsider threats. So, basically some software, hardware and procedural methods could be used for this particular protection.

So, what is required is to have some kind of protection that means some kind of countermeasures at the software level as well as at the hardware level. Software level, one could use different application firewalls for this particular protection. At the hardware level, countermeasures could be used, some kind of proxy or router or similar kind of device, which will have the protection against this kind of outsider threats. So, these are the different measures that could be taken.

(Refer Slide Time: 12:40)

Page 3/2

Elements of cybersecurity(Contd.)

- Information Security
 - Information security is recognized as a subset of cybersecurity.
 - A set of strategies is known as information security, which handles some tools and policies. These policies filter the threats.
 - These strategies help maintain the availability, integrity and confidentiality of business data.

Source: Techtarget.co

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

NPTEL

Video feed of a presenter.

Information security, is basically recognized, as a subset of Cybersecurity, where we are talking about a set of strategies that should be adopted, which will have some policies associated with it, and some tools. And these policies, the tools also are supposed to filter the different threats, based on certain rules. As a consequence, implementation of all these different policies rules we are going to have, we will maintain the availability, the integrity, and the confidentiality of the data, and this is very paramount. So, information security, protecting, the availability, integrity, and confidentiality of the data, in the context of businesses and industries is very important.

(Refer Slide Time: 13:38)

Page 3/2

Elements of cybersecurity(Contd.)

- Network Security
 - Network security is a process by which we take physical and software actions for protecting the network architecture.
 - It provides protection from unofficial access, improper use, fault, deletion, demolition.
 - Create a protective platform for users and computers.
 - It combines multiple layers of defences at the edge and in the network.

Source: Cisco: Secur

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

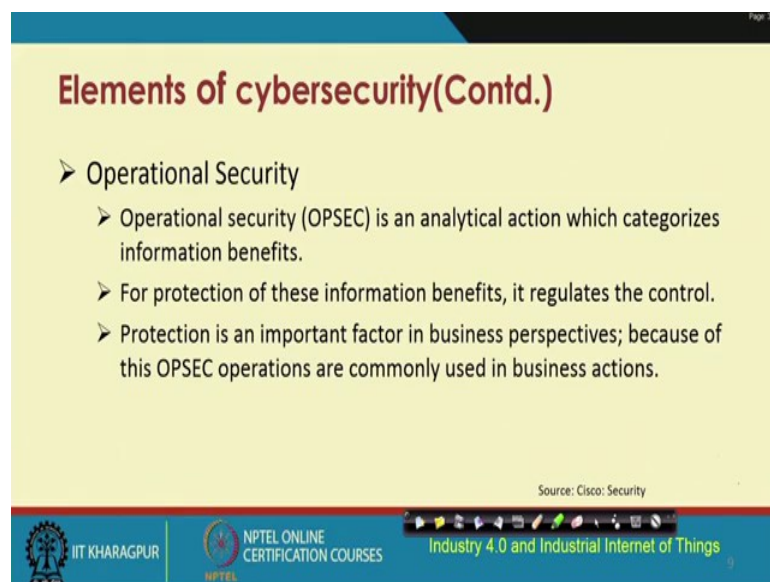
NPTEL

Video feed of a presenter.

Network security as the name says we have to protect our network from unauthorized access. So, basically the physical and software actions that would be required for protecting the network architecture those processes will have to be laid down.

Network security would provide protection from unauthorized access, improper use, fault, deletion, demolition, and so on. So, it is a protective platform, it is a protective platform that will have to be created on top of the basic network, for protecting from unauthorized users, protecting from damage unauthorized access, and damage to the existing infrastructure like computers and so on. So, network, basically is a vulnerable point through which potential attackers can get in and launch different attacks.

(Refer Slide Time: 14:43)



The slide is titled "Elements of cybersecurity(Contd.)" and is presented on a yellow background. It contains a list of bullet points under the heading "Operational Security". The text is as follows:

- Operational Security
 - Operational security (OPSEC) is an analytical action which categorizes information benefits.
 - For protection of these information benefits, it regulates the control.
 - Protection is an important factor in business perspectives; because of this OPSEC operations are commonly used in business actions.

At the bottom of the slide, there is a footer with the following information: "Source: Cisco: Security", "IIT KHARAGPUR", "NPTEL ONLINE CERTIFICATION COURSES", and "Industry 4.0 and Industrial Internet of Things".

Operation security is an analytical action, which categorizes the information benefits and for protection of these information benefits, it regulates the control. So, protection is an important factor in business perspective, because of the operational security operations the business actions are going to be protected.

(Refer Slide Time: 15:08)

Page 3/3

Elements of cybersecurity(Contd.)

- End-User education
 - End-users are the biggest security risk for an industry. They are the first to compromise the security.
 - Employees do not have all information about all the attacker, hence they can easily open the doors for the attackers.
 - As cybercrimes are increasing, it will be more important for industry to educate their employees about cyber-attacks.

Source: Cisco: Security

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

NPTEL

End-user education, end users are the biggest security risks for an industry. They are the first to be compromised in terms of security. So, employees and the end-users, typically, do not have all types of idea about the information threats and threats to the infrastructure. So, these end-users can be the vulnerable points in terms of security. They will have to be educated enough so that unintentionally they do not open the doors for the attackers. And as cyber-crimes are increasing it is more important for the industry to educate their employees about potential cyber attacks.

(Refer Slide Time: 15:58)

Page 3/3

Types of Cybersecurity threats

- Ransom-ware
 - It provides a facility to the attacker in which the attacker locks the user's computer files by using an encryption and demand some money to unlock them.
 - Example: Locky
- Malware
 - A computer program which is used to disturb the computer user, such as computer viruses, spyware etc.
 - Example: Trojan Horse

Source: Techtarget.c

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

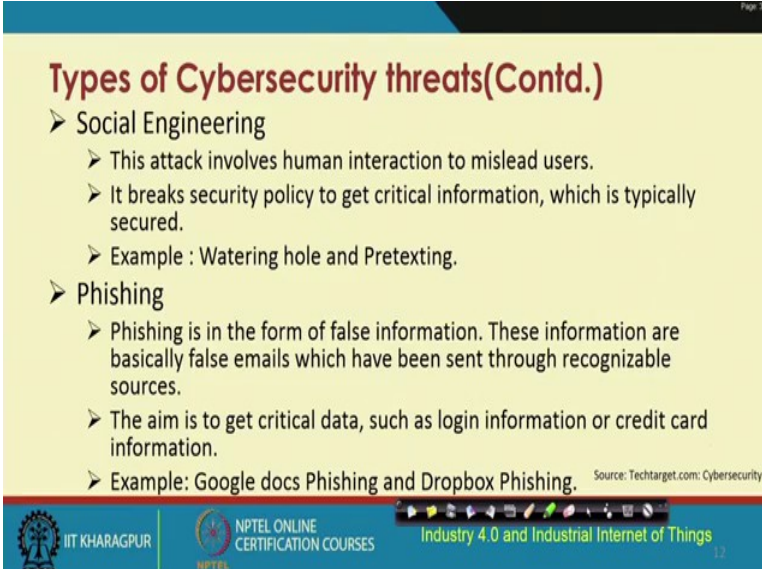
NPTEL

So, what are the different types of Cybersecurity threats? Cybersecurity threats are varied, they are of different types and understanding all of them is a herculean task, by itself.

So, ransom-ware is a very common, common type of attacker. It provides a facility to the attacker in which the attacker locks the user's computer files, by using an encryption and the attacker will demand some money in order for them to lock the system to be further used by the legitimate users. They will lock the system from being used. One of the examples of this type of attack is the Locky, a ransom-ware type of attack.

Malware, and as this name suggests it is a computer program, which is used to disturb the computer user such as different computer viruses, spyware and so on. And spyware computer viruses we are already familiar with like Trojan Horse. So, these are the ones that basically they disrupt the normal operation of the computers and the cyber infrastructure, and they will not basically protect or they may not disturb completely, they may not disrupt the functioning of the system completely, but at certain operations, certain procedures, certain processes, might be disrupted and that will basically disturb the regular user from performing their legitimate tasks.

(Refer Slide Time: 18:00)



The slide is titled "Types of Cybersecurity threats(Contd.)" and is presented on a yellow background with a blue header and footer. It lists two types of threats: Social Engineering and Phishing. Social Engineering is described as involving human interaction to mislead users, breaking security policy to get critical information, with examples like Watering hole and Pretexting. Phishing is described as the form of false information, such as false emails, with the aim of getting critical data like login information or credit card information, and examples like Google docs Phishing and Dropbox Phishing. The slide includes logos for IIT KHARAGPUR, NPTEL ONLINE CERTIFICATION COURSES, and Industry 4.0 and Industrial Internet of Things. A source citation "Source: Techtargget.com: Cybersecurity" is also present.

Types of Cybersecurity threats(Contd.)

- Social Engineering
 - This attack involves human interaction to mislead users.
 - It breaks security policy to get critical information, which is typically secured.
 - Example : Watering hole and Pretexting.
- Phishing
 - Phishing is in the form of false information. These information are basically false emails which have been sent through recognizable sources.
 - The aim is to get critical data, such as login information or credit card information.
 - Example: Google docs Phishing and Dropbox Phishing.

Source: Techtargget.com: Cybersecurity

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

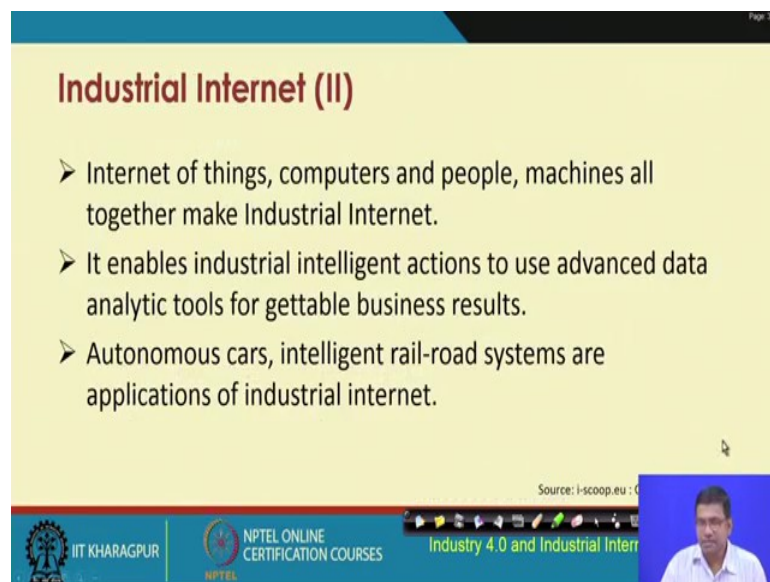
Social engineering, this attack involves human interaction to mislead the users. Social engineering breaks the security policy to get critical information, which is typically

already secured. So, security policies are basically broken in this kind of social engineering Cybersecurity attack. So, examples are watering hole and pretexting.

Phishing is a form of attack, where false information is sent, and these information are basically in the form of sending false emails, which have been sent through recognizable sources and the aim is to get critical data such as login information or credit card information. So, phishing attacks, who are already in the emails, which are basically phishing attacks, which will ask you for credit card information, the login information saying that the email account is going to be invalid after a few days. These kind of attacks are going to be made and will basically, if somebody is not already educated about the potential threats from these kind of attacks, the user would supply the credit card information that is requested or supply the username and password to the attacker unintentionally and that way they will lose access to their system.

So, example of this thing is Google docs phishing and Dropbox phishing attacks and they are like these different types of other phishing attacks that are possible on different systems.

(Refer Slide Time: 19:42)



The slide is titled "Industrial Internet (II)" in red text. It contains three bullet points: "Internet of things, computers and people, machines all together make Industrial Internet.", "It enables industrial intelligent actions to use advanced data analytic tools for gettable business results.", and "Autonomous cars, intelligent rail-road systems are applications of industrial internet." The slide is part of a presentation from IIT Kharagpur, NPTEL Online Certification Courses, and is titled "Industry 4.0 and Industrial Intern". A small video inset in the bottom right corner shows a man speaking. The source is cited as "Source: i-scoop.eu : 6".

Now, let us go back to the industrial internet. So, when we are talking about industrial internet, we are talking about typically use of different things sensors, actuators, internet of things. So, internet of things computers, people, machines all together are different participate participants in the development of the industrial internet. The industrial

internet enables the industrial intelligent actions to use advanced data analytic tools for getting desired business results. Examples of industrial internet are basically outcomes such as having autonomous cars, and intelligent railroad systems.

(Refer Slide Time: 20:37)

The slide is titled "Why IIoT Security Standards is required?" and contains the following content:

- Industries will need to use diverse systems and equipment but everything will be integrated on smart factory floor.
- Legacy systems must be brought under implementation.
- Every weak line in the chain puts whole factory at risk.
- Leaving security at the hands of individual IIoT implementers is dangerous.

Source: i-scoop.eu : Cybersecurity-IIoT

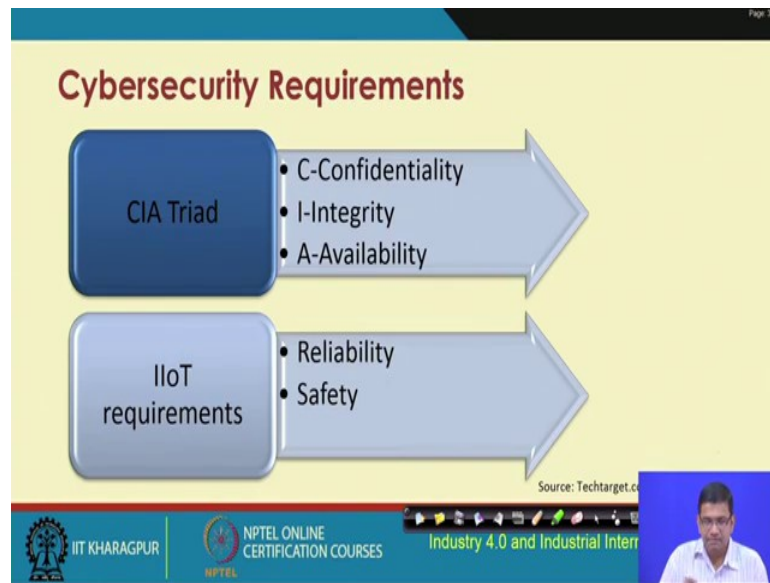
Footer: IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES | Industry 4.0 and Industrial Internet of Things

So, for IIoT securities security issues are important and securing the standards for securing the systems are required to be designed. So, industries will need to use diverse systems and equipment but everything will be integrated on the smart factory platform.

When we are talking about industries certain things are legacy, which have been there for decades in the industry whereas, certain systems might be the recent ones, which have already been built to be secured. So, legacy systems particularly should be taken seriously in the in the in the process of implementation because these systems might be the points of vulnerability for launching different attacks, for the attackers to get into the system the legacy systems could be the ones, which could be the vulnerable points because those days earlier days security was not well understood systems were designed not to be always secured and so on.

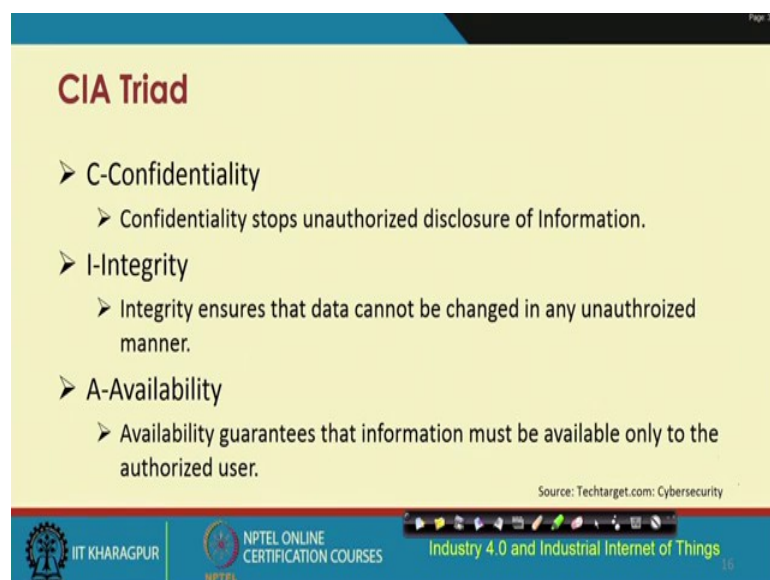
So, there are some potential possibilities of leaving some points in those systems, which basically the attackers can launch the attacks. So, every week line in the production system, in the industrial process puts the whole factory at risk. So, living security at the hands of the individual IIoT implementers is consequently dangerous.

(Refer Slide Time: 22:15)



So, what are the Cybersecurity requirements in the context of a IIoT and Industry 4.0? The first one is the fundamental one, which is not only applicable for IIoT but for any computing system, this is known as the CIA Triad, C stands for confidentiality, I stands for integrity and A stands for availability. And the second set of requirements are basically the IIoT specific requirements, which talk about reliability and safety.

(Refer Slide Time: 22:50)



So, confidentiality in the CIA Triad stops from unauthorized disclosure of information. I stands for integrity, which ensures that the data cannot be changed in any unauthorized

manner and A stands for availability, which guarantees that the information must be available only to the authorized user.

(Refer Slide Time: 23:12)

The slide features a yellow background with a blue header and footer. The title 'Cybersecurity: Challenge in IIoT' is in red. Two bullet points are listed. A small video inset shows a man speaking. The footer contains logos for IIT KHARAGPUR, NPTEL ONLINE CERTIFICATION COURSES, and 'Industry 4.0 and Industrial Intern'. A source credit 'Source: Cybersecurity' is also present.

Cybersecurity: Challenge in IIoT

- Cybersecurity has a major role in digital economy and it certainly is a big challenge in IIoT as well.
- In current digital transformation, capabilities such as manufacturing, logistics, shipping, healthcare and industries, which comes under the industrial internet, data breaches can occur, which increases different kinds of cybercrimes and cyber threats.

Source: Cybersecurity

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

In the context of IIoT, these are some of the challenges with respect to provisioning Cybersecurity. So, basically when we are talking about industries, we are talking about machines, where different sensors, actuators are all deployed and these nodes are all inter-network, they are all interconnected.

So, basically if you need to have such a kind of system getting some kind of a transformation that the industries will have to go through to transform from the physical systems the standalone physical systems, without these kind of infrastructure, that has been existing for years, and transforming into something that is smarter, connected machines with sensors, actuators. So, this transformation will have to take place. When this transformation is going to take place, you have to take into account all these different points of vulnerability, that can be potentially introduced through this transformation process.

So, when we talk about transformation capabilities such as manufacturing, logistics, shipping, healthcare and industries these will have to be taken in the into consideration differentially, differently in the context of industrial internet. So, what might happen is one might incur data breaches, which increases different types of cyber crimes and cyber threats because there are different types of attacks, that are possible.

(Refer Slide Time: 24:47)

The slide is titled "Cybersecurity for Industry 4.0" in a bold, dark red font. It contains four bullet points, each starting with a right-pointing arrowhead. The text is as follows:

- Traditional cybersecurity mechanisms have the characteristics- confidentiality, authenticity, integrity, non-repudiation and access-control.
- These methods provide safety in network and computer attacks.
- The new internet security deals with other attacks which are capacious and very fast.
- Some methods are required for Industry 4.0 systems which enables automatic detection to cyber-attacks.

At the bottom of the slide, there is a footer area. On the left, it features the IIT KHARAGPUR logo and the text "IIT KHARAGPUR". In the center, it says "NPTEL ONLINE CERTIFICATION COURSES" with the NPTEL logo. On the right, it says "Industry 4.0 and Industrial Interr" (partially cut off). A small video inset in the bottom right corner shows a man speaking. The source "Source: Cybersecurity" is noted in the top right of the slide content area.

Cybersecurity for Industry 4.0, which will need to be taken into consideration like that confidentiality, authenticity, integration, non-repudiation, and access-control.

We are gradually trying to make our machines and different devices in the industry smarter. So, we are introducing computers networks into our systems. So, there are some new internet security issues, that will have to be identified through this introduction and transformation process. These new security issues will have to be identified and the potential attacks that can come in we will also have to be analyzed, identified and resolved. So, different methods we will have to be devised for handling the different security issues, security threats, in the context of industry 4.0.

(Refer Slide Time: 25:49)

Cyberattack Detection: Methodologies and Algorithms

- Computational Intelligence systems (CIS)
 - An algorithm is required for CIS which combines and filters the data. This data is created by different types of events in a cyber domain.
 - Cyber-attack recognition systems deal with extensive volume of big dimensional data along with uniform advancing attack features.
 - CIS have become reasonable preferences to build new categorization algorithms for detection systems.

Source: Cybersecurity

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

Different methodologies have been proposed, different algorithms are there, one of which is for cyberattack detection. A computational intelligent system platform, which can predict if there is some kind of attack that is going to come in the future. Basically this platform implements an algorithm that is required, which combines and filters the data, and collected, will be analyzed to identify, whether there is a potential threat, that can come in the future. So, this is the CIA system that and this is how it performs.

(Refer Slide Time: 26:34)

Software-Defined Cloud Manufacturing Architecture (SDCMA)

- There are mainly three parts of SDCMA
 - Software Plane
 - Hardware Plane
 - Ensemble Intelligence Framework (EIF).
- Software plane consists of control elements (CE).
- CE are used as data tap points, since they have deep observation into the communications and activities.

Source: Cybersecurity

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

And another one is the software defined cloud manufacturing architecture. In this basically you have 3 parts of the system one is the software plane, second is the hardware plane and the third is the ensemble in intelligence framework the EIF.

The software plane basically consists of different control elements in the CEs, and each of these CEs is used as the data tap points, since they have deep observation into the communication and activities.

(Refer Slide Time: 27:07)

SDCMA(Contd.)

- In SDCMA, the streaming data is supplied to EIF by CE.
- Sensed data is detected by EIF.
- EIF is also responsible for detecting abnormality.

Source: Cybersecurity for Industry 4.0: Thames

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

In SDCMA, the streaming data is supplied to the EIF by the CE, and the sense data is detected by the EIF, and this EIF is also responsible for detecting the abnormality.

(Refer Slide Time: 27:22)

The slide is titled "References" in a bold, dark red font. It contains a list of seven references, numbered [1] through [7]. The references are as follows:

- [1] Thames L. & Schaefer D.(2017). Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing.Springer.
- [2] Li BH, Zhang L, Wang SL, Tao F, Cao JW, Jiang XD et al. (2010) Cloud manufacturing: a new service oriented networked manufacturing model. Comput Integr Manuf Syst 16(1):1-7
- [3] Ghorbani AA, Lu W, Tavallaee M.(2010) .Detection approaches. Springer, J Network Intrusion Detection and Prevention.
- [4] <https://searchsecurity.techtarget.com/definition/cybersecurity>.
- [5] <https://www.cisco.com/c/en/us/products/security/what-is-network-security.html>
- [6] <https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/cybersecurity-industrial-internet-things/>
- [7] Xu X.(2012).From cloud computing to cloud manufacturing. Rob Comput Integr Manuf 28(1):75-86.

At the bottom of the slide, there are three logos: the IIT Kharagpur logo on the left, the NPTEL Online Certification Courses logo in the center, and the text "Industry 4.0 and Industrial Internet of Things" on the right. A navigation bar with various icons is also visible at the bottom.

So, with this we come to an end of this lecture. So, what we have done is we have understood the essence that why Cybersecurity is important, the essence of it we have understood, the different elements of Cybersecurity, the possible types of attacks that might be launched on these IoT and IIoT platforms in Industry 4.0. And if you are interested to know more in-depth of these things, these are some of the references that is given in front of you and you can go through them. There are many different other references that can also be obtained through some kind of search. You will be able to get the other differences talking about different issues, different solutions and so on.

So, Cybersecurity, security for IoT security, for IIoT or nowadays, and lot of research are going on these topics. So, if you are indeed interested to deep down into each of these issues you have to basically go through these different literatures that are available and if you are also interested if you are a security researcher, you might be interested to implement them. So, for that also you need to go through these different literatures in these differences and outside in more detail.

With this we come to an end.

Thank you.