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

Security requirements Threat analysis

Security requirements

Authentication

IoT devices must establish authentication, non-repudiation, integrity at several levels. Which is used to help devices to communication between the users and built the trust among each other

Confidentiality

Confidentiality is important for IoT in a way that the wireless communication between one object to other different objects is particularly sensitive and vulnerable to confidentiality threats. Attackers are always snooping for confidential data and information for their use.

Access Control

It discusses the permission in the usage of resources and data assigned to different devices of the wide and vast area of the IoT networks. Data holder and data collector are present when dealing with access control in IoT.

How to overcome this issue?

- Learn the most likely **threats**
- Understand the **risks**
- **Update** the apps regularly
- **Secure** the network
- Enable strong **authorization**
- Secure **communication**
- Secure control **applications**
- Secure **API** integrations
- **Monitor** IoT apps

IoT threats

- Spoofing threats
- Information disclosure threats
- Tampering threats
- Elevation of privilege threats

Spoofing

Attackers intercept or partially override the data stream of an IoT device and spoof the originating device or system, which is also known as a man-in-the-middle attack. They intercept shared key information, control devices or observe sent data.

Tampering

Attackers can gain access to the firmware or OSes of the devices running an IoT app and then partially or completely replace it on the device. They then use the genuine device and application identities to access the network and other connected services. For example, SQL or XML injection attacks and DDoS attacks are tampering threats for IoT apps

Information disclosure

Attackers eavesdrop on broadcasts to obtain information without authorization, jam the signal to deny information distribution or partially override the broadcast and replace it with false information. They then threaten to release or sell the data.

Elevation of privilege

Attackers use unsecured IoT apps to change the access control rules of the application to cause damage. For example, in an industrial or manufacturing environment, an attacker could force a valve to open all the way that should only open halfway in a prod