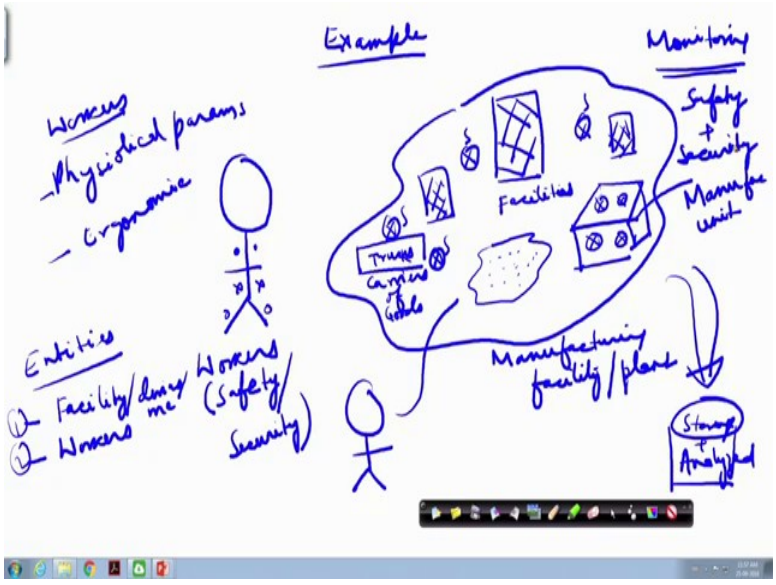
Introduction to Industry 4.0 and Industrial Internet of Things
Prof. Sudip Misra
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 54
IIOT Applications: Oil, Chemical and Pharmaceutical Industry

When we are talking about a manufacturing plant, at a very high level we are talking about 2 distinct entities one is the workers, who are working in that plant and second is basically the equipments that are there in the plant, the machineries that are there in the plant. So, securing both of these entities and ensuring their safety, safety: the physical safety and security of these and also their operations is what is very important. So, plant safety and security is very important in all modern manufacturing plants.

So, now the question is that it is important, but now in the modern world how you can make things smarter and now that we are talking about IIoT and industry 4.0 and their implementation. How you could use IIoT technologies to make smart plant safety and security monitoring and control system. So, let us look at a case study first.

(Refer Slide Time: 01:44)



So, let us say I am going to run you through an example, let us look at this particular example. Let us say that in a typical manufacturing plant this is your manufacturing plant. A typical manufacturing plant would have different facilities, different buildings, for doing different stuff, all right are going to have different facilities.

We are also going to have let us say a manufacturing unit these manufacturing units can be in multiples. So, these manufacturing units can be connected with one another so that the output from one unit goes as an input to another unit and the process continues. So, different manufacturing units might be there which again are going to be connected.

So, output from one unit goes as input to another unit, again the output from the second unit goes as input to the third and the process continues. So, you are going to have manufacturing units, you are also going to have different logistic facilities such as trucks, different trucks or the different other carriers of goods and you could have maybe some ecological facilities such as water pond etc. So, this is at a very high level how a manufacturing facility or a manufacturing plant basically is going to look like.

But one thing I have missed in this I have talked about only nonliving things, I have talked about only the goods, about the buildings, about the manufacturing units, those are the ones I have talked about, but the essential component that I have missed out so far is this worker. And we have many such workers like this who are basically doing the work over here in this manufacturing facility. So, we have these different workers and it is very important to ensure that these workers are safe and they are secured.

So, as I told you at the outset in a manufacturing facility we are talking broadly about 2 types of entities, one is the workers and second is basically the different facilities that are there, the different devices, the machinery and so on and so forth. So, these are the 2 main entities in a manufacturing unit, in a manufacturing plant.

So, you see that you have to monitor you have to ensure the safety and security of both of these. So, again our IoT sensors and other techniques, technologies that we have learnt previously could help us in doing. So, for the worker's safety we could have these workers fitted with different sensors for monitoring their physiological parameters. So, for workers we can monitor their physiological parameters, we could have different sensors to monitor their ergonomic conditions of work and likewise these different workers could be fitted with diverse types of sensors for continuously monitoring their activities, their health status, their workplace and so on.

Like this there are other sensors that could be used and could be deployed in this manufacturing facility itself, these are different other sensors, these trucks could be fitted with different sensors, these manufacturing units would comprise of different sensors,

different machinery in these units are going to be fitted with different sensors. So, these all these sensors from these nonliving things plus the sensors fitted to these living things they are going to send lot of data and as we have seen previously this data can be collected, stored and analyzed, storage plus analyzed in order to gain insights about what is going on.

So, this is the monitoring process in the manufacturing plant for ensuring the safety and security of different objects, different machinery, the workers working in them and so on and so forth. Control is also possible so, remotely it is possible this is the maintenance part that I have told you. So, we are not only monitoring these different entities, but also we can have control over certain machinery remotely. We can send some signals; some feedback signals back to the source from where the data originated to make the machine tool work in a much more efficient manner or do certain things in a certain way or know something that has already been done as a mistake. So, like these different things are possible.

So, having understood this let us now go back and try to understand the basic concepts of plant security and safety and how IIoT can help us.

(Refer Slide Time: 09:45)

So, if we are talking about safety and security, there are 3 different prongs. So, this is basically the 3 different corners of the intrusion triangle, the famous intrusion triangle, the popular intrusion triangle has three different corners, three different features that will

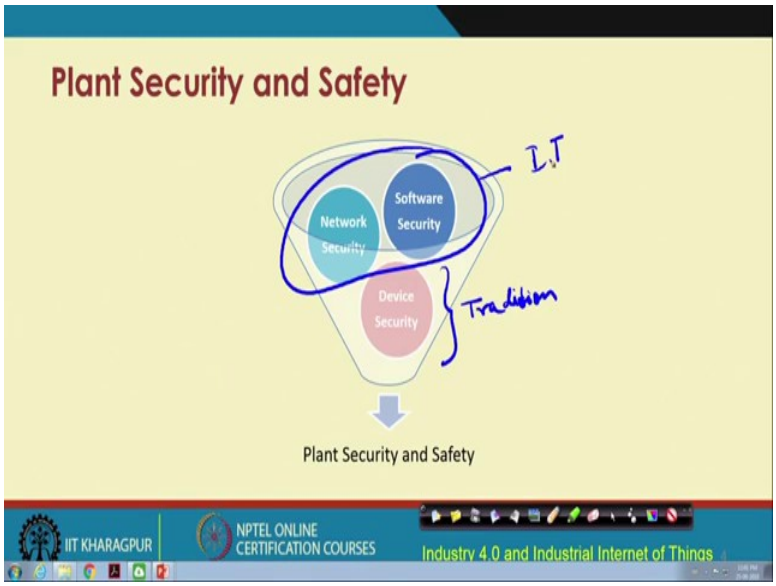
have to be taken into account. Number 1 consider that we have an intruder, so the intruder will have some kind of motive; some motive must be there for the intruder to do certain thing.

Second thing that the intruder would consider is the means how? So, motive is there, but then how the intruder is going to intrude that is the second thing, the means. And third is the opportunity, merely having the motive to intrude and nearly having the means is not going to make the intruder successful, the intruder should also have the opportunity for intrusion.

(Refer Slide Time: 11:04)

So, when we are talking about plant safety specifically as I said before 2 entities humans and plant resources, their safety, their well being is very important. It is also very important to ensure that these different machinery they do not malfunction and cause hazards to the workers that are working surrounding those machinery or along with those machinery. So, plant safety is very important.

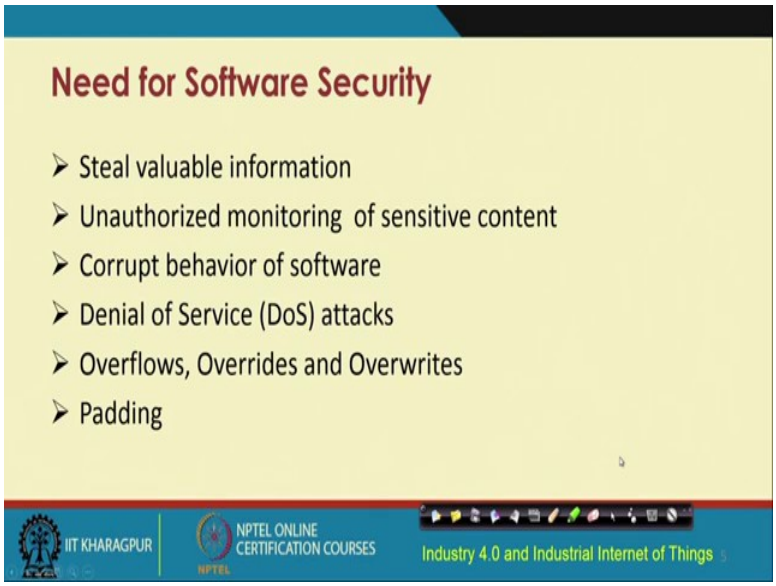
(Refer Slide Time: 11:37)



So, when we talk about security and safety in the plants these are the 3 main things that we will have to consider if we are talking about an IIoT implementation. Recall from a previous lecture what we discussed about IIoT. In IIoT we are talking about going beyond the operations, incorporation or inclusion of information technology and improving upon the operational technologies. So, IT-OT integration once again we have to relook at.

So, the security of these operational technologies would include the device security, the machine security, and the sensors that are embedded in them, their security and so on. So, all these machinery, their device security, but when you talk about IT additional things such as the network, the software, etc. also come into picture; so, network security, software security, addition additionally in addition to the device security are also important. So, we will have the device security this is from the traditional device security, and newly due to the integration of IT we have the concerns about network security and software security.

(Refer Slide Time: 13:18)

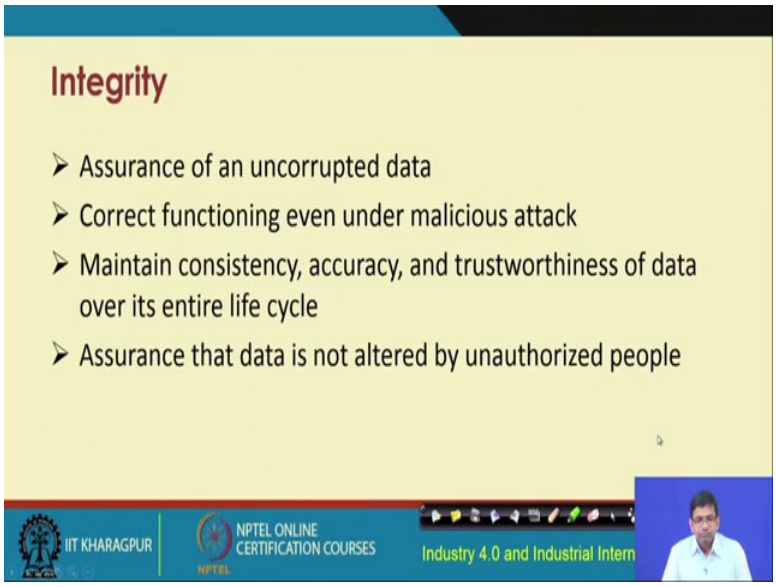


So, there is need for software security, because if the software that is implemented and is running in the automation process, if that software is not secured that can pose as a vulnerable point to steal valuable information. So, this authorized monitoring of sensitive content is important, it is important to ensure that the software does not become corrupt or does not behave corrupt, denial of service attacks should be prevented by the software. So, software security is very important.

(Refer Slide Time: 13:59)

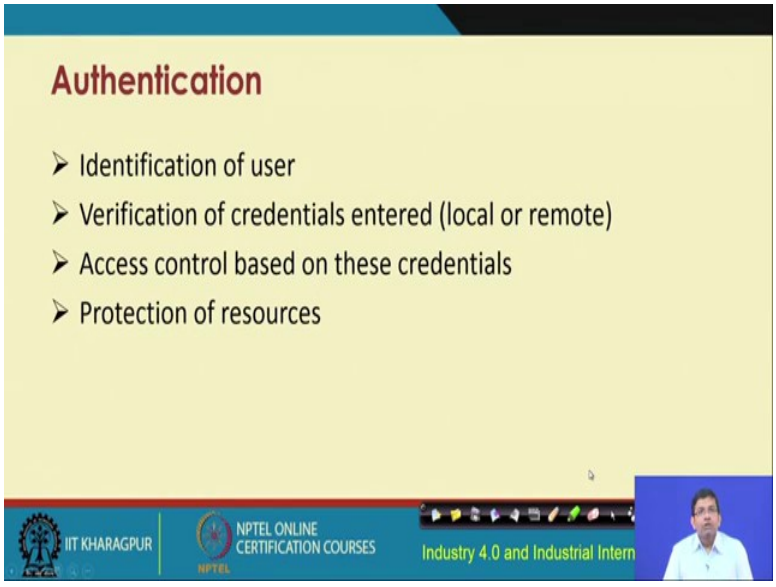
Software security involves ensuring authentication, integrity and availability. In the lecture on security in IIoT, I discussed these different features in adequate detail. So, this software security will have to ensure all these 3 different features of authentication, integrity and availability and their implementation.

(Refer Slide Time: 14:30)



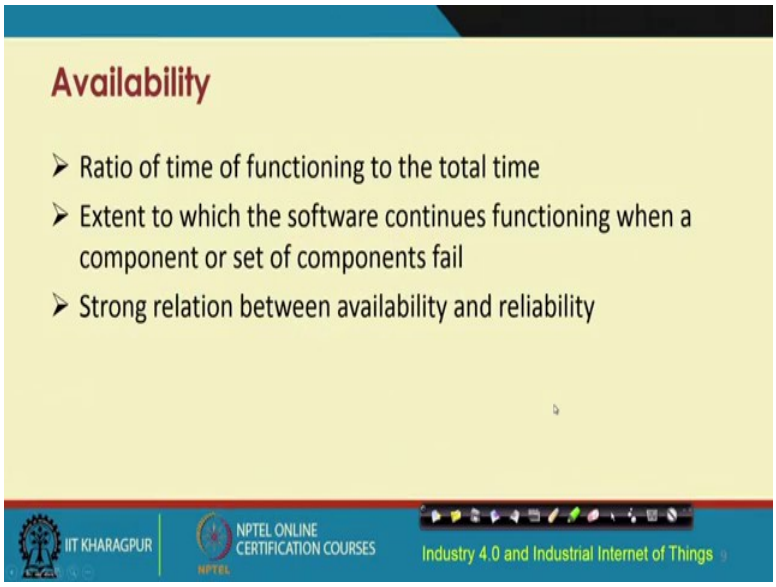
Integrity talks about assurance of an uncorrupted data.

(Refer Slide Time: 14:38)



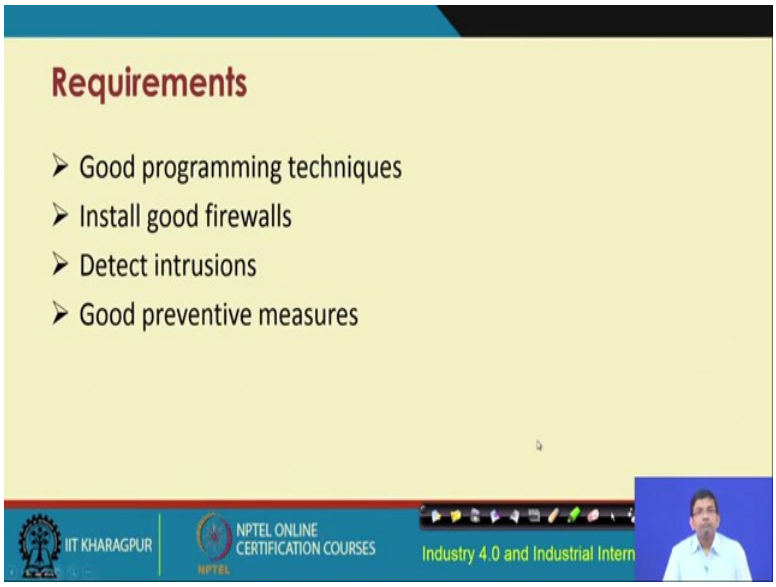
Authentication talks about identification of user correctly and ensuring that the credentials that are entered locally or remotely through the machine by the user are all correct and we are given, we are authenticating a particular user to be a legitimate one.

(Refer Slide Time: 14:59)



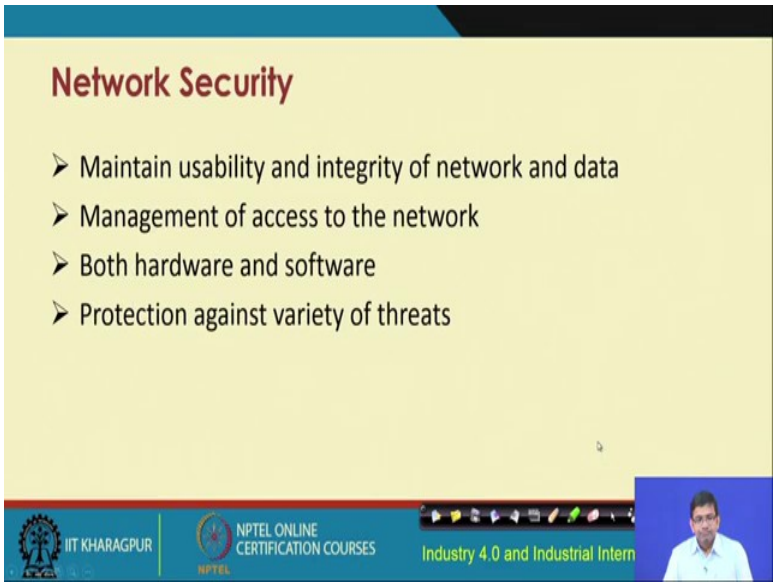
And the third one is availability, which talks about the ratio of the time of functioning to the total time. So, ensuring that the machine is made available, the software is made available as much long as possible.

(Refer Slide Time: 15:16)



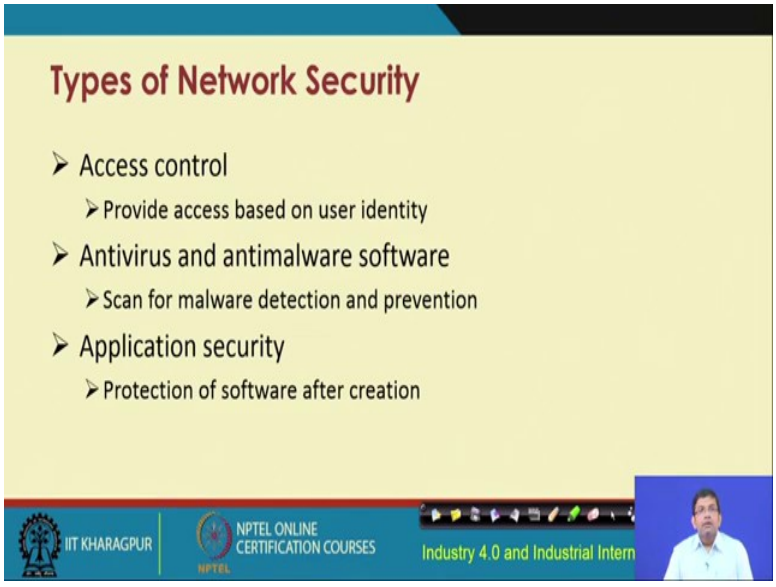
There are different requirements with respect to ensuring good programming techniques, installing good firewalls, detecting intrusions, good preventive measures, etc. these are some of these techniques for ensuring the security and safety in an IIoT enabled system.

(Refer Slide Time: 15:45)



Network security talks about securing the entire network so that the vulnerabilities in the network, the vulnerable points in the network are minimized.

(Refer Slide Time: 15:53)

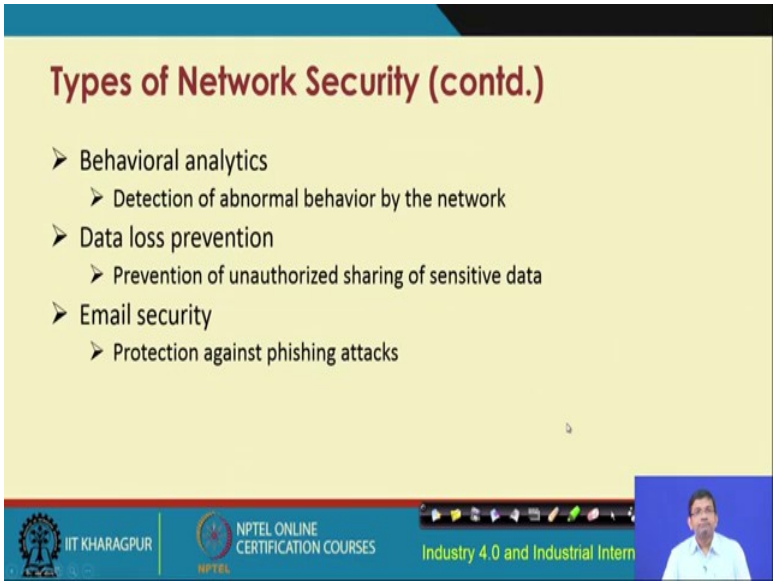


There are different types of network security: access control based on who the actual users are and how much access this should have in the system, not that all users are

going to have 100 percent access to all the different components of the system. Certain users are going to have access to certain components other users are going to have access to the other components of the system and so on.

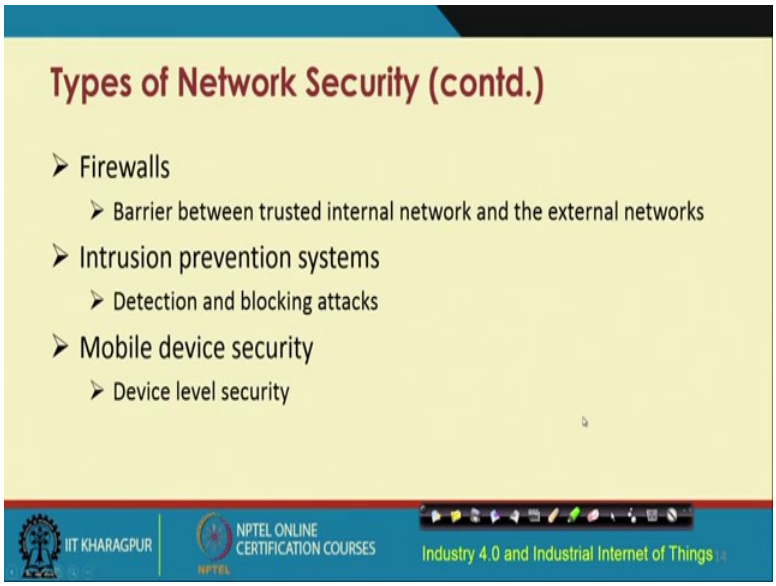
So, controlling this access based on the privileges that are dictated through the policy documents, those should be implemented. Antivirus, antimalware software should be should be used in order to protect the network, then application layer security for protection of the software after it is development that also should be done.

(Refer Slide Time: 16:47)



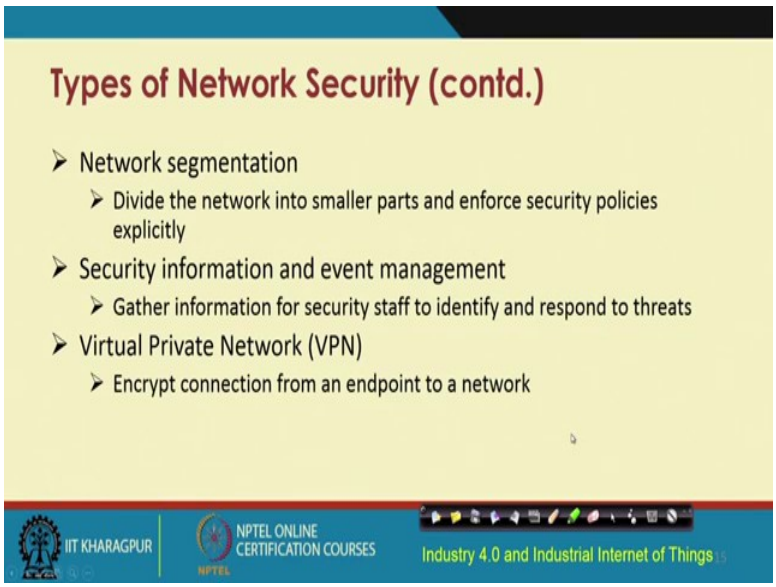
There are different types of security issues; behavioral analytics for detecting abnormal behavior by the network should be done. Data loss prevention should be ensured and email security should be ensured to protect against phishing attacks.

(Refer Slide Time: 17:06)



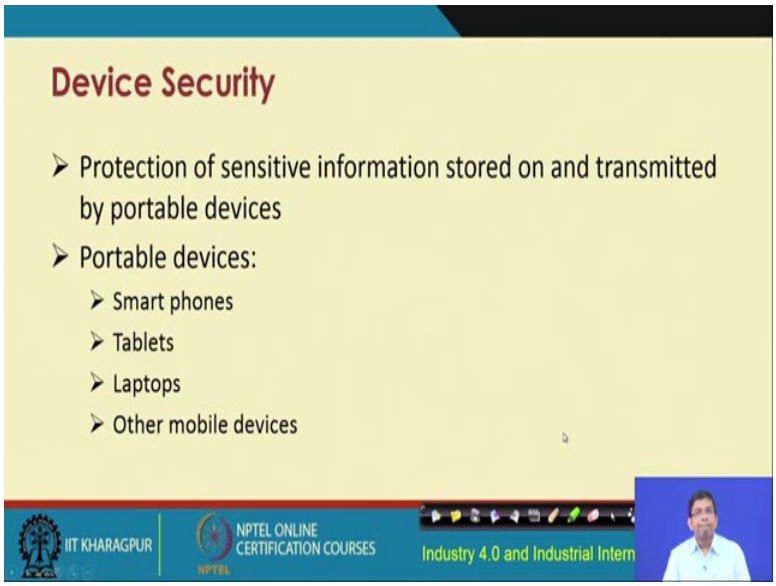
Firewalls, intrusion prevention systems, intrusion detection systems, mobile device security, these are also other concerns of network security.

(Refer Slide Time: 17:18)



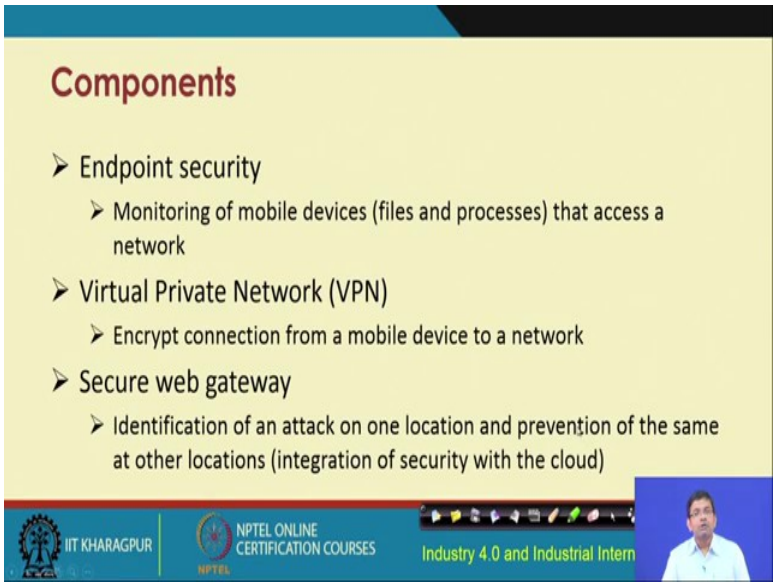
Network segmentation, which is basically dividing the network into smaller parts and enforcing security policies explicitly in those different subdivided parts that is network segmentation. VPN security; security of information and event management these are all the different other concerns in network security.

(Refer Slide Time: 17:39)



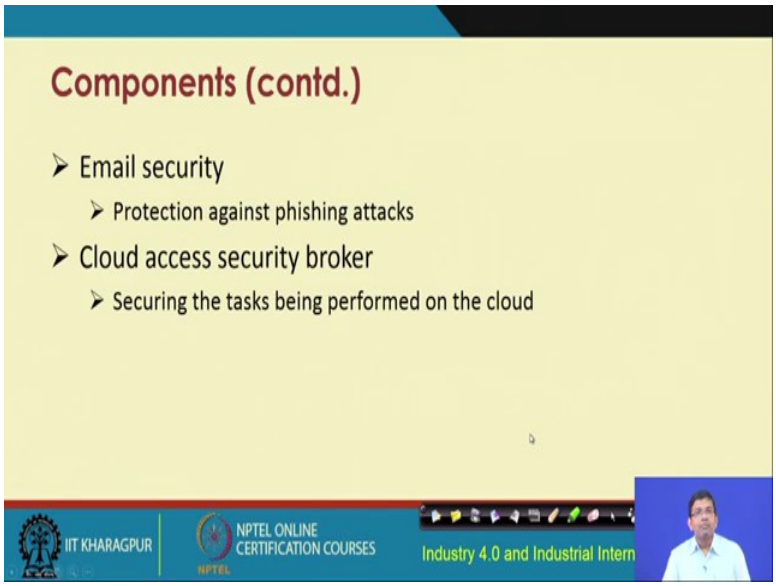
Device security is very important, protection of the sensitive information that are stored in the devices and the different devices such as smartphones, tablets, laptops, etc., their device security is very important.

(Refer Slide Time: 17:56)



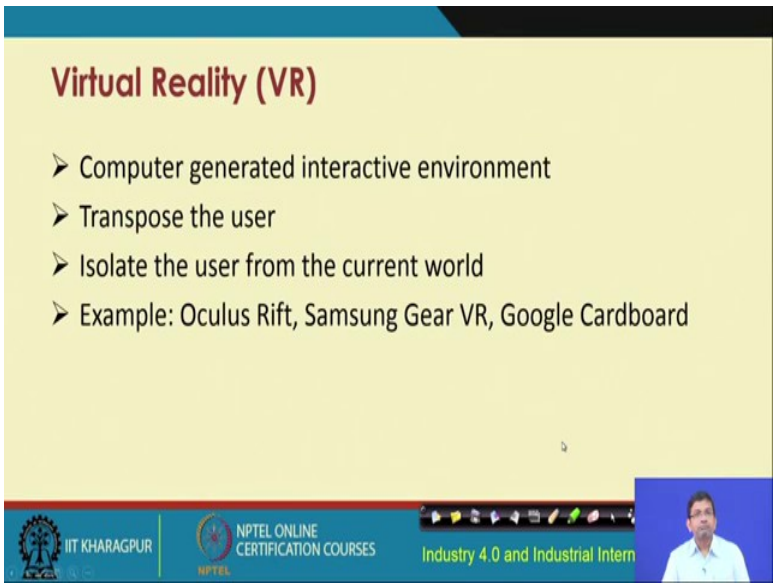
Components in a particular network which improves the different devices, their security, endpoint security, VPN security, you know the gateway security all of these different network components and their security are very important.

(Refer Slide Time: 18:13)



Email security also likewise and cloud security, because cloud is like a third party service in most of the cases. So, securing the cloud and ensuring the integration of the cloud to the home system and the communication between the home system and the cloud, and their security these are also different other components of security in IIoT implementation.

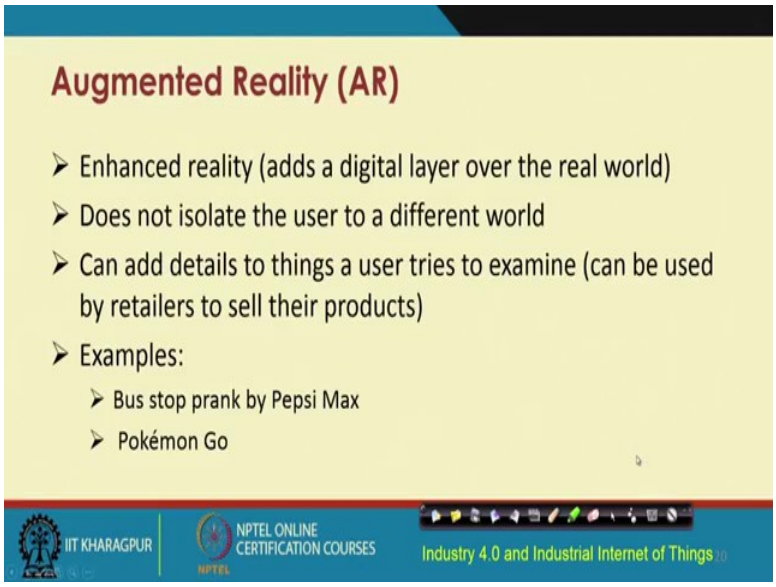
(Refer Slide Time: 18:41)



Now, let us talk about virtual reality, virtual reality and augmented reality we talked about a lot in a separate lecture and if you recall that these are very important

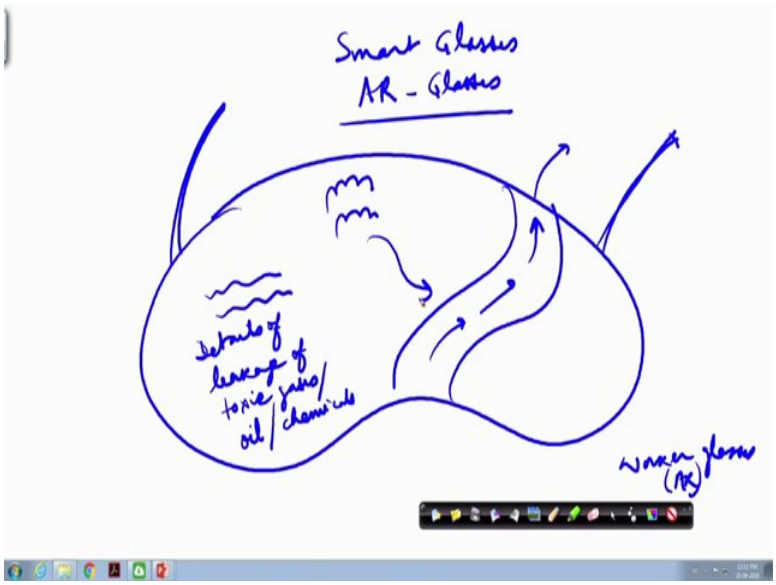
components that could be used in the industry in order to improve the efficiency of the processes to offer training to the workers and so on. So, augmented reality as well as virtual reality we have discussed in length in a previous lecture we are not going to do that once again over here, but one thing I would like to highlight over here.

(Refer Slide Time: 19:17)



So, virtual reality and augmented reality is something that we have understood, but let me show you, let me draw a schematic of how augmented reality would help in ensuring safety and security in a manufacturing plant.

(Refer Slide Time: 19:36)

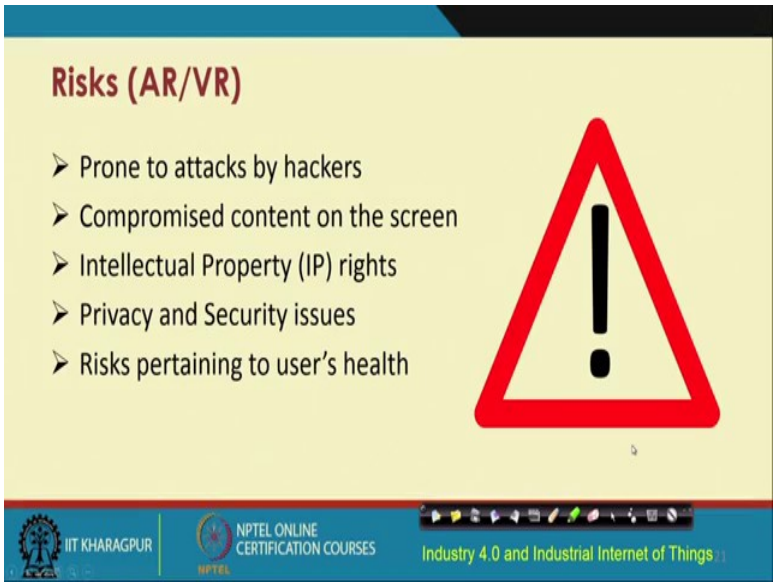


So, all of us have heard about smart glasses. So, smart glasses and augmented reality enabled glasses, AR glasses could be used to improve the safety and security in a manufacturing power plant. So, let us say that we have a glass like this. So, this glass could be basically fitted to the different workers. So, these are the worker glasses, these are the AR glasses, let us say AR or smart glasses which could be owned by the workers.

So, these glasses could help using suitable augmented reality implementations to get details of, let us say details of leakage of toxic gases, leakage of not just toxic gases, but also may be leakage of oil in a manufacturing plant maybe in some machine some oil is getting leaked and so on or maybe some other chemicals leakage of other chemicals, these are some of these examples. So, leakage could be detected by wearing these AR enabled glasses, smart glasses. So, these are possible. If there is a leakage, let us say that there is a leakage right, it would be possible to get the directions a safe way out from this facility so that the worker is not affected due to this kind of event. So, the safe passage way out basically can be directed to this AR enabled glass.

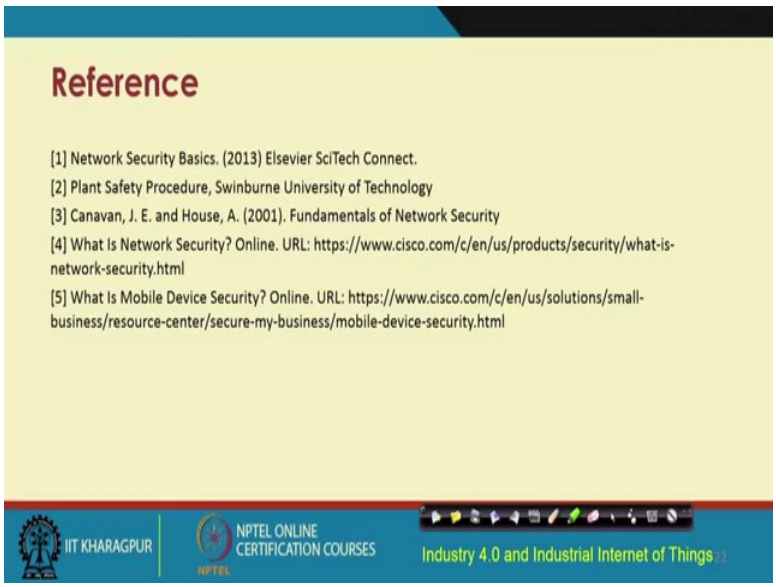
So, like this you could have different other implementations, let us say that if there is a fire or maybe if there is some other event, undesirable event that has happened. So, then taking the requisite action that direction the guidance can be offered by these AR enabled glasses. So, AR enabled glasses lot of research work is going on some industries are already in this space they are working on development of these AR enabled glasses, implementing different functionalities, custom functionalities are implemented in these different AR enabled glasses. So, these could be owned by the workers to ensure their safety and security.

(Refer Slide Time: 22:51)



However this AR/VR enabled solutions, these are new IT based solutions. So, they are prone to IT attacks by different, so there are different attackers who could be performing different attacks. So, it might so happen that the content of the screen due to an attack might get compromised and that is going to pose additional risks to these different workers who would be using these different devices.

(Refer Slide Time: 23:28)



So, in a nutshell this is what I have covered. So, this is basically how these augmented reality glasses could help in improving the safety and security in these manufacturing plants is what I discussed at the end.

I started discussing about what are the security and safety issues in a manufacturing plant and how IIoT can come as a rescuer for implementing these safety and security issues in a manufacturing plant so that the devices can be safely and securely managed and stored and also they the human resources the workers could also be having a safe working environment a secured working environment. So, these are different references once again as usual and with this we come to an end of this particular lecture as well.

Thank you.