Dated 03/04/2023

ASSIGNMENT - 2 SET-1

Name: Sahil Kaundal UID: 21BCS8197

Branch: CSE (Lateral Entry) Group: 616-A

Semester: 6th Subject Code: 20CST-357

Subject: Internet Of Things

Q1. Relate Communication Models in IoT.

Ans

IoT (Internet of Things) is a network of physical devices, vehicles, buildings, and other objects that are embedded with electronics, software, sensors, and network connectivity, which enables them to collect and exchange data. Communication models are crucial in IoT because they determine how devices exchange information with each other and the cloud.

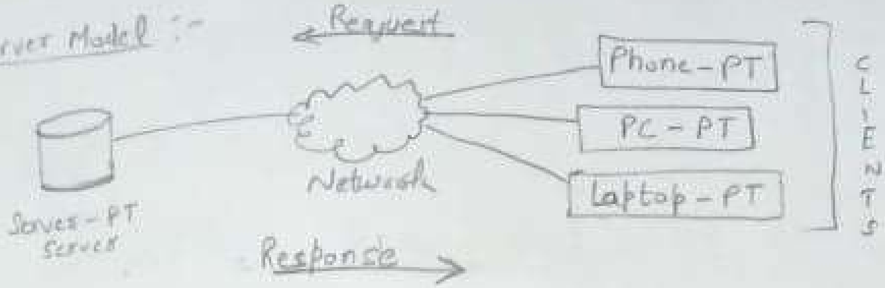
- Client-Server Model :- In this model, devices are divided into two categories : clients and servers. Clients initiate requests to servers, which then respond to the requests by providing data or services. This model is commonly used in IoT applications that involves cloud-based services.

- Publish-Subscribe Model :- In this model, devices are divided into two categories : publishers and subscribers. Publishers publish data to specific topics or channels, and subscribers subscribe to those topics or channels to receive data. This model is commonly used in IoT applications that involve real-time data streaming.

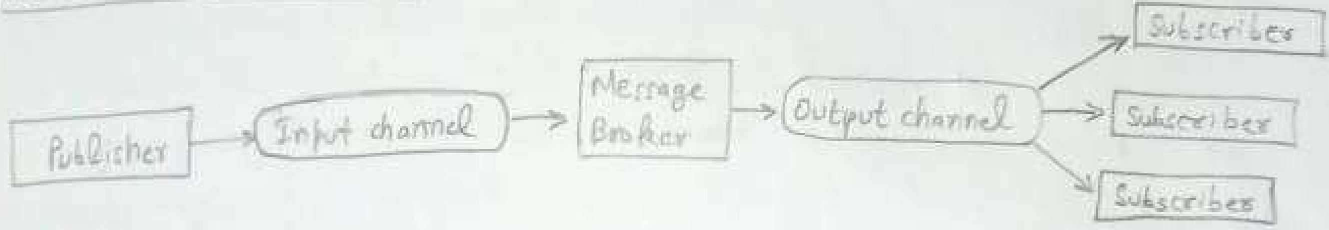
- Mesh Network Model :- In this model, devices are connected in a mesh topology, where each device is connected to multiple

Teacher Signature

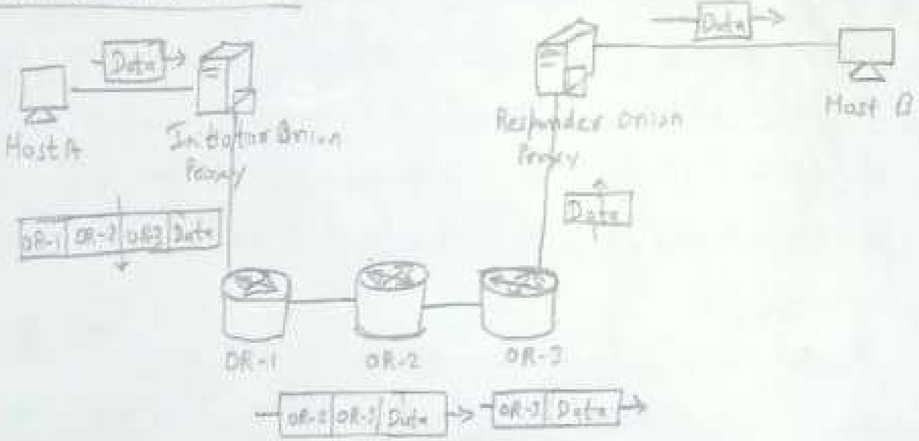
- Client Server Model :-



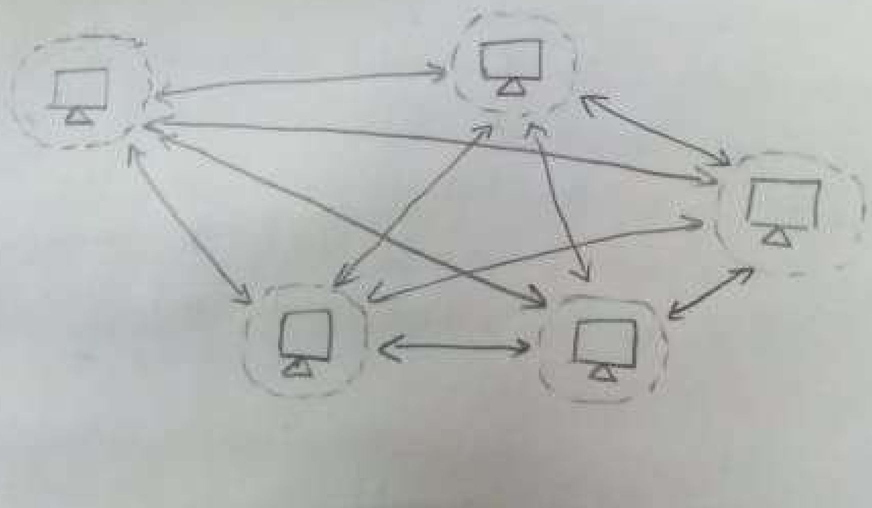
- Publish - Subscriber Model :-



- Mesh Network Model :-



- Peer-to-Peer Model :-



other devices, forming a decentralized network. This model is commonly used in IoT applications that require reliable communication and fault tolerence.

- Peer-to-Peer Model :- In this model, devices communicate directly with each other without the need for a central server. This model is commonly used in IoT applications that requires low-latency communication, such as in smart homes and industrial automation.

The choice of communication model in IoT depends on the specific requirements of the application, such as data latency, reliability, security, and scalability.

Q2. Gateways are more powerful computing devices than sensors. Justify the statement.

Ans.

The statement "Gateways are more powerful computing devices than sensors" is generally true in the context of IoT (Internet of Things) systems.

A sensor is a devices that measures and collects data from its environment, such as temperature, humidity, pressure, or motion. Sensors are typically small, low-power devices designed to operate in harsh environments, with limited processing capabilities, memory, and communication capabilities. Their main function is to capture data and transmit it to a higher-level system for further processing and analysis.

A gateway is a device that acts as an intermediary b/w sensors and the cloud or other computing systems. Gateways provide more powerful computing capabilities than sensors, including processing power, memory, storage and communication interfaces. They can perform local processing of data, run analytics algorithms, perform data filtering and aggregation, and manage network connectivity, security, and device management.

The key advantages of using gateways over sensors are:

- Processing power:- Gateways are equipped with more powerful processors, enabling them to perform complex data processing tasks that sensors are not capable of.

- Memory and storage:- Gateways have larger memory and storage capacity than sensors, allowing them to store and process more data.

- Communication interfaces:- Gateways support a wider range of communication protocols and interfaces than sensors, allowing them to connect to different types of sensors and networks.

- Device management: Gateways provide advanced device management capabilites, such as firmware updates, remote configuration, and monitoring.

- Security: Gateways can implement advanced security measures, such as encryption and authentication, to protect data and devices from cyber threats.

Gateways plays a crucial role in IoT systems by providing a bridge between sensors and the cloud or other computing systems.

Q3. Read the following paper and List the mentioned Security challenges

Ans:-

Following are security challenges :-

1. Authentication and Access Control : Authentication is any process by which a system verifies the identity of a user who wishes to access control is typically based on the identity of user who requests access to a resource, authentication is essential to effective security.

2. Network Slicing Security :- It can be dedicated to one enterprise customer, or shared by multiple tenants.

3. Secure Communication :- When two entities are communicating and do not want a third party to listen in.

4. Virtualization Security :- Security solutions that are software-based and designed to work within a virtualized IT environment.

5. IOT Security :- It is the technology segment focused on safeguarding connected devices and networks in the internet of things.

6. Denial of Service (DOS) :- It is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

7. Network function Virtualization (NFV) :- It is the replacement of n/w appliance hardware with virtual machines.

8. Privacy Challenges

9. Supply Chain Security :- Involves both physical security related to product and cybersecurity for s/w and services.

Q4. With proper example explain Back-End Data Sharing Model.

Ans.

The back-end data sharing model is a common approach to data sharing in modern web applications. In this model, data is stored on the server-side, and different client applications can access and manipulate the data through an API (Application Programming Interface).

let's take the example of a social media platform, which allows user to post photos, videos and comments, and follow other users. In this case, the back-end data sharing model would work as follows:

- Data storage :- The platform would use a database or a distributed storage system to store the data, including user profiles, posts, comments, and relationships between users.

- API endpoints :- The platform would expose a set of API endpoints that client applications can use to interact with the data. For eg, the API could include endpoints for creating and retrieving user profiles, posting photos and videos, commenting on posts, and following or unfollowing other users.

- Authentication and authorization :- The API would require authentication and authorization to ensure that only authorized users can access and manipulate the data. This could be achieved through the use of tokens or API keys, and by implementing different levels of access based on user roles and permissions.

- Client applications :- The platform would provide client applications.

Dated.....................

such as mobile apps or web apps, that use the API to access and manipulate the data. for eg, a mobile app could use the API to display a user's timeline, upload a photo or video, or comment on a post.

- Data Synchronization :- The API would ensure that the data is synchronized across different client applications and devices. for eg. if a user posts a photo from their mobile app, the data should be immediately available on the web app and any other client applications that the user is using.

Overall, the back-end data sharing model provides a flexible and scalable approach to data sharing in modern web applications. By storing the data on the server-side and exposing it through a well-defined API, different client applications can access and manipulating the data in a consistent and secure way. This approach also enables developers to build client applications using different technologies and platforms, while still being able to share and synchronize the same data.