

UNT 5:

Diff MC and MP:

Interfacing:

Topic 1...Need of security in IOT – WHY?

Q1: Explain the need **of security in IOT?**

Ans: KALI LINUX.. ..//

....definition...applications..block diagram....

Challenge 1: Gaps in technical sophistication....

10 days..15 august...AMAZON..

Amazon/ azure/ **google>>..cheapest plan....best security...**

2.7..<<3.0<<..4.1 industry standards

4.5<<<<

New types of attacks:

By nature, a complex system of connected devices opens many new attack vectors, even if each device is secure when used independently. Since a system's most vulnerable point determines its overall security level, a comprehensive, end-to-end approach is required to secure it. Such approaches are difficult to develop, however, because most hackers concentrate on breaching a specific element within the technology stack by using one methodology. By contrast, system operators or integrators must provide end-to-end protection against all possible attack vectors, dividing their attention and resources across the system.

It is not yet clear who will take the lead in developing end-to-end security solutions for the IoT. Component suppliers and OEMs are not well positioned to accomplish this task, since the IoT includes such a broad network of devices of different provenance. Integrators are better positioned to provide solutions, but they often lack the necessary capabilities.

Indian railways..original idea..NOT..gaps..: 169 Km/h

Europe:...C + P..... 400 km/h

STANDARD: GIAI 202....example of Std....Copy: Europe

Challenge 2: Standards are absent or immature

The IoT lacks well-established overarching standards that describe how the different parts of the technology stack should interact. Instead, large players and industry organizations use their own solutions. Some segments, such as industrials, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years. In other segments, such as automotive or smart buildings, standards are rudimentary. This lack of standards may slow IoT adoption or discourage device manufacturers and others from developing new technological solutions, since they do not know whether their innovations will meet the guidelines that eventually become dominant. In addition, IoT players will have difficulty developing end-to-end security solutions without common standards.

Challenge 3: Customers and end users view IoT security as a commodity

Our research confirmed that customers and producers consider security essential, but they also view it as a commodity—a basic feature that does not merit higher prices. This creates a fundamental disconnect between the desire for security and the willingness to pay for it. In our survey, 31 percent of semiconductor leaders claimed that their manufacturing customers want to try to avoid all security breaches at any cost; an additional 38 percent believed that their customers want security solutions that eliminate at least 98 percent of potential risks (Exhibit 2). Only 15 percent of respondents believed that their customers would be willing to pay a premium higher than 20 percent for the next tier of enhanced chip security. More than 40 percent indicated that their customers either are unwilling to pay any premium or expect security costs to decline.

Challenge 4: **Semiconductor companies struggle to profit from security**

India: Intel: plant open why>>..atMOSPHERE: ..POLLUTION....MEH

Semiconductor companies who manufacturer semiconductor devices.

Intel: processor:

With end customers and device manufacturers unwilling to pay for significant security measures, semiconductor companies are in a bind. In our survey, 38 percent of semiconductor executives said that it is highly difficult to make money by offering security solutions, and 40 percent said it is difficult. Their troubles may largely stem from the long-standing, widespread perception that software providers have greater security expertise. For those semiconductor companies that choose to create security software, or that are forced in that direction, the potential profits may not be commensurate with the effort required. After all, many semiconductor players have stepped up their software ventures in recent years, but most have been disappointed with their returns.

Topic 2..Common IoT security measures include:

- **Incorporating security at the design phase.** IoT developers should include security at the start of any consumer-, enterprise- or industrial-based device development. Enabling security by default is critical, as well as providing the most recent operating systems and using secure hardware.
- Hardcoded credentials should never be part of the design process. An additional measure developers can take is to require credentials be updated by a user before the device functions. If a device comes with default credentials, users should update them using a strong password or [multifactor authentication](#) or [biometrics](#) where possible.
- **PKI and digital certificates.** Public key infrastructure ([PKI](#)) and [509 digital certificates](#) play critical roles in the development of secure IoT devices, providing the trust and control needed to distribute and identify public encryption keys, secure data exchanges over networks and verify identity.
- **API security.** Application performance indicator (API) security is

essential to protect the integrity of data being sent from IoT devices to back-end systems and ensure only authorized devices, developers and apps communicate with APIs.

- **Identity management.** Providing each device with a unique identifier is critical to understanding what the device is, how it behaves, the other devices it interacts with and the proper security measures that should be taken for that device.
- **Hardware security.** Endpoint hardening includes making devices tamper-proof or tamper-evident. This is especially important when devices will be used in harsh environments or where they will not be monitored physically.
- Strong encryption is critical to securing communication between devices. Data at rest and in transit should be secured using cryptographic algorithms. This includes the use of key lifecycle management.
- **Network security.** Protecting an IoT network includes ensuring port security, disabling port forwarding and never opening ports when not needed; using antimalware, firewalls and intrusion detection system/intrusion prevention system; blocking unauthorized IP addresses; and ensuring systems are patched and up to date.
- **Network access control.** [NAC](#) can help identify and inventory IoT devices connecting to a network. This will provide a baseline for tracking and monitoring devices.
- IoT devices that need to connect directly to the internet should be segmented into their own networks and have access to enterprise network restricted. Network segments should be monitoring for anomalous activity, where action can be taken, should an issue be detected.
- **Security gateways.** Acting as an intermediary between IoT devices and the network, security gateways have more processing power, memory and capabilities than the IoT devices themselves, which provides them the ability to implement features such as firewalls to ensure hackers cannot

access the IoT devices they connect.

- **Patch management/continuous software updates.** Providing means of updating devices and software either over network connections or through automation is critical. Having a coordinated disclosure of vulnerabilities is also important to updating devices as soon as possible. Consider end-of-life strategies as well.
- IoT and operational system security are new to many existing security teams. It is critical to keep security staff up to date with new or unknown systems, learn new architectures and programming languages and be ready for new security challenges. C-level and cybersecurity teams should receive regular training to keep up with modern threats and security measures.
- **Integrating teams.** Along with training, integrating disparate and regularly siloed teams can be useful. For example, having programming developers work with security specialists can help ensure the proper controls are added to devices during the development phase.
- **Consumer education.** Consumers must be made aware of the dangers of IoT systems and provided steps they can take to stay secure, such as updating default credentials and applying software updates. Consumers can also play a role in requiring device manufacturers to create secure devices, and refusing to use those that don't meet high security standards.

With any IoT deployment, it is critical to weigh the cost of security against the risks prior to implementation.

Topic 3.....

IoT security and privacy concerns

Although IoT is rapidly growing, it still faces security and privacy issues:

Security Risks

IoT devices are connected to your desktop or laptop. Lack of security increases the risk of your personal information leaking while the data is collected and transmitted to the IoT device.

IoT devices are connected with a consumer network. This network is also connected with other systems. So if the IoT device contains any security vulnerabilities, it can be harmful to the consumer's network. This vulnerability can attack other systems and damage them.

Sometimes unauthorized people might exploit the security vulnerabilities to create risks to physical safety.

Privacy Risks

In IoT, devices are interconnected with various hardware and software, so there are obvious chances of sensitive information leaking through unauthorized manipulation.

All the devices are transmitting the user's personal information such as name, address, date of birth, health card information, credit card detail and much more without encryption.

Though there are security and privacy concerns with IoT, it adds values to our lives by allowing us to manage our daily routine tasks remotely and automatically, and more importantly, it is a game-changer for industries.

IoT applications across industries

Various companies now help businesses use IoT to solve long-standing, industry-specific challenges. They develop IoT solutions that connect things, collect data and derive insights with open and scalable solutions that reduce costs, improve productivity and increase revenue. Let's see the industry categories, that are using IoT solutions in the figure below:

How to secure your data on IoT devices

http

https:SECURE..

#1 Understand the Advantages of Connecting to the Internet

Don't connect your smart device to the internet just because it has the capability. First you should check what features are available in your device without connecting it to the internet. You might discover that your smart device has good features which are available without internet connection. In that scenario, it is better to use the device offline. This is a good way of protecting your security without having to spend anything.

#2 Use Secondary Network

Most of the time, your WiFi router is capable of creating multiple networks which helps you to create restricted access for your family and your guests. You should also think of creating an extra network just for your internet of things devices. This will help you to curb unauthorised access to your sensitive data when you are accessing your connection through your smart devices. Having a separate connection to act like a buffer will help to ensure that no outside entity is allowed to access your shared files and other kinds of encrypted data.

#3 Keep Changing your Passwords

It is important that you keep changing your passwords on your PC's, individual accounts and mobile devices. You must be knowing this. What you should also remember is that it is equally important to change the passwords you use on your internet of things devices. You should be diligent with these passwords and ensure that each device has a unique password. You can use a password manager to remember your passwords or even use the traditional method of pen and paper. Remember that every password must be changed twice every year.

Advertisement

#4 Don't Enable Universal Plug & Play Features

Nearly all smart devices have a feature, called as UPnP. With this feature, different devices can find one another and connect to each other. This feature makes the devices more convenient because you don't need to configure each of these devices separately. What you need to be aware, however is that UPnP protocols make use of local networks for connecting and are thus vulnerable to outside access. In case there is an attack, outside entities might be able to gain access to multiple devices simultaneously. Hence, it is a good practice to turn off the UPnP feature on every device.

#5 Update your every Device

You should enable automatic updates, if it is available and in its absence, check regularly for firmware updates. This is necessary as this is the way new security patches are installed on your devices. As hackers and other intruders are consistently coming up with new ways to hack IoT devices, technology manufacturers are involved in the constant effort to counteract such threats with security measures. Thus, making sure that all your devices are updated will help to strengthen the security in your house as a whole.

#6 Reduce your use of Cloud Technology

As you might know, most IoT providers provide free cloud storage with their devices. The reason for this is that it is considered as emerging technology. However, there are some potential drawbacks with this technology. The first one is that you need an active connection if you want to access the data that you store in the cloud; that information cannot be accessed without a connection. Secondly, outsiders might be able to hack into your connection as you are accessing your account. So, before you start using the cloud, make sure that you are familiar with the ways to secure your data and thoroughly understand the privacy measures.

#7 Be Careful of Where you Take your Wearables ELE

Wearable devices use WIFI connectivity to collect and store personal data, so that it can later provide you with an accurate analytics. Hence, when you take your wearable device to a public place, as it connects with the public WIFI, your data becomes instantly accessible to whoever is connecting to the same network. So, it is a safe bet to avoid taking your wearables which has a shared network. In case you do take it, ensure that you disable the device when you are not using it.

#8 Avoid using Devices that are Risky

There are some IoT devices that need to be constantly connected to the internet to operate effectively. There are also some that do not bring as much efficiency to your life as you had thought of. It is, therefore, a good practice to evaluate the usefulness of your devices from time to time. If you feel that they don't add anything to your life or if they seem risky, better discard them. Additionally, if there is a single device that can replace several others, invest in that device. This is because the smaller number of devices that you use, the less is the risk factor.

What Is Artificial Intelligence (AI)?

[Artificial intelligence](#) (AI) refers to the simulation of human intelligence in machines that are programmed to **think like humans** and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal.

Understanding Artificial Intelligence

When most people hear the term artificial intelligence, the first thing they usually think of is robots. That's because big-budget films and novels weave stories about human-like machines that wreak havoc on Earth. But nothing could be further from the truth.

Artificial intelligence is based on the principle that human intelligence can be defined in a way that a machine can easily mimic it and execute tasks, from the most simple to those that are even more complex. The goals of artificial intelligence include learning, reasoning, and perception.

As technology advances, previous benchmarks that defined artificial intelligence become outdated. For example, machines that calculate basic functions or recognize text through optimal character recognition are no longer considered to embody artificial intelligence, since this function is now taken for granted as an inherent computer function.

AI is continuously evolving to benefit many different industries. Machines are wired using a cross-disciplinary approach based in mathematics, computer science, linguistics, psychology, and more.

Applications of Artificial Intelligence

The applications for artificial intelligence are endless. The technology can be applied to many different sectors and industries. AI is being tested and used in the healthcare industry for dosing drugs and different treatment in patients, and for surgical procedures in the operating room.

Other examples of machines with artificial intelligence include computers that play chess and [self-driving cars](#). Each of these machines must weigh the consequences of any action they take, as each action will impact the end result. In chess, the end result is winning the game. For self-driving cars, the computer system must account for all external data and compute it to act in a way that prevents a collision.

Artificial intelligence also has applications in the financial industry, where it is used to detect and flag activity in banking and finance such as unusual debit card usage and large account deposits—all of which help a bank's fraud department. Applications for AI are also being used to help streamline and make trading easier. This is done by making supply, demand, and pricing of securities easier to estimate.

Categorization of Artificial Intelligence

Artificial intelligence can be divided into two different categories: weak and strong. [Weak artificial intelligence](#) embodies a system designed to carry out one particular job. Weak AI systems include video games such as the chess example from above and personal assistants such as Amazon's Alexa and Apple's Siri. You ask the assistant a question, it answers it for you.

[Strong artificial intelligence](#) systems are systems that carry on the tasks considered to be human-like. These tend to be more complex and complicated systems. They are programmed to handle situations in which they may be required to problem solve without having a person intervene. These kinds of systems can be found in applications like self-driving cars or in hospital operating rooms.

Example of AI

```
import speech_recognition as sr

sr = sr.Recognizer()

print("I am your script and listening you.....")

with sr.Microphone() as m:
    audio=sr.listen(m)
    query=sr.recognize_google(audio,language='eng-in')
    print(query)
```

Machine learning

Machine learning is a method of data analysis that automates analytical **model building**. It is a branch of artificial **intelligence** based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Machine Learning is the field of study that gives computers the capability to learn without being explicitly programmed. ML is one of the most exciting technologies that one would have ever come across. As it is evident from the name, it gives the computer that makes it more similar to humans: ***The ability to learn***. Machine learning is actively being used today, perhaps in many more places than one would expect

Process machine learning

1. **Data Collection:** Collect the data that the algorithm will learn from.

2. **Data Preparation:** Format and engineer the data into the optimal format, extracting important features and performing dimensionality reduction.
3. **Training:** Also known as the fitting stage, this is where the Machine Learning algorithm actually learns by showing it the data that has been collected and prepared.
4. **Evaluation:** Test the model to see how well it performs.
5. **Tuning:** Fine tune the model to maximise it's performance.