Unit-1

Date: 21/02/24 Page No.

Topic:

Assignment -1

1) What are the key components of the IOT ecosystem? Explain their roles with examples.

→ The IOT ecosystem consists of several key components that work together to enable the seamless flow of data between devices, networks and users.

→ Key components:-

(1) Devices (Things):-

→ Role:- These are the physical objects or sensors that collect and send data. They could range from simple sensors to more complex devices with embedded computing capabilities.

→ Example:- Wearable Devices, Connected cars.

(2) Connectivity (Network Infrastructure):-

→ Role:- This layer connects the devices to the Internet or local ~~from~~ Networks and ensure that data can be transmitted & between devices, Sensors, and Central systems.

→ Example:- WiFi, Cellular Networks, Bluetooth, Zigbee.

(3) Applications (User-Interfaces):-

→ Role:- These are the Software platforms or applications that allows users to interact with the IoT System providing insights, Control, and decision-making Support.

→ Example:- Smart home apps like Google Home, Amazon Alexa, Health-Care Applications.

Date: _____ Page No.

Topic: _____

2. Discuss the Why Security is Critical for IOT and Mobile devices. Provide Examples of risks associated with Inadequates Security in these environments.

→ Security is Critical for IOT and Mobile devices due to the interconnected and often sensitive nature of the data and operations they handle.

→ This devices are frequently Connected to the Internet, Communicating with other devices, systems, and Cloud platforms, Creating a broad attack surface that Cybercriminals Can Exploit.

→ Risk associated with Inadequates Security in these environment:-

(1) Data breaches:-

→ Attackers gaining Unauthorized access to personal, Corporate, or Sensitive data - through poorly Secured devices.

(2) Botnets and DDos Attacks:-

→ A botnet is a network of compromised IOT devices used to carry out malicious actions, such as Distributed Denial of Service attacks.

(3) Unauthorized Access and Control:-

→ Attackers may gain control of devices, manipulating them to steal data, disrupt operations, or cause damage. This can occur if devices lack proper authentication or authorization mechanisms.

(4) Privacy Violations:-

→ Sensitive personal data, such as location, health metrics, or personal preferences, can be exposed or misused if security is inadequate.

3) List and Explain three major vulnerabilities in IoT and Mobile environments. How do these vulnerabilities Impact devices functionality and user privacy?

→

(1) Insecure Network Communication:-

→ IOT and Mobile devices often Rely on Wireless Networks, Such as WiFi, Bluetooth, and cellular Networks, to Communicate. If These Communications are not encrypted or properly Secured, they can be intercepted by attackers through man-in-the-middle attacks or network Sniffing.

→ Impact:-

→ Device Functionality.

→ User privacy.

Date: Page No.
Topic:

(2) Weak Authentication and Access Control.

→ Many IOT and Mobile devices use weak or default passwords, lack Multi-factor authentication (MFA), or fail to implement strict access control measures. Attackers can exploit these weaknesses to gain unauthorized access to devices, apps or networks.

→ Impact:

→ Device functionality.

→ User privacy.

(3) Lack of Software Updates and patching

→ Many IOT and Mobile devices do not receive timely security updates or patches, leaving them vulnerable to known exploits and security flaws. Device manufacturers may neglect to release updates, or users may fail to install them, increasing the likelihood of

Successful attacks.

-> Impact:-

-> Device functionality.

-> User privacy.

4) Describe the three layers of IOT architecture: perception, Networks, and Application. Include the function of each layer in the IOT ecosystem.

->

(1) Perception layer:-

-> The perception layer is the 'sensing' layer, responsible for collecting real-world data from the environment. It consists of sensors, actuators, and other devices that gather data related to physical parameters such as temperature, humidity, motion, pressure, or even user interactions.

Topic:

(2) Network layer:-

→ The Network layer is responsible for transmitting the data collected by the perception layer to other devices or systems for further processing, storage or action. It include communication technologies such as wifi, Bluetooth, Zigbee, cellular networks and more advanced technologies like 5G.

(3) Application layer:-

→ The application layer is the top-most layer in the IOT architecture and provides specific services to end users based on the data received and processed the lower layers. It includes the software and platforms that allow users to interact with the IOT systems, such as Mobile apps, dashboards, and web interfaces.

5) Explain the differences between MQTT and CoAP Communication protocols in IOT. Include Examples of where each protocol is used.

→

	MQTT	CoAP
Protocol:	Publish / Subscribe	Request / Response
Transport Protocol	TCP / IP	UDP
Message Model	Publish / subscribe	Request / Response (like HTTP)
Message Delivery	Reliable (QoS level 0, 1, 2)	Unreliable, but supports Blockwise Transfer for larger m
Overhead	Low (but higher than CoAP)	Very low, minimal headers.
Security	TLS / SSL (over TCP)	DTLS (Datagram Transport layer Security)

6) What Security Measures are essential for the Perception layer of IOT architecture? How do these Measures address physical threats to IOT devices?

→

(1) Physical Tamper Detection and protection:-

→ Tamper-resistant hardware:-

→ Many IOT devices are designed with Tamper-resistant enclosures or materials that make it harder for attackers to physically access or alter the device.

→ How it Addresses Physical Threats:-

→ Prevents physical attacks where attackers might open the devices to steal sensitive information or manipulate it functionality.

(2) Secure Boot and device Authentication:-

→ Secure boot:-

→ Secure boot ensures that the devices starts only with verified, trusted software. During the boot process, the firmware checks the integrity of the software and ensures that no unauthorized changes have been made to the firmware.

→ How it Addresses physical Threats:-

→ Prevents the installation of unauthorized firmware or malicious software, which could result from physical tampering or theft.

→ Ensures that only trusted devices can transmit data, preventing malicious devices from infiltrating the Network.

Date: _____ Page No.

Topic: _____

7/ Discuss the role of the application layer in IOT architecture. What security challenges are unique to this layer, and how can they be mitigated?

→ The application layer is the topmost layer in the IOT architecture and is responsible for providing end-user services, applications, and functionalities based on the data collected and processed by the underlying layers.

→ challenges:-

→ Authentication and Access Control:

→ Since the application layer is responsible for manging users and device interactions it is highly susceptible to unauthorized access, data breaches, or abuse of privileges. Weak or poorly implemented authentication mechanisms can allow attackers to gain control of devices, modify configurations, or steal sensitive

data.

→ Mitigation:-

→ Strong authentication:-

→ Implement robust authentication mechanisms, such as multi-factor authentication (MFA), OAuth, or biometric verification, to ensure that only authorized users can access the application.

→ Role-Based Access Control:-

→ Define User roles with specific permissions to ensure that only authorized individuals can access critical functions or data.