SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Information Technology

Course Name – Internet of Things & AI

III Year / V Semester

Unit 3- INTERNET OF THINGS CHALLENGES

Vulnerabilities of IoT, Security, Privacy

1. Lack of physical hardening

The lack of physical hardening has always been a concern for devices within the internet of things. Since most IoT devices are remotely deployed, there is no way to properly secure devices that are constantly exposed to the broader physical attack surface.

2. Insecure data storage and transfer

As more people utilize cloud-based communications and data storage, the cross-communication between smart devices and the IoT network increases. However, any time data is transferred, received, or stored through these networks, the potential for a breach or compromised data also increases.

3. Lack of visibility and device management

Many IoT devices remain unmonitored, untracked, and improperly managed. As devices connect and disconnect from the IoT network, trying to monitor them can grow to be very difficult. Lack of visibility into device status can prevent organizations from detecting or even responding to potential threats.

4. Botnets

Botnets are a series of internet-connected devices that are created to steal data, compromise networks, or send spam. Botnets contain malware that allows the attacker to access the IoT device and its connection to infiltrate an organization's network, becoming one of the top threats for businesses.

5. Weak passcodes

Although intricate passcodes can prove to be secure for most IoT devices, one weak passcode is all it takes to open the gateway to your organization's network. Inconsistent management of passcodes throughout the workplace enables hackers to compromise your entire business network.

6. AI-based attacks

Hackers now can build AI-powered tools that are faster, easier to scale, and more efficient than humans, to carry out their attacks.

- **Weak or hardcoded passwords**

Many passwords are easy to guess, publicly available or can't be changed. Some IT staff don't bother changing the default password that shipped with the device or software.

- **Unsecured network services and ecosystem interfaces.**

Each IoT app connection has the potential to be compromised, either through an inherent vulnerability in the components themselves or because they're not secured from attack. That includes any gateway, router, modem, external web app, API or cloud service connected to an IoT app.

- **Outdated or unsecured IoT app components**

Many IoT applications use third-party frameworks and libraries when built. If they're obsolete or have known vulnerabilities and aren't validated when installed in a network, they could pose security risks.

- **Unsecured data storage and transfer**

Different data types may be stored and transmitted between IoT applications and other connected devices and systems. All must be properly secured via Transport Layer Security or other protocols and encrypted as needed.

Privacy

Privacy typically refers to the user's ability to control, access, and regulate their personal information, and security refers to the system that protects that data from getting into the wrong hands, through a breach, leak, or cyber attack.

Security challenges

- Lack of physical security.
- Botnet attacks.
- Lack of visibility.
- Ransomware.
- Use IoT security analytics.
- Improve network visibility.
- Encrypted communication.
- Authentication.

Security vs Privacy

Security is about the **safeguarding of data**, whereas privacy is about the **safeguarding of user identity**.

Difference between Security and Privacy

S. No.	Security	Privacy
1.	Security is something about data safeguarding.	Privacy is something about user identity's safeguarding.
2.	Security can be defined as protection against various unauthorized access to information.	Privacy can be harder to specify because user-specific information can be secure information as well.
3.	Example: Clinic staff and hospital apply secure systems for communicating with patients regarding their health-related information, rather than transferring information by email accounts.	Example: It might limit the record access of patient health to particular staff members of the hospital, like medical assistants, nurses, and doctors.
4.	Security is any state of being free through potential threats or personal freedom.	Privacy indicates anyone who feels free from any unwanted attention.
5.	There are three primary objectives of security such as availability, integrity, and confidentiality.	On the other side, privacy represents many rights of organizations and individuals related to personal data.