Module 3

Q1. What is IoT?

The Internet of Things (IoT) refers to a network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, actuators, software, and network connectivity, allowing them to collect and exchange data.

Key Characteristics:-

1. Connectivity: IoT devices are equipped with communication capabilities, enabling them to connect to the internet or other devices within the network. Common communication protocols include Wi-Fi, Bluetooth, Zigbee, and cellular networks.
2. Sensors and Actuators: IoT devices are equipped with sensors to collect data from the surrounding environment. Actuators enable devices to perform actions based on the received data. Examples of sensors include temperature sensors, motion sensors, and cameras.
3. Data Collection and Analysis: IoT devices generate large amounts of data through sensor readings. This data is sent to a centralized platform or the cloud for analysis. Advanced analytics, machine learning, and artificial intelligence may be applied to derive meaningful insights from the data.
4. Interoperability: IoT systems emphasize interoperability, allowing devices from different manufacturers to communicate and work together seamlessly. Standardized communication protocols play a crucial role in achieving interoperability.
5. Remote Monitoring and Control: IoT enables remote monitoring and control of devices and systems. Users can access and manage IoT devices from anywhere with an internet connection, providing flexibility and convenience.
6. Automation: IoT facilitates automation by allowing devices to respond to specific conditions or triggers automatically. This can enhance efficiency, reduce human intervention, and enable smart decision-making.
7. Real-time Communication: IoT systems often operate in real-time or near-real-time, allowing for quick responses to changes in the environment or conditions. This is particularly important in applications such as industrial automation and healthcare.

Q2. List any 5 examples of IoT.

1. Smart Home Devices:

    - Devices such as smart thermostats (e.g., Nest), smart lighting systems, and connected security cameras enable homeowners to control and monitor their home environment remotely. These devices can be managed through mobile apps or voice commands, providing convenience and energy efficiency.
2. Wearable Health Trackers:
    - Wearable devices like fitness trackers and smartwatches collect health-related data, including steps taken, heart rate, sleep patterns, and more. Users can track their fitness goals, and healthcare professionals can use the data for remote patient monitoring and preventive healthcare.
3. Industrial IoT (IIoT) in Manufacturing:
    - In manufacturing, IoT is applied for predictive maintenance, real-time monitoring of equipment, and optimizing production processes. Sensors on machinery collect data, allowing manufacturers to identify potential issues before they cause downtime and improve overall operational efficiency.
4. Smart City Infrastructure:
    - Cities leverage IoT to create smart city solutions for better urban management. Examples include smart traffic management systems that use sensors to optimize traffic flow, waste management systems with smart bins that notify authorities when full, and environmental monitoring for air quality and noise levels.
5. Precision Agriculture:
    - In agriculture, IoT technologies are used for precision farming. Sensors in the field monitor soil moisture, temperature, and crop health. Drones equipped with cameras provide aerial views, helping farmers make data-driven decisions about irrigation, fertilization, and pest control to optimize crop yield.

Q3. Describe IoT UPnP protocol.

- Universal Plug and Play
- networking protocol or a set of networking protocols which enables devices like personal computers, WiFi, Mobile devices, printers etc. to discover each other and establish connections for sharing services and data
- intended to be used on residential networks.
- UPnP can be considered as an extension of Plug and Play which enables users to connect devices directly to a computer without any manual configurations to the device or to the computer.

Working:

- UPnP assumes that a device is compatible with (IP) Addressing, for using protocols built on it, like HTTP, XML, TCP, UDP.
- It uses these protocols to advertise the device's presence and for data transfer.

Addressing:

1. UPnP uses IP addressing. Hence, when it is initiated it acts as a Dynamic Host Configuration Protocol (DHCP) client to assign itself an IP and searches for a DHCP server.
2. If no DHCP server is found, the device assigns itself an IP using a process known as AutoIP, which assigns an IP unique to its local network.
3. If during DHCP transaction, device gets a domain name through a Domain Name Server(DNS), it uses that domain name, else it uses it's IP.

Key Components:

- Discovery:
  - Simple Service Discovery Protocol(SSDP):
    - SSDP is the protocol used by UPnP devices to discover each other.
    - When device is added to the network, it allows the device to advertise it's services to other devices on the network, by sending SSDP alive messages.
    - SSDP also allows a device to passively listen to SSDP alive messages from other devices on the network.
    - When two devices discover each other, a discovery message is exchanged, it contains essential information like the device type and it's services.
- Device Description:
  - When devices discover each other, for the devices to learn more about each other they exchange information in XML format.
  - These messages contain information like Manufacturer name, Model Name, Manufacturer Websites, services provided by device, etc.
- Service Calls:
  - After getting information about the device and it's services, the control point can call for the service to the URL provided by manufacturer.
  - This is done by a protocol known as Simple Object Access Protocol(SOAP) which passes XML messages.
- Event Notification:
  - General Event Notification Architecture(GENA) s the architecture used for event notification in UPnP.

    - This is used by services to respond to service calls.
    - These messages are also sent in XML format.
- Presentation

Advantages:

- It allows real Plug and Play compatibility.
- It is backed by various big vendors and companies like Microsoft and Intel, which makes it an industry standard.
- It is an ideal architecture for home devices and networks.

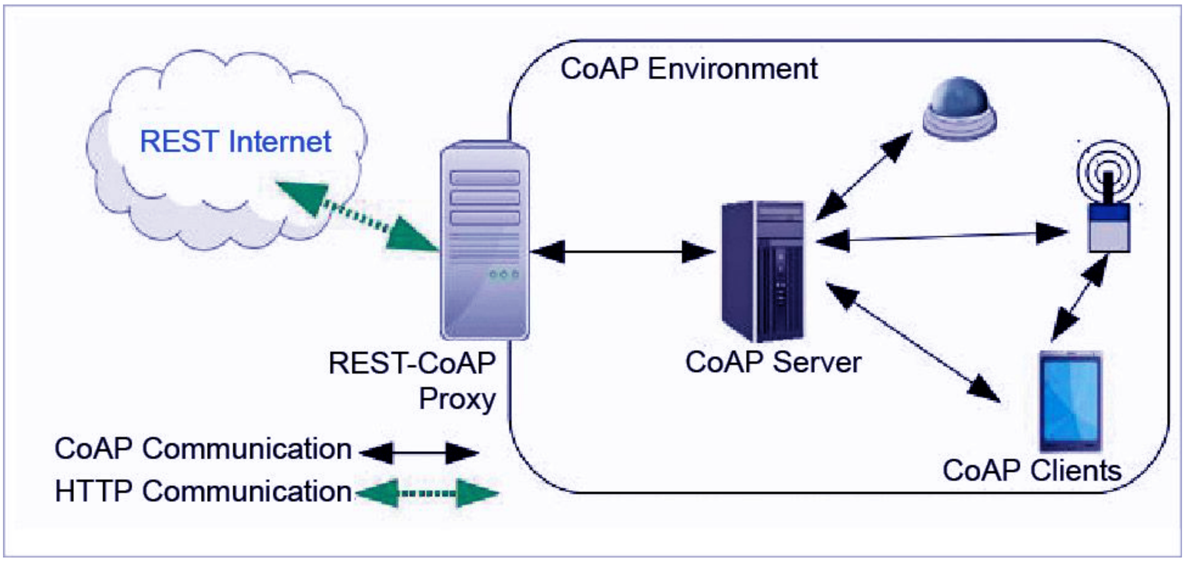
Disadvantages:

- Any malicious program on your network can use UPnP, in the same way a legitimate program uses it.
- Control points do not require any authentication, hence any program on your computer can ask to forward a UPnP port

---

Q4. explain CoAP protocol.

- **CoAP (Constrained Application Protocol)** is a session layer protocol that provides the RESTful (HTTP) interface between HTTP client and server.
- It is designed to use devices on the same constrained network
- This protocol is specially built for IoT systems primarily based on HTTP protocols.
- The whole architecture of CoAP consists of CoAP client, CoAP server, REST CoAP proxy, and REST internet.



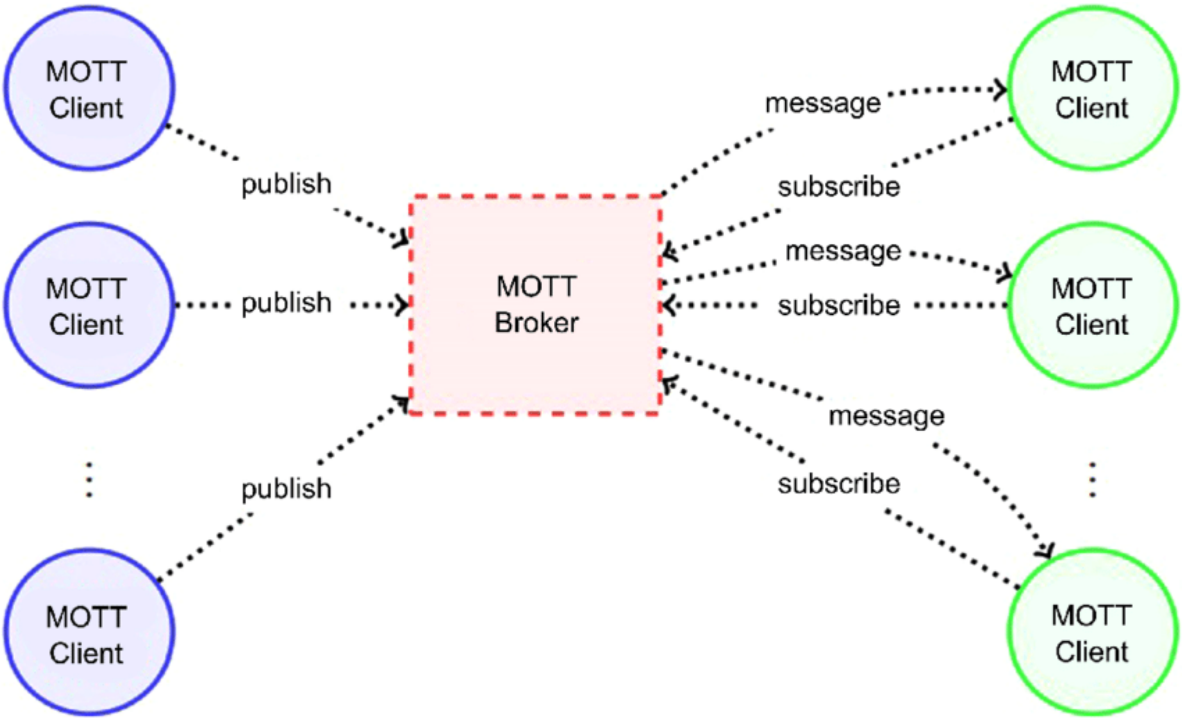
- The data is sent from CoAP clients (such as smartphones, RFID sensors, etc.) to the CoAP server and the same message is routed to REST CoAP proxy. The REST CoAP proxy interacts outside the CoAP environment and uploads the data over REST internet.

Q5. Discuss MQTT protocol.

- Message Queuing Telemetry Transport
- Standard messaging protocols for IoT
- Fields of automotive, manufcaturing, telecommunication, oil and gas

Architecture:

- MQTT protocol is based on publish/subscribe architecture.
- three major components: publishers, subscribers, and a broker.
- publishers are lightweight sensor devices that send their data to connected broker and goes back to sleep whenever possible.
- Subscribers are applications, which are interested in a certain topic or sensory data, so they are connected to brokers to be informed whenever new data are received.
- The broker receives the sensory data and filters them in different topics and sends them to subscribers according to interest in the topics.



Difference between CoAP and MQTT:

Basis of		
COAP		
MQTT		
Abbreviation	Constrained Application Protocol	Message Queuing Telemetry Transport
Communication Type	It uses Request-Response model.	It uses Publish-Subscribe model
Messaging Mode	This uses both Asynchronous and Synchronous.	This uses only Asynchronous
Transport layer protocol	This mainly uses User Datagram protocol(UDP)	This mainly uses Transmission Control protocol(TCP)
RESTful based	Yes it uses REST principles	No it does not uses REST principles
Effectiveness	Effectiveness in LNN is excellent.	Effectiveness in LNN is low.
Communication Model	Communication model is one-one.	Communication model is many-many.

LNN- labelling neural network

Q6.Elaborate XMPP protocol.

- Extensible Messaging Presence Protocol
- protocol for streaming XML elements over a network in order to exchange messages and presence information in close to real time.
- This protocol is mostly used by instant messaging applications like WhatsApp.
- **X :** It means eXtensible. XMPP is a open source project which can be changed or extended according to the need.

- **M :** XMPP is designed for sending messages in real time. It has very efficient push mechanism compared to other protocols.
- **P :** It determines whether you are online/offline/busy. It indicates the state.
- **P :** XMPP is a protocol, that is, a set of standards that allow systems to communicate with each other.

basic requirements of any Instant Messenger which are fulfilled by XMPP:

1. Send and receive messages with other users.
2. Check and share presence status
3. Manage subscriptions to and from other users.
4. Manage contact list
5. Block communications to specific users.

Advantages:

- It is free and decentralized which means anyone can set up an XMPP server.
- It is based on open standards.
- It supports multiple implementations of clients and servers.
- It is flexible, XML-based and can be extended. So, suitable for both instant messaging features and custom cloud services.
- It is efficient, can support million of concurrent users on a single service

Decentralised –

XMPP is based on client-server architecture, i.e. clients don't communicate directly, they do it with the help of server as intermediary.
It is decentralised means there is no centralised XMPP server just like email, anyone can run their own XMPP server.

Q7. Explain various IoT services as a platform

An IoT platform is an integrated service that fulfills the gap between the IoT device and application and offers you to bring physical object online.

1. **Clayster:**
   - When we create a service for a service platform, the executable EXE file already exists.
   - Therefore, we have to create a library project instead and make sure that the target framework corresponds to the version of the Clayster distribution.
   - Such a project will generate a **dynamic link library** (**DLL**) file.

libraries available in the Clayster distribution:

- **Clayster.AppServer.Infrastructure**: This library contains the application engine available in the platform. It also provides report tools, cluster support, manages backups and rendering support for different types of GUIs.
- **Clayster.Library.Abstract**: This library contains a data abstraction layer, and is a crucial tool for the efficient management of objects in the system.
- **Clayster.Library.Installation**: This library defines the concept of packages.
- **Clayster.Library.Meters**: It contains an abstraction model for things such as sensors, actuators, controllers, meters, and so on

2. **thinger.io:**
3. SenseIoT
4. Carriots

Q8. Explain the risks of IoT technology

The Internet of Things (IoT) technology brings numerous benefits, but it also introduces various risks and challenges, ranging from privacy and security concerns to operational and regulatory issues.

1. **Security Vulnerabilities:**
    - Weak authentication, encryption, and insecure communication protocols can expose devices to hacking, data breaches, and unauthorized access.
2. **Data Privacy Concerns:**
    - IoT devices collect vast amounts of data from sensors and user interactions, raising privacy concerns regarding the collection, storage, and use of personal and sensitive information. Unauthorized access to IoT data can lead to privacy violations, identity theft, and surveillance issues.
3. **Data Integrity and Trustworthiness:**
    - Data tampering, manipulation, or corruption can undermine the accuracy and reliability of IoT systems, leading to erroneous outcomes and safety risks.
4. **Lack of Interoperability:**
    - Interoperability challenges arise when IoT devices and systems from different vendors or platforms cannot communicate and work together seamlessly. Incompatibility between devices, protocols, and standards can hinder integration efforts, limit scalability, and increase complexity.
5. **Operational Risks:**
    - IoT deployments may face operational risks such as system failures, network outages, and performance issues.
6. **Supply Chain Risks:**

  - IoT devices rely on complex supply chains involving multiple suppliers and manufacturers, increasing the risk of counterfeit components, supply chain disruptions, and compromised integrity.

7. **Regulatory and Compliance Challenges:**
   - Compliance with regulations and standards, such as data protection laws, industry regulations, and cybersecurity frameworks, can pose challenges for IoT deployments. Non-compliance may result in legal liabilities, fines, and reputational damage for organizations.

Q9. What are the various modes of attack for IoT?

1. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:**
   - DoS and DDoS attacks flood IoT devices or networks with an overwhelming volume of traffic, causing them to become unavailable or unresponsive to legitimate users.
2. **Botnets and Botnet-based Attacks:**
   - Botnets consist of compromised IoT devices controlled by a central command and control (C&C) server. Attackers can use botnets to launch various attacks, including DDoS attacks, spam campaigns, and distributed scanning.
3. **Malware and Ransomware Attacks:**
   - Malicious software (malware) targeting IoT devices can infect and compromise their functionality, allowing attackers to gain unauthorized access, steal data, or disrupt operations.
   - Ransomware attacks encrypt data on IoT devices and demand ransom payments for decryption.
4. **Credential Attacks and Brute Force Attacks:**
   - Attackers attempt to gain access to IoT devices or networks by exploiting weak or default credentials, using techniques such as brute force attacks, dictionary attacks, or credential stuffing.
5. **Man-in-the-Middle (MitM) Attacks:**
   - MitM attacks intercept communication between IoT devices and their intended recipients, allowing attackers to eavesdrop on or manipulate data exchanges. This can occur in both wired and wireless communication channels.
6. **Physical Attacks and Tampering:**

   - Physical attacks involve gaining physical access to IoT devices or infrastructure, allowing attackers to tamper with hardware components, implant malicious hardware, or extract sensitive information.
7. **Supply Chain Attacks:**
   - Supply chain attacks target vulnerabilities in the manufacturing, distribution, or procurement process of IoT devices. Attackers may compromise components, firmware, or software during production or distribution.

Q10. Explain tools available for IoT security and interoperability.
Various tools, including hardware and software platforms, network analyzers, and IoT-specific platforms, empower developers to **build**, **connect**, **analyze**, and **monitor IoT solutions** efficiently.

1. **Firewalls:**
   - A firewall is the first (of many) layers of defense against malware ,viruses and other threats. It scrutinizes and filters both incoming and outgoing data.
   - Users can also customize rules and policies based on their needs.
   - For example, it’s often necessary to create exceptions that allow certain apps to pass through the firewall so that they don’t constantly trigger false alarms.
2. **Anti-virus software:**
   - Signature-based antivirus software scans files (from any source) to make sure that there aren’t any hidden threats. And if it finds something shady or scary, it can often remove or quarantine the affected file.
   - While antivirus software certainly isn’t bulletproof — especially when it comes to zero-day threats — it’s still a critical piece of the cyber security puzzle.
3. **Anti-Spyware software:**
   - As the term implies, spyware secretly snoops on victims to see where they go online and, even more so, what they type — such as usernames and passwords, and any other confidential or personal data.
   - That’s where anti-spyware software fights back by (ideally) detecting and removing threats such as key loggers, password recorders, and so on.
4. **Eclipse IoT:**

   - Eclipse IoT offers standardized APIs, protocols, and development frameworks for device management, data exchange, and application integration. It supports interoperability testing and validation of IoT solutions.
5. **AWS IoT Device Management:**
   - AWS IoT Device Management provides tools for device registration, configuration, and monitoring, as well as firmware updates and remote diagnostics. It ensures secure and reliable operation of IoT devices in diverse deployments.
6. **OpenVAS (Open Vulnerability Assessment System):**
   - OpenVAS conducts vulnerability assessments and penetration tests to identify and address security vulnerabilities in IoT devices, networks, and applications. It helps organizations improve their security posture and resilience against cyber threats.
7. **Metasploit:**
   - Metasploit provides a range of tools and modules for conducting penetration tests, exploiting vulnerabilities, and assessing the security of IoT devices and networks. It enables organizations to simulate real-world attack scenarios and assess their security defenses.