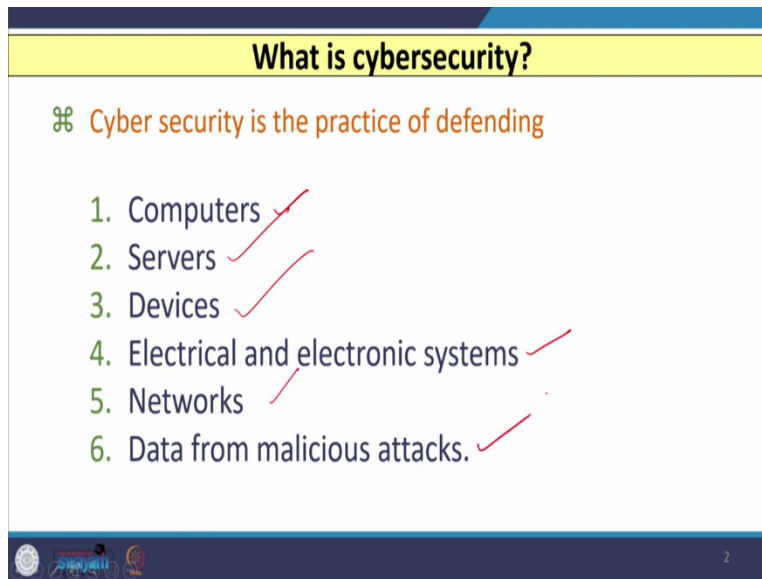


**Digital Protection of Power System**  
**Professor Bhaveshkumar Bhalja**  
**Department of Electrical Engineering**  
**Indian Institute of Technology, Roorkee**  
**Lecture 38**  
**Cyber Security Issues in Power System Network**

Hello friends. So, in this lecture, we will discuss about the Cyber Security Issues related to the Power System Network. So, let us discuss first what is cyber security.

(Refer Slide Time: 00:39)



**What is cybersecurity?**

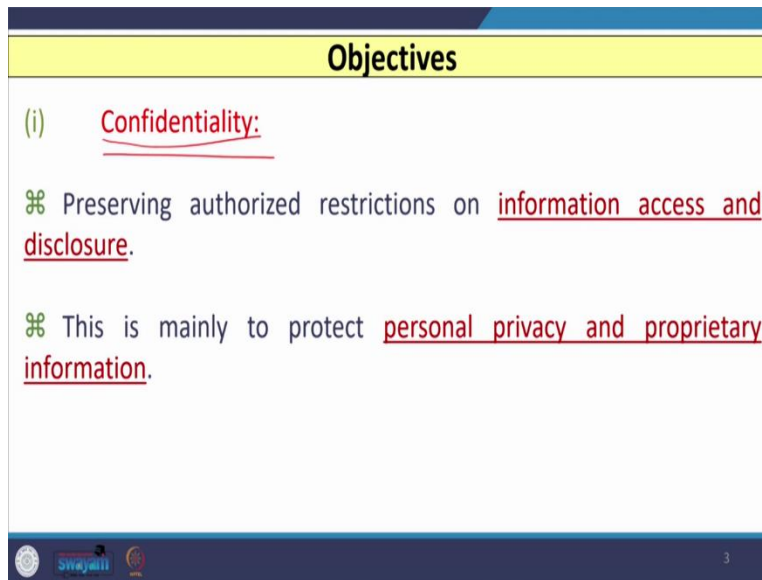
⌘ Cyber security is the practice of defending

1. Computers ✓
2. Servers ✓
3. Devices ✓
4. Electrical and electronic systems ✓
5. Networks ✓
6. Data from malicious attacks. ✓

2

So, cyber security is the practice of defending computers, the servers, devices, electrical and electronic systems, networks and data from the malicious attacks. If we have a computer or system or a server and that contains data and if any malicious attacks are there, then the practice of defending such things against any type of attack that is known as cyber security. Now, let us see what are the main objectives of cybersecurity. So, basically there are three main objectives of cyber security.

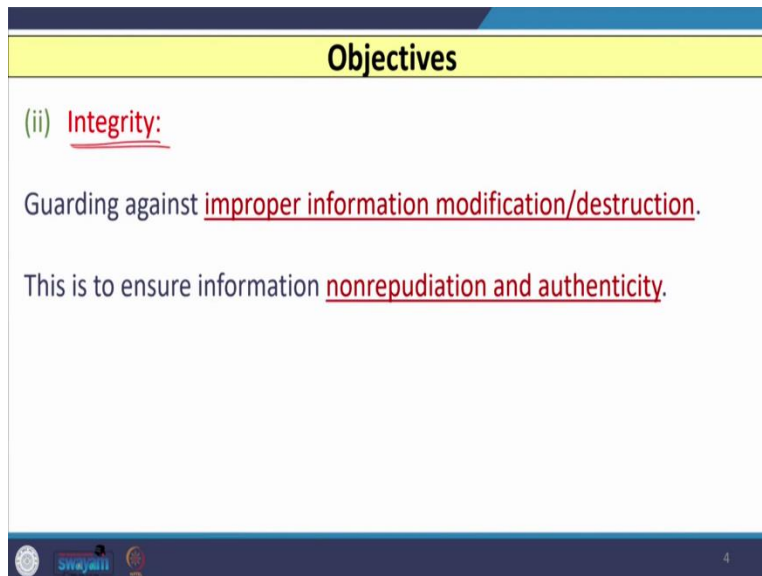
(Refer Slide Time: 01:16)



The slide is titled "Objectives" in a yellow header. It lists objective (i) as Confidentiality:. Below this, two bullet points are shown: the first is "Preserving authorized restrictions on information access and disclosure." and the second is "This is mainly to protect personal privacy and proprietary information.". The slide footer contains the Swayam logo, the number 3, and a small circular icon.

The first one is the confidentiality. So, preserving authorized restrictions on information access and disclosure are related with the confidentiality. This is mainly to protect the personal privacy and proprietary information. So, all those things are covered under the first objective, that is the confidentiality.

(Refer Slide Time: 01:39)



The slide is titled "Objectives" in a yellow header. It lists objective (ii) as Integrity:. Below this, two bullet points are shown: the first is "Guarding against improper information modification/destruction." and the second is "This is to ensure information nonrepudiation and authenticity.". The slide footer contains the Swayam logo, the number 4, and a small circular icon.

The second objective is known as the integrity. So, guarding against improper information modification or destruction, that comes under the objective of integrity. And this is to ensure information of non-repudiation and authenticity. So, integrity is related to the destruction or

modification of improper information. So, that we want to avoid and that comes under the integrity objective of the cyber security.

(Refer Slide Time: 02:13)

**Objectives**

(iii) Availability:

This ensures timely and reliable access to and use of information.

5

The third objective is related to the availability. So, in this objective, it is ensure that timely and reliable access to the information for particular users who are intended for. So, those are covered in this type of objective that is availability.

(Refer Slide Time: 02:34)

**TYPES OF CYBER ATTACKS**

<b>Types of Cybersecurity Threats</b>	1 Malware	2 Phishing	
3 Spear Phishing	4 Man in the Middle Attack	5 Denial of Service Attack	6 SQL Injection
7 Zero-day Exploit	8 Advanced Persistent Threats	9 Ransomware	10 DNS Attack

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/>

6

Now, let us discuss the what are the various types of cyber attacks possible in any network. So, as you can see the first type of attack possible that is the malware, the second type of attack is known as phishing attack, the third is known as the spear phishing attack, the fourth one is the man in the middle attack, the fifth one is the denial of service attacks and sometimes it is also related as DOS or termed as DOS, the sixth one is the SQL injection attack, the seventh one is the zero-day exploit attack, the eighth one is advanced persistent threats, the ninth one that is related to the ransomware, and tenth one that is the DNS attack. So, total 10 types of attacks are possible in any network. Now, let us discuss what is the meaning of this attack and how it is possible and on which devices a particular attack is targeted. Let us discuss one by one. So, let us start our discussion with the first one that is the malware.

(Refer Slide Time: 03:47)

The slide is titled "TYPES OF CYBER ATTACKS" in a yellow header. Below the header, the first item is "(i) Malware:". It is followed by two bullet points, each with a right-pointing arrowhead. The first bullet point is "It is done by malicious software." and the second is "It executes unauthorized actions on the victim's system.". At the bottom of the slide, there are logos for "Sri Jayanti" and "Stealth Labs", a source URL "Source: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/", and the number "7".

So, malware is done by malicious software. So, some malicious software is used to execute such attack and whenever such attack is there, it executes unauthorized action on the victim's system. So, unauthorized action is there which is not allowed for a particular system that is done in or that is carried out in this type of attack that is known as malware attack.

(Refer Slide Time: 04:14)

**TYPES OF CYBER ATTACKS**

(ii) Phishing:

- It is a type of social engineering attack.
- It used to steal user data, including login credentials and credit card numbers.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 8

The second type of attack that is known as the phishing type of attack. So, it is a type of social engineering attack and it is used to steal the user data, maybe some login credentials or credit card details, those things are still using such type of attacks and such type of attacks are very, very important in nowadays as we are moving towards digitization of each and every system.

(Refer Slide Time: 04:44)

**TYPES OF CYBER ATTACKS**

(iii) Spear phishing:

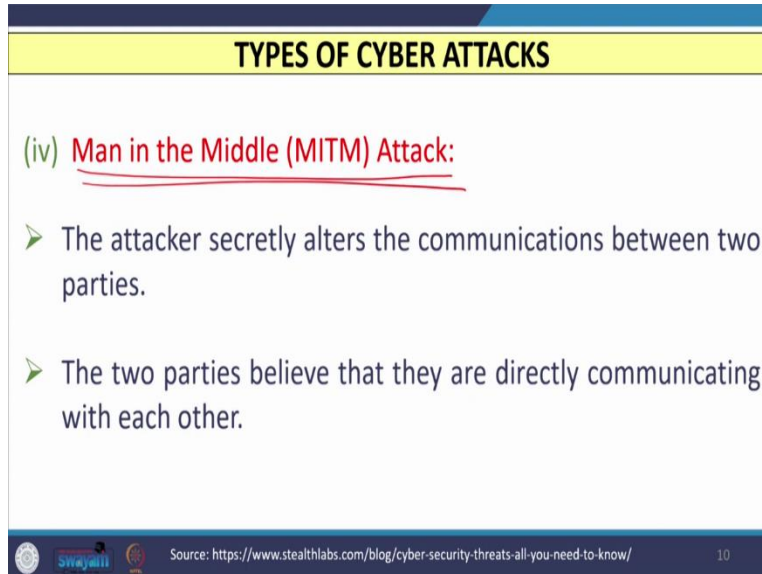
- It is an email or electronic communications scam.
- It is targeted towards a specific individual, organization or business.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 9

The third type of attack that is known as the spear phishing attack. So, spear phishing attack is an email or electronic communication scam. And in this thing, the target audience are specific

individuals, maybe one big organization or small organization or any business company, those are targeted under spear phishing type of attack.

(Refer Slide Time: 05:12)



**TYPES OF CYBER ATTACKS**

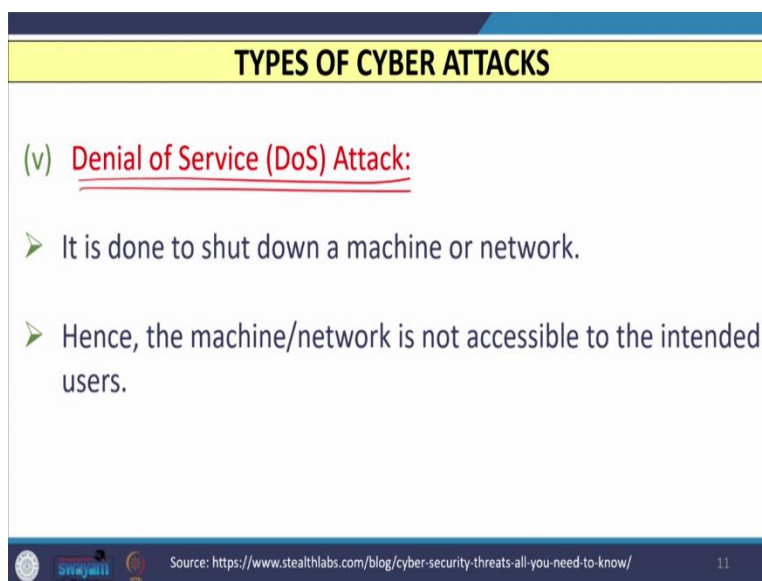
(iv) Man in the Middle (MITM) Attack:

- The attacker secretly alters the communications between two parties.
- The two parties believe that they are directly communicating with each other.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 10

The fourth type of attack is known as MITM attack that is Man In The Middle attack. So, here in this attack, the attacker secretly alter or changes the communications between the two parties. So, the two parties, they believe that they are directly communicating with each other, but actually they are not doing that is not the situation when such type of attack takes place.

(Refer Slide Time: 05:40)



**TYPES OF CYBER ATTACKS**

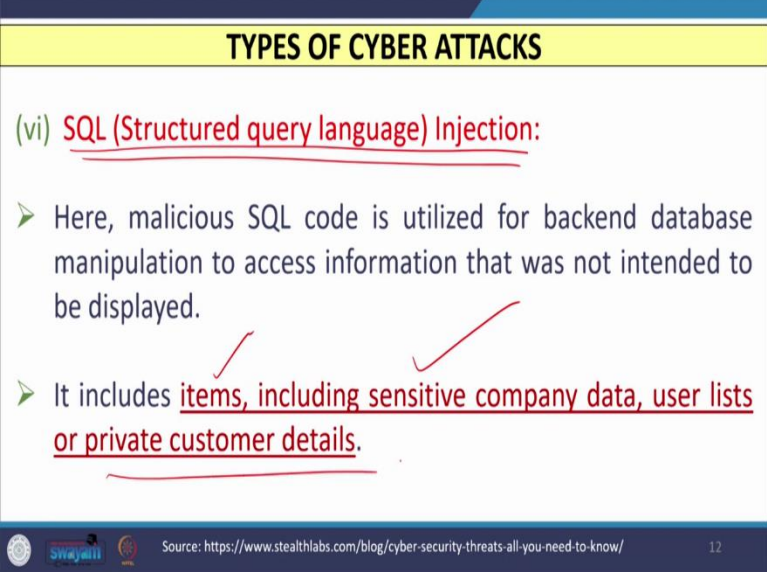
(v) Denial of Service (DoS) Attack:

- It is done to shut down a machine or network.
- Hence, the machine/network is not accessible to the intended users.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 11

The fifth type of attack is known as denial of service attack. So, in this type of attack, normally the machine or the network is targeted, and this type of attack is done to shut down a particular machine or to shut down a particular network. And hence machine or network is not accessible to the intended users, but now it is accessible to some attackers. So, this is done in this type of attack.

(Refer Slide Time: 06:06)



The slide is titled "TYPES OF CYBER ATTACKS" in a yellow header. Below the header, the text "(vi) SQL (Structured query language) Injection:" is written in red. Two bullet points follow: the first starts with a green arrow and describes the use of malicious SQL code for database manipulation; the second also starts with a green arrow and lists examples of stolen data, with red checkmarks above the words "items" and "sensitive". At the bottom, there are logos for "swayam" and "stealthlabs", a source URL, and the number "12".

**TYPES OF CYBER ATTACKS**

(vi) SQL (Structured query language) Injection:

- Here, malicious SQL code is utilized for backend database manipulation to access information that was not intended to be displayed.
- It includes items, including sensitive company data, user lists or private customer details.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 12

The next type of attack is known as SQL injection attack. So, it is SQL is nothing but the Structured Query Language. And here in this attack, some malicious SQL code is utilized for backend database manipulation to access the information that was not intended to be displayed. This type of attack is there, then that includes the items, maybe including some sensitive company data, or maybe user list or private customer details, all these things are steal when such type of attack takes place.

(Refer Slide Time: 06:46)

**TYPES OF CYBER ATTACKS**

(vii) Zero Day Exploit:

- It occurs on the same day a weakness is discovered in software.
- At that point, it's exploited before a fix becomes available from its creator.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 13

The seventh type of attack is known as zero-day exploit attack. So, this type of attack occurs on the same day when a weakness is discovered in a software. So, at that point, it is exploited before a fix that becomes available from its original creator. So, before it detected some type of attacks that is already there.

(Refer Slide Time: 07:12)

**TYPES OF CYBER ATTACKS**

(viii) Advanced Persistent Threats:

- Here, an unauthorized user gains access to a system or network.
- It remains there for an extended period of time without being detected.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 14

The eighth type of attack that is known as advanced persistent threat. So here, an unauthorized user gains an access to a system or for a particular network, and it remains there for an extended



period of time without being detected. So, the user who is using a particular detail that is not aware that some other person is also accessing the same type of data or some other information.

(Refer Slide Time: 07:42)

**TYPES OF CYBER ATTACKS**

(ix) Domain Name System (DNS) Attack:

- The DNS system is a crucial part of the internet infrastructure and it has many security holes.
- The attacker exploits vulnerabilities in the DNS.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 15

The ninth type of attack is known as DNS attack, it is Domain Name System attack. So, we know that normally DNS system is a crucial part of internet infrastructure, and it has many security holes. So, the attacker exploits vulnerabilities available in the DNS attack. And then such type of attack takes place.

(Refer Slide Time: 08:05)

**TYPES OF CYBER ATTACKS**

(x) Ransomware:

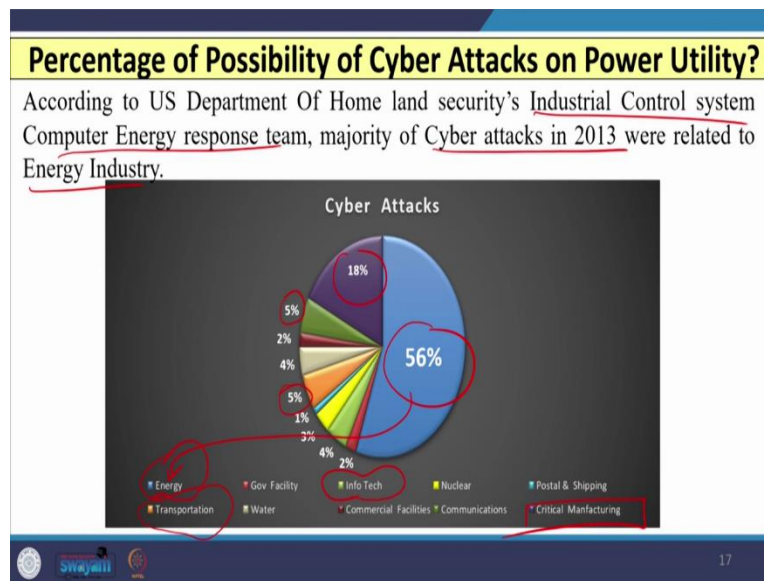
- The attacker locks and encrypts the victim's data, important files and then demands a money to unlock and decrypt the data.
- It takes advantage of human, system, network, and software vulnerabilities to infect the victim's device.
- This can be a computer, printer, smartphone, wearable, point-of-sale (POS) terminal, or other endpoint.

Source: <https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/> 16

The next attack and the last type of attack that is known as ransomware. So, here in this attack, attacker locks and encrypts the victim's data, maybe some important files are there. And then the attacker demands money to unlock, and to decrypt the same data or the information, some important files. So, this type of attack, whenever takes place, maybe some money is demanded.

And it takes the advantage of maybe human, maybe system, maybe network or software vulnerabilities to infect the victim's devices. So here, the ransomware type of attack is possible on a computer, maybe on a printer, maybe on a smartphone, maybe on a variable, maybe on a point of sale terminal or machine or any other endpoint.

(Refer Slide Time: 09:00)



Now, with this background, let us see what is the percentage possibility of cyber attack on power utility. So, one survey was carried out by the US Department of Homeland and Securities. And in that survey, this is done by Industrial Control System, Computer Energy Response Team. And here, the survey was targeted on the cyber attacks that has already occurred in 2013, related to energy industry.

And they found that out of the total attack 56 percent of the attacks that was on energy related issues. 18 percent of the attacks, that was on manufacturing type of systems or industries. Maybe you can see that 5 percent of the attacks, that is on Info Tech and maybe another 5 percent of the attack that is on transportation and remainings are there maybe 1 percent 2 percent or maybe less than 5 percent but we can say that maximum percentage of cyber attacks that is possible and that

was already there in 2013 that is on energy related industries or utilities or any other private or public power producers.

(Refer Slide Time: 10:23)

**Cyber Attacks on Power Utility**

- ⌘ Utilities play an important role as operators of critical infrastructure systems and providers of essential services.
- ⌘ Cyberattacks may damage power grid due to which widespread infrastructure failures may occur.

According to US Department Of Home land security's Industrial Control system Computer Energy response team ( ICS-CERT ) , majority of Cyber attacks in 2013 were related to Energy Industry. 18

So, utilities play an important role as an operator of critical infrastructure system and providers of essential service because utility is going to provide very important and several essential service to the customer or consumer. So, cyber attacks may damage the power grid due to which widespread infrastructure failures may occur, because utility is providing several services in this services exchange of data is there and if such type of cyber attack is there, then widespread failures may occur, and we have to prevent such type of attack on the power utility.

(Refer Slide Time: 11:05)

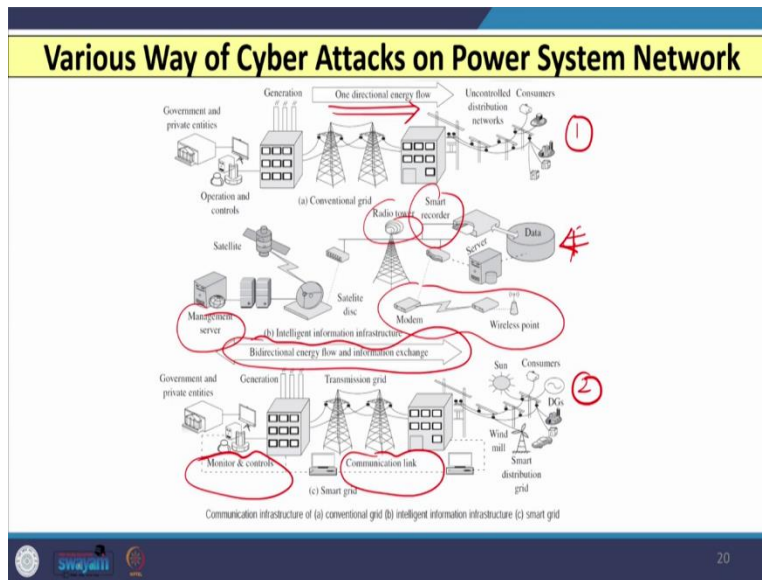
Are Cyber Attacks Possible on Power Utility?		
Cyber Attack On Iranian Nuclear Enrichment Facility in 2009. ①	• Malware was injected through USB Drive.	• Specific SCADA and PLC systems were targeted.
Cyber-attack On Ukraine Power Grid in December 2015. ②	• Compromise of corporate networks using spear-phishing emails. • Installed Black Energy 3 Malware.	• 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours.
Cyberattack in 2017	• Ransomware virus	• hitting more than 150 countries
Black out in three cities of USA in 2017.	• A series of power outages in Los Angeles, San Francisco, and New York City.	

Now, let us see whether the cyber attacks are actually there or not on power industry. So, the first cyber attack was detected or noticed on Iranian nuclear enrichment facility in 2009. And this attack was because of the malware which was injected through USB drive. And the targets are specific SCADA system that is supervisory control and data acquisition system, programmable logic control systems, these two things are targeted in this type of attack.

The second type of attack that was on Ukrainian power grid, which was occurred in 2015 December, and in this type of attack, this was done because of the installation of the black energy, three malware and the target are 30 substations were switched off because of this attack. And about 230 thousand people were left without electricity for a period of 1 to almost 6 hours.

In 2017 also, cyber attack was detected and that was because of the ransomware virus and this type of attack hit more than 150 countries. And again, in US in 2017 blackout was observed in three cities and these three cities are Los Angeles, San Francisco and New York. And this was also because of the cyber attack.

(Refer Slide Time: 12:42)

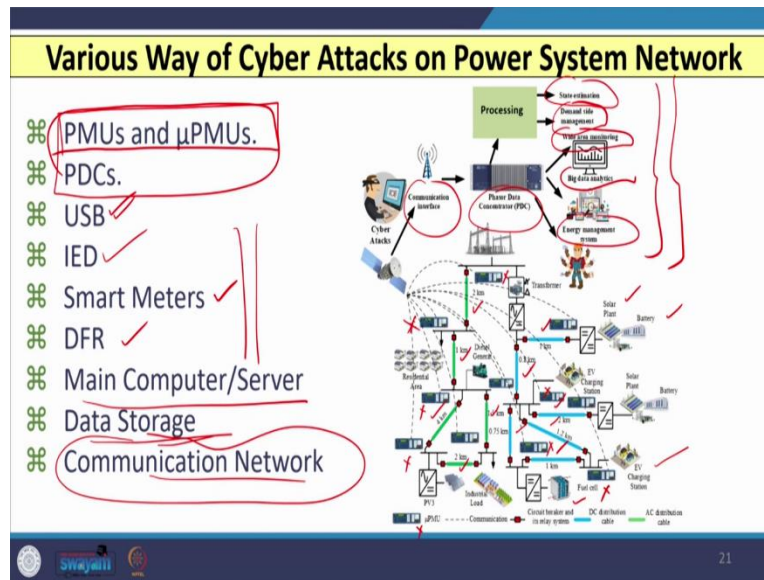


So, let us see what are the various way of cyber attacks that was possible or that is going to occur in power system network. So, here you can see that the two grids are shown. One is my conventional grid, where the flow of energy is unidirectional only from left to right. Whereas in second case, the smart grid structure that is displayed.

And here you can see the energy and information exchange flow both were the bidirectional, so it can be from left to right or it can be from right to left. And here you can see in this middle one, the intelligent information infrastructure that was shown and in that management servers are there, satellites are also used maybe for communication purpose, recorders are also there, some radio towers are there, modems and wireless points are also there.

So, wherever the direction of power flow and information exchange both are bidirectional, maybe from left to right or maybe from right to left, then in that case, we have to use communication link, we have to use modems, wireless point servers, maybe we have several monitors and controls. So, whenever such things are involved, then cyber attacks are always possible in this scenario.

(Refer Slide Time: 14:15)



Now, if I consider the devices on which cyber attacks are possible, then those devices are the phasor measurement units or synchrophasor devices for example, PMUs and micro PMUs. So, here you can see that I have shown you the hybrid AC DC micro grid, where the AC grid that is shown by this green color lines or cables or feeders and the DC grids that was shown with these blue color cables and at various points, you can see I have installed the phasor measurement units is basically micro phasor measurement units. So, these were installed at several points. And you can see we have a renewable energy sources connected at various points like solar, battery, maybe we have a fuel cell, maybe we have an EV charging station, maybe we have also some wind farms are there, diesel generators are there, and this hybrid AC DC micro grid, you can see each PMU installed, they are connected with GPS system and the information exchange that is possible and all these PMUs are sending data to the available nearest PDC that is Phasor Data Concentrator.

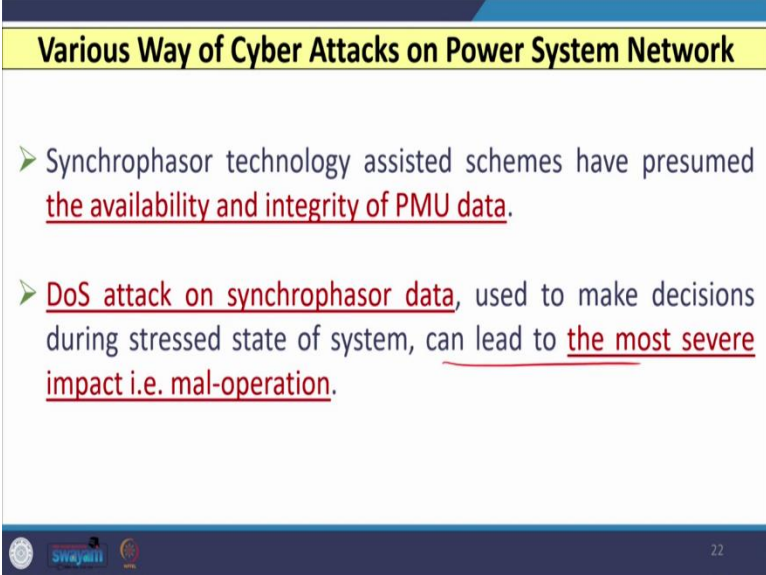
So, whenever cyber attack is there communication interface is always there and PDC is further processing the data. Maybe it can be used for state estimation. It can be also used for another application like DSM that is demand side management. Maybe it can be also used for Wide Area monitoring protection and control, or maybe it can be used for some energy management system along with these SCADA applications. So, all these applications are there.

And here you can see the information exchange is there through communication network, servers are also involved and hence, the cyber attacks are possible. So, we have synchrophasor devices

like PMUs and PDC. We are also utilizing in the substation, some USB for information exchange for taking the data for transferring the data. So, there are also cyber attacks are possible.

We are also utilizing intelligent electronic devices installed at various substations, we have also installed smart meters for billing purpose, we have also installed digital fault recorders. So, all these devices are taking data and sending to the main control center and then there the information exchange is there. So, cyber attacks are always there. We have main computers and server where data storage is there and for all these devices communication network is there. So, cyber attacks are always possible on all such devices.

(Refer Slide Time: 17:18)



**Various Way of Cyber Attacks on Power System Network**

- Synchrophasor technology assisted schemes have presumed the availability and integrity of PMU data.
- DoS attack on synchrophasor data, used to make decisions during stressed state of system, can lead to the most severe impact i.e. mal-operation.

22

Now, whenever we consider the synchrophasor technology assisted schemes, then in all these schemes, it is assumed that availability and integrity of PMU data are always there. So, if I use PMU based protection scheme, if I use PMU based monitoring scheme, then all these schemes I assumed that PMU data that is available without any attack without any problem without any issue, and there is no issue of availability and integrity of PMU data.

So, any type of attack maybe denial of service attack, maybe false data injection attack or any type of attack on such synchrophasor data, which are used to make certain decisions of the system or of the network then this can lead to severe impact on the decision making and several mal-operations are also there, if such data are impacted means PMU data's are impacted, then final decision making that is always affected.

(Refer Slide Time: 18:24)

**Cyber Attacks on Various Layer of Communication Network**

- **1) Hardware Layer:** In this layer, executing software is required for components such as PLCs and RTUs for information communication and control.
- **2) Firmware Layer:** The firmware resides between the hardware and software.
  - It includes data and instructions, which are used to control the hardware.

23

Now, let us see how the cyber attacks on various layers of communication networks that is possible. So, we have hardware layer and, in this layer, executing software is required for components such as programmable logic controllers or maybe remote terminal units for exchange of information and controlling purpose. So, here also cyber attacks are possible. The second we are using firmware layer which resides between the hardware layer and the software layer. And this includes data and instructions which are used to control the hardware. So, cyber attacks are also possible here.



(Refer Slide Time: 19:02)

**Areas Vulnerable to Cyber Attacks**

③ **Software Layer:** Control Center employs a variety of software platforms and applications. Hence, vulnerabilities in the software may range from simple coding errors to poor implementation of access control mechanisms.

24

The third type of layer that is known as software layer. So, control center employs a variety of software platforms and applications. So, vulnerabilities in software that may range from simple coding errors to maybe poor implementation of access of control mechanisms. So, these are always there and hence cyber attacks are possible on software layer also.

(Refer Slide Time: 19:31)

**Areas Vulnerable to Cyber Attacks**

④ **Network Layer:** Vulnerabilities can be introduced into the power control system network in different ways such as

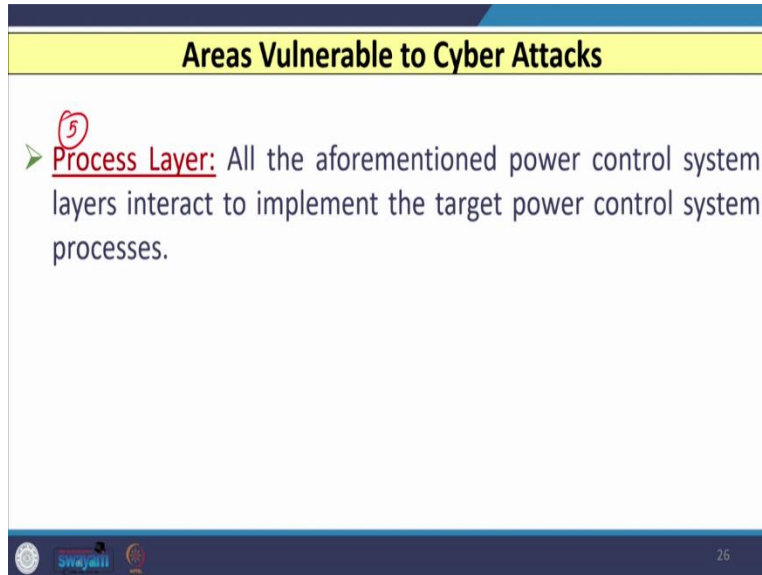
- (i) firewalls, ✓
- (ii) modems ✓
- (iii) fieldbus network
- (iv) communications systems and routers
- (v) remote access points and protocols and control network.

25

The fourth type of layer that is known as network layer and vulnerabilities can be introduced in the power system control network in many ways, like firewalls, maybe modems are also used, field bus network, we have communication systems and routers, remote access points and protocols and

control networks are also there. So, there are fair chances of the possibility of cyber attacks on network layer also.

(Refer Slide Time: 20:02)



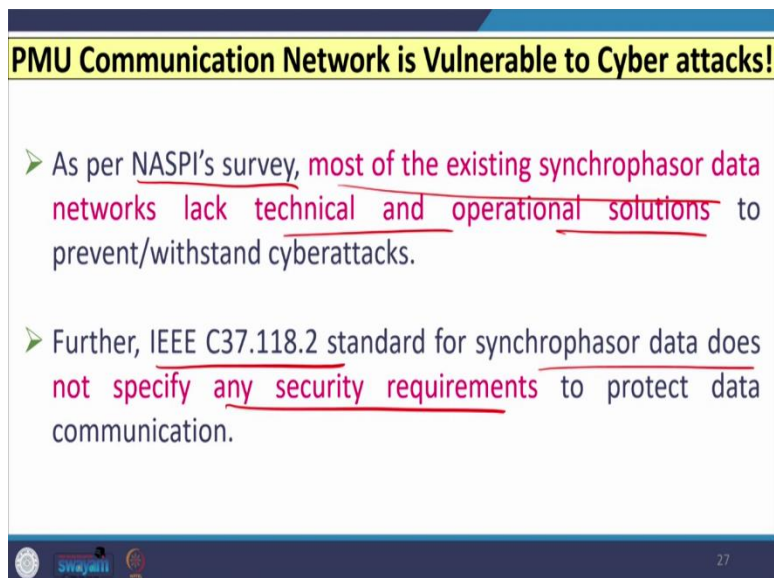
**Areas Vulnerable to Cyber Attacks**

- <sup>5</sup> Process Layer: All the aforementioned power control system layers interact to implement the target power control system processes.

26

The fifth layer is the process layer. All the aforementioned power control system layers interact to implement the target power system control process and hence the cyber attacks are inevitable in this situation also.

(Refer Slide Time: 20:16)



**PMU Communication Network is Vulnerable to Cyber attacks!**

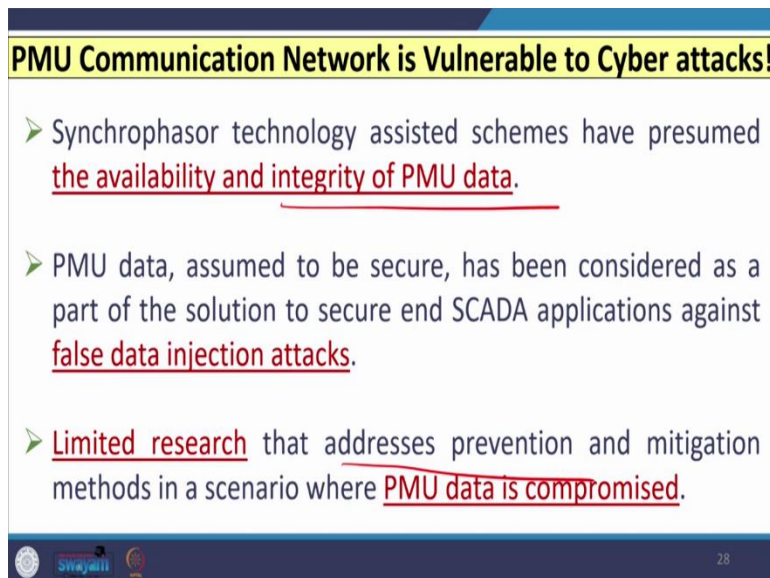
- As per NASPI's survey, most of the existing synchrophasor data networks lack technical and operational solutions to prevent/withstand cyberattacks.
- Further, IEEE C37.118.2 standard for synchrophasor data does not specify any security requirements to protect data communication.

27

Now, with this background, let us see PMU communication network is vulnerable to cyber attacks or not. So, as per the NASPI survey, so it is the national Americans Synchrophasor Initiative Survey that was carried out in 2016. And most of the existing synchrophasor data networks lack the technical and operational solutions to prevent such cyber attacks.

So, whatever PMUs we have installed, those PMUs are not capable to prevent or to withstand any cyber attacks. So, if cyber attack is there on PMUs then PMU data are definitely impacted and because of that whatever decision-making process is there that is badly affected. Moreover, IEEE C37.118.2 standard, which is meant for synchrophasor data that does not specify any security requirements to protect data communication. So, this was also not mentioned in this.

(Refer Slide Time: 21:26)



**PMU Communication Network is Vulnerable to Cyber attacks!**

- Synchrophasor technology assisted schemes have presumed the availability and integrity of PMU data.
- PMU data, assumed to be secure, has been considered as a part of the solution to secure end SCADA applications against false data injection attacks.
- Limited research that addresses prevention and mitigation methods in a scenario where PMU data is compromised.

28

So, synchrophasor technology assisted schemes help resumed that the PMU data that was already available. So, if any type of attacks are there, maybe we have denial of service attack, maybe we have false data injection attacks, then whatever applications are there, let us say for example, we are using PMUs along with SCADA system, and those applications are affected badly and limited research that is there, which has addressed the prevention and mitigation of such type of the cyber attacks when PMU data are compromised or impacted.

(Refer Slide Time: 22:06)

### Impact of Cyber Attack on PMU Data- A Case Study

- DoS attack on synchrophasor data can create missing data which can disrupt the situational awareness of the grid.
- False Data Injection (FDI) attack can force the system operator/automated end applications to take wrong decisions (which can harm the stability of the power system).

29

So, now, let us see one case study that indicates that what is the impact of cyber attack on PMU data. So, here in this case study, we have considered one of the cyber attack, that is the denial of service attack, and this attack was carried out on synchrophasor data that can create missing data, which can disrupt the situational awareness of the entire grid or network. So, false data injection attack can force the system operator or maybe automated and applications to take wrong decisions. And these decisions can harm the stability of the entire power system network.

(Refer Slide Time: 22:48)

### Impact of Cyber Attack on PMU Data- A Case Study

Attacks on PMU data can adversely impact

- Wide area monitoring protection and control applications like
  - 1. Supervisory Protection of Transmission Lines
  - 2. Adaptive Relaying.
  - 3. SCADA Applications like State estimation for which PMU data is used as redundant measurements.

30

So, wherever attacks on PMU data, that can adversely impact several applications. So, if attacks are there on PMU data, maybe because of denial of service, or maybe because of let us say, false data injection, then the packets that is to be sent or received by the PMUs, that those things were impacted. And because of that, this impact is going to affect several applications in wide area monitoring protection and control, like supervisory protection of transmission lines, maybe adaptive relaying, maybe SCADA applications like state estimation, in which PMU data is used as redundant measurements.

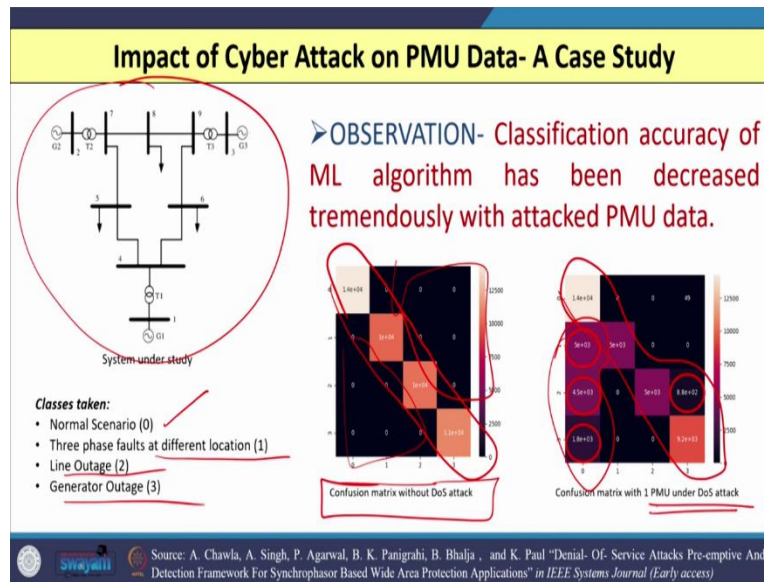
(Refer Slide Time: 23:31)

**Impact of Cyber Attack on PMU Data- A Case Study**

- An experiment was performed to study impact of cyber attack on popular Random forest classifier (used for identifying system state) using DoS Impacted PMU data.
- ML Algorithms are found to be quite effective in assisting PMU data based wide area applications like classifying system state as stressed or normal.

So, to understand this, an experiment was performed to study the impact of cyber attack on random forest classifier using denial of service type of cyber attack, and based on this attack, the PMU data that was impacted badly and then that was given to this classifier and it has been found that because of these, the accuracy of this classifier has been reduced tremendously. So, again to increase the accuracy of this classifier, the machine learning algorithms are found to be quite effective, which can easily assist the PMU data based wide area applications like classifying system state, whether the system is in normal condition or whether the system state is under stressed condition or not. So, that can be done.

(Refer Slide Time: 24:25)



So, here what we have done in this case study we have considered a nine-bus system. And on this bus system, we have considered various stages, like let us say normal scenario, maybe we have considered the three-phase fault at various locations, maybe line outages we have considered, generator outages we have considered and we have assumed that denial of service attack is already there. And PMU data that was impacted and based on that, we have used the random forest classifier.

And whenever we use random forest classifier or any classifier, then the confusion matrix is the one type of parameter which can easily detect whether the accuracy of this classifier is very high or it is not a particular or not up to the mark. So, here what we have found that whenever there was no denial of service attack on the PMU data, then you can see the diagonal elements of this confusion matrix that was accurate, and hence the accuracy of this classifier that is very high.

However, whenever the denial of service attack that was done on one PMU and because of that, that PMU data was impacted, then you can see that along with diagonal terms in confusion matrix, some non-diagonal terms are also introduced, which was not there in an earlier case, so that clearly indicates that the accuracy of this classifier that is reduced. Now, here we have assumed that DOS attack is there only on one PMU data, but if multiple PMU data's are impacted, then this accuracy that is going to be reduced more compared to the this case.

(Refer Slide Time: 26:21)

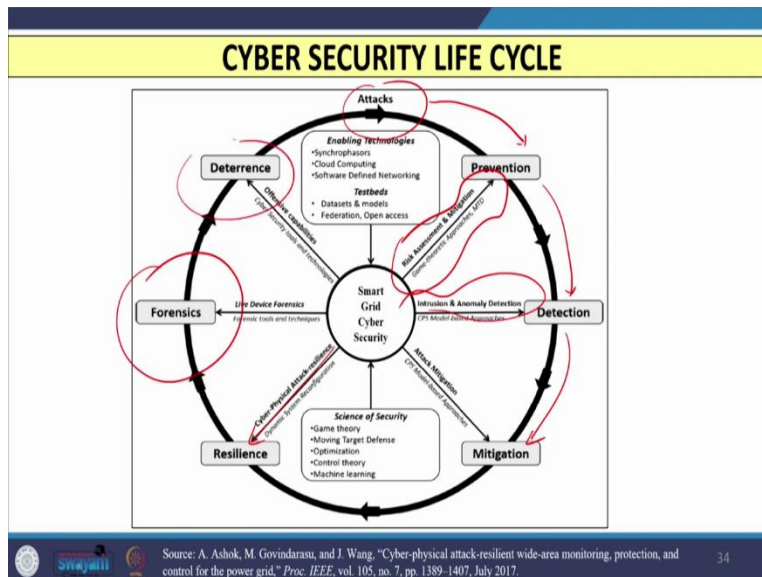
### Motivation for Cyber-Security Initiative for PMU data

- Synchrophasor technology assisted schemes have presumed the availability and integrity of PMU data.
- PMU data, assumed to be secure, has been considered as a part of the solution to secure end SCADA applications against false data injection attacks.
- Limited research that addresses prevention and mitigation methods in a scenario where PMU data is compromised.

33

So, this is going to lead the motivation for Cyber-Security Initiative related to the PMU data.

(Refer Slide Time: 26:33)



So, we know that whenever we have any initiative we have to take, then we have to consider the cyber security lifecycle. So, whenever any cyber attacks are there on any power system network, then we need some prevention technique and these prevention techniques are related to maybe game theoretic approaches or maybe some other approaches, which are related to risk assessment and mitigation. So, such type of prevention techniques we have to design.

Then we have to detect the cyber attacks. So, intrusion and anomaly detection are there based on cyber physical system models approaches. So, we can use several approaches based on game theory, maybe on optimization control theory, machine learning, maybe pattern recognition, and then we have to go for the mitigation against the cyber attacks. And once we have then we have to design our system such that it is going to improve the resiliency against the cyber attacks. Of course, forensic and the deterrence are also there, when we consider the lifecycle related to the cyber security.

(Refer Slide Time: 27:45)

The slide is titled "CYBER SECURITY INITIATIVES IN INDIA" in a yellow header. Below the title, the text "IT Act, 2000/2008 ( No. 21)" is circled in red. The main text states: "It is the primary law dealing with Cyber Crime and electronic commerce." Below this, there are two bullet points: "➤ National Critical Information Infrastructure Protection centre (NCIIPC) was created in 2014 by Gol under section 70 A of IT Act." and "➤ Two important documents of NCIIPC: 1. Guidelines for protection of critical Infrastructure (CII). 2. Framework for evaluation of Cyber Security." The bottom of the slide features logos for "Swayam" and "35".

Now, with this background, let us see that Cyber Security Initiatives that is also there in our country in India. So, in 2000 IT Act that was passed, which was amended in 2008. And this is dealing with cybercrime and electronic commerce. Based on that National Critical Information Infrastructure Protection Center was created in 2014 by government of India under Section 70A of this IT Act. This NCIIPC has two important tasks. The first is they provide guidelines for protection of critical infrastructure. And they also formed a framework for evaluation of cyber security.



(Refer Slide Time: 28:38)

**CYBER SECURITY INITIATIVES IN INDIA**

Computer Emergency response Teams (CERT-In) under section 70(B).

It responds to computer security incidents, report on vulnerabilities and promotes effective IT security practices.

ISO: 27001 (2005) for Industry:

It is a standard related to Information Security Management System.

36

Based on this the Computer Emergency Response Team that is CERT-In that was formulated under Section 70B. And the function of this CERT-In is to respond to computer security incidents, report on vulnerabilities and promotes effective IT security practices. For industry also, ISO 27001 that was given in 2005 that is also a standard related to information security management system.

(Refer Slide Time: 29:13)

**CYBER SECURITY INITIATIVES IN INDIA**

Indian Electricity Grid code Clause 4.6.5:

All utilities shall have cyber security framework to identify the critical cyber asset and protect them.

IS-16335 :2015 Power Control Systems-Security Requirement:

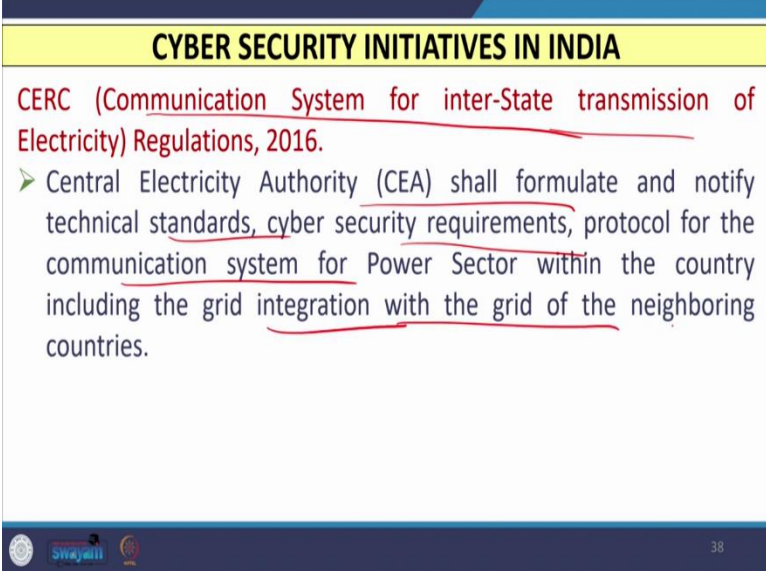
It specifies requirement for identification and protection of critical assets for all entities involved in generation, transmission, distribution and trading of electric power.

37

Indian Electricity Grid code Clause 4.6.5, that is also there, which clearly indicates that all utilities shall have cyber security framework to identify the critical cyber asset and protect them against all types of cyber attacks. IS-16335, that was given in 2015 on power control systems security

requirement. So, this specifies requirement for identification and protection of critical assets for all entities involved in generation, transmission, distribution and trading of electric power.

(Refer Slide Time: 29:56)



**CYBER SECURITY INITIATIVES IN INDIA**

**CERC (Communication System for inter-State transmission of Electricity) Regulations, 2016.**

- Central Electricity Authority (CEA) shall formulate and notify technical standards, cyber security requirements, protocol for the communication system for Power Sector within the country including the grid integration with the grid of the neighboring countries.

38

Again in 2016, Central Energy Regulatory Commission has given communication system for inter-state transmission of electricity regulations, and based on these regulations, CEA shall formulate and notify technical standards, cyber security requirements, protocols for communication system for power sector within the country including the grid integration with the grid of the neighboring countries. So, all these initiatives that was taken place in our country.

So, here in this lecture, we started our discussion with the, what is the meaning of cyber security, then we have considered the 10 different types of attacks and that is possible in any network. And after that, we have seen that if attacks are there on power utility, then what are the ways, what are the devices or based on which cyber attacks are possible that we have discussed. And then at last we have discussed if cyber attacks are there at different layers of communication, then that is also there.

And then we have discussed one case study related to the impact of PMU data because of the denial of service type of cyber attacks. And we have found that the accuracy of a particular classifier that has been reduced drastically. And then we have discussed the several initiatives related to cyber security, which was taken place in our country. Thank you.