SMVS
Page No.
Date : / /

1 Draw and Explain Building Block of IoT?

=> Iot consists of multiple components working together to collect, process, transmit and store data for decision making.

This are the Key Building Block of IOT:

1 Sensors: It is present in Data Collection Layer and responsible for gathering real-time data from the environment.

They can detect various physical and environmental parameter.

Sensors and Actuators
Processors
Gateways and Communication
Application
Database

SMVS
Page No.
Date : / /

Ex. Temperature sensors, Motion Sensors, Humidity Sensors

2. Actuators: The Actuators are present in Action Layer and it is device that convert digital signals into physical actions.

They receive commands from processors and perform operations like opening valves, rotating motors or switching lights on/off.

3 Processors: Processors are present in Processing Layer and it acts as the "brain" of an Iot system, managing data processing and decision-making.

It can be a microcontroller or a microprocessor depending on the complexity of the application

Processor collects data from sensors, enable real-time decision-making etc.

SMVS
Page No.
Date : / /

4 Gateways : Gateway present in communication Layer and it act as a bridge between IoT devices and the server.

Gateways used for converting different communication from one protocol to other protocol.

Also provides the security by providing encryption and authentication.

5 Applications : Application are present in User Interface Layer which allows users to interact with IoT systems, monitor data and control devices remotely.

These can be mobile apps, web dashboards or desktop software.

6 Database / Data Storage :

IoT generates vast amounts of data that must be stored and analyzed for insights.

Data storage enables historical analysis and AI-based predictions.

SMVS
Page No.
Date : / /

2 Enlist the good practices For securing IoT Systems.

=> Securing IoT Systems is crucial to prevent cyber threats, data breaches and unauthorized access.

This are the some Good Practices to secure IoT system.

(A) Device Security:

To Secure Device, Uses -
- Use Strong or Multi Factor Authentication
- Secure Boot and Firmware Integrity
- Regular Updates etc.

(B) Network Security:

To Secure Network, Use
- Segment IoT Networks
- Use Secure Communication Protocals
- Restrict Unauthorized Access

SMVS
Page No.
Date : / /

(C) Data Security:

To Maintain Data Security:
- Use Encrypt Data Storage and Transmission
- Minimize Data Collection
- Implement Secure APIs

(D) Identity and Access Management:

To Maintain this security:
- Use Role-Based Access control
- Regular Access Audits.
- Unique Device Identities

(E) Monitoring and Incident Response:

To Secure Monitoring Process:
- Use or Set up Alerting System
- Log and Monitor IoT Activities
- Develop an Incident Response Plan

(F) Secure Coding Practices or Perform Security Testing or Implement Secure Software Updates.

(G) Security Awareness and Training:

Educate users and employees and EnForce security Policies.

3 Explain Physical and Logical Design in IoT.

=> Physical Design:

The Physical design of an IoT system consists of the hardware components.

It includes sensors, actuators, connectivity modules, processors and storage elements that enable devices to function and communicate effectively.

Connectivity	Processor	Audio / Video	I/O Inter-
USB Host	CPU	Interface	face
Ethernet		HDMI	
		RCA video	UART
Memory Interface	Graphics	Storage Interface	SPI
NAND/NOR	GPU	MMC	I2C
DDR2/DDR3		SDIO	

SMVS
Page No.
Date : / /

(A) Things (Devices):

This are the essential components of an IoT systems, each with a unique identifier.

They collect, process and act on data from the environment.

Functions : Sensing, Actuation, Processing, Monitoring

(B) Connectivity Devices:

These devices enables communication between nodes devices (Things) and server.

There are Two types of Connectivity:

(i) Wired Connection:
- USB Ports : Used For data transfer b/w IoT devices and computer.
- Ethernet Ports : Provide High-speed internet

(ii) Wireless Connection:
- Wi-Fi : High speed connectivity
- Bluetooth, Zigbee, Cellular etc.

(C) Processors: It act as the brain of an IoT system, handling data processing, decision-making and communication.

Functions: - Sensors data analysis and Filtering
- Execution of communication Protocols.
- Controling actoator etc.

(D) Audio / Video Interface:

Enable IoT device to capture, transmit and process audio and video data.

Comman Interface:
- HDMI - For High-resolution video and audio output
- RCA - Analog Video and Audio connection etc.

(E) I/O Interface:

Provide connection points for sensors and actuators to communicate with the processing unit.

SMVS
Page No.
Date : / /

Types :
(i) UART : Serial Communication Interface for Low-speed data transfer.
(ii) SPI : High-speed communication for connecting multiple devices.
(iii) I^2C : Used for communication b/w sensors and microcontroller

(E) Storage Interface :

IoT device required onboard storage for buffering data.

Storage Options :

(i) SD Cards : Used in devices like Raspberry Pi for storing logs, Firmware.

(ii) MMC Cards : Embedded storage used in some IoT sensors.

(iii) SDIO : Provide additional memory and wi-fi connectivity.

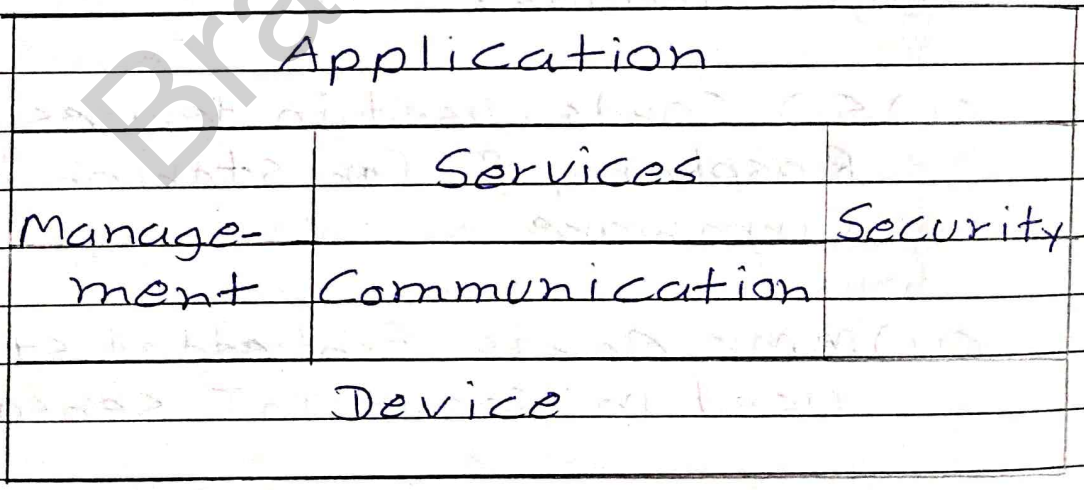
=> Logical Design:

The Logical design of an IoT system includes,

(A) Functional Blocks
(B) Communication Model
(C) Communication APIs

A Functional Blocks:

Functional blocks that provide the system for identification, sensing, actuation, communication and management.



(1) Application Block: Acts as a user interface for monitoring and controling IoT devices.

Allows users to analyze system

SMVS
Page No.
Date : / /

performance and take necessary actions.

(2) Management Block : Responsible for administration and coordination of IoT components.

Manages device configuration, updates and troubleshooting.

(3) Services Block : Ensures IoT devices work efficiently and deliver accurate information.

Provides Function like :
Device Monitoring and Control
Data Publication and Deletion
System restoration.

(4) Communication Block : Facilitates data exchanges between devices, servers and applications.

Uses wired and wireless communication protocol.

(5) Security Block : Ensures data integrity, privacy and protection from cyber threats.

Implements Authentication, encryption and access control.

(6) Device Block: Comprises physical IoT sensors, actuators and controllers.

Collects data from the environment and send to other functional block for processing.

B Communication Models:

IoT systems rely on various communication models to exchange data between devices, servers and users.

This are the Communication model e use in IoT.

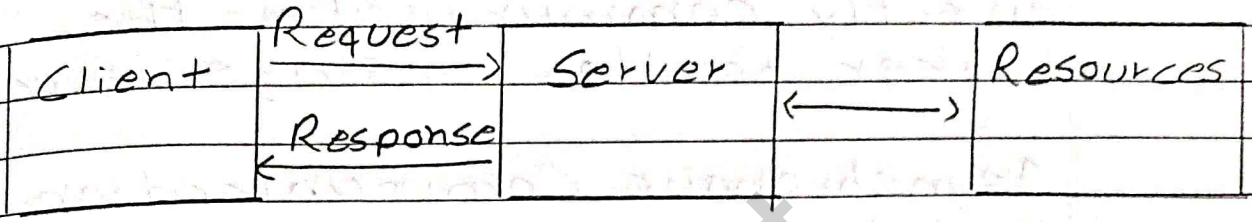
(1) Request - Response Model:

It includes two main entities: the client and server

The Client sends a request and the server responds with the requested data.

SMVS
Page No.
Date : / /

Server is connected with Resources and this is synchronous communication mechanism.

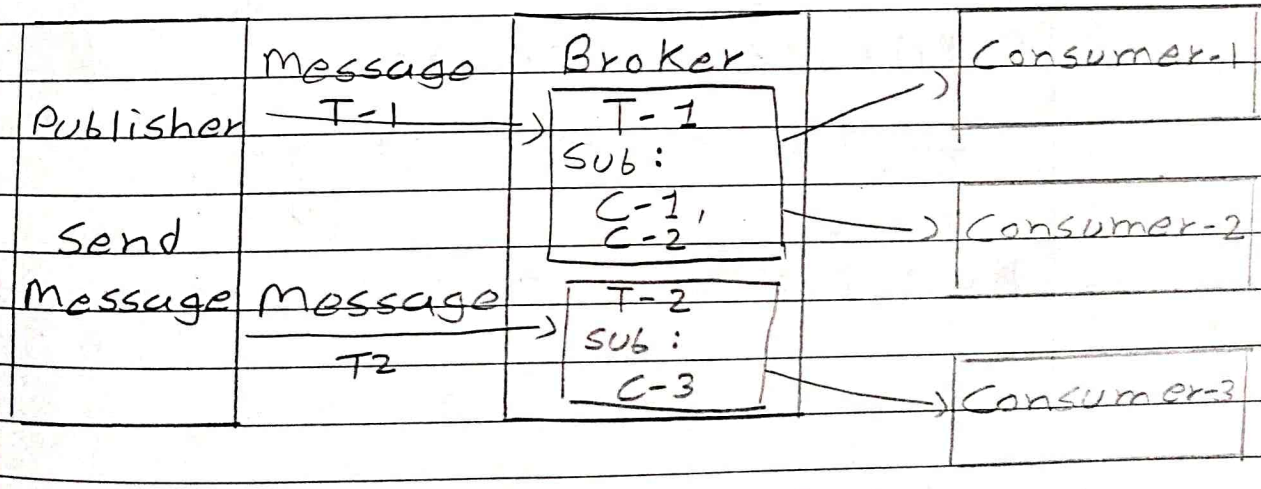


Suitable For applications where real-time data is not critical and use HTTP/HTTPs Protocol.

(2) Publish - Subscribe Model:

It includes main Three entities:

(i) Publisher : Sends Messages



(ii) Broker : Manages messages and topics.

(iii) Consumer: Receive message by subscribing to topics.

Publishers and Subscribers don't directly communicate - the broker handles message delivery.

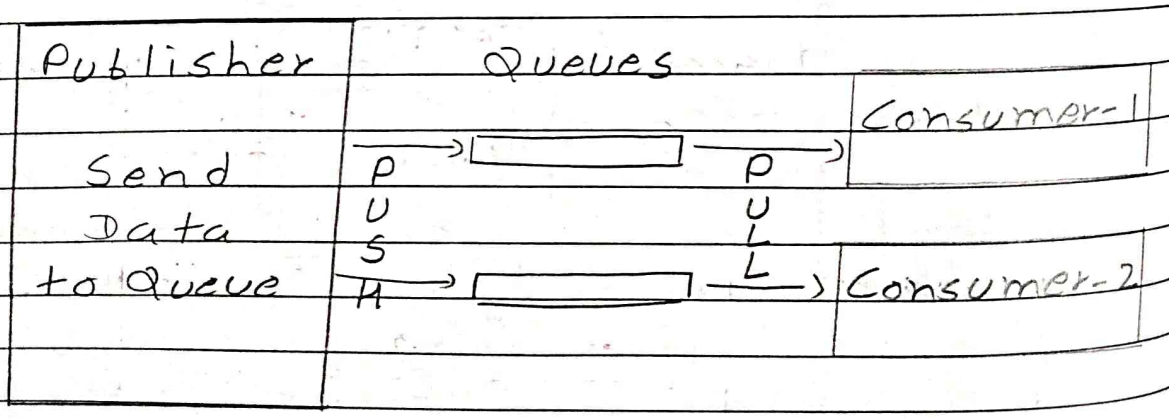
Asynchronous Communication Model.

(3) Push - Pull Model:

It involves three main entities:

(i) Publisher: Generates and pushes data.

(ii) Queue: Temporarily stores message.



(iii) Consumer: Pulls data from the Queue when needed.

SMVS
Page No.
Date : / /

It is suitable for Large-scale systems where continuous data flow is needed.

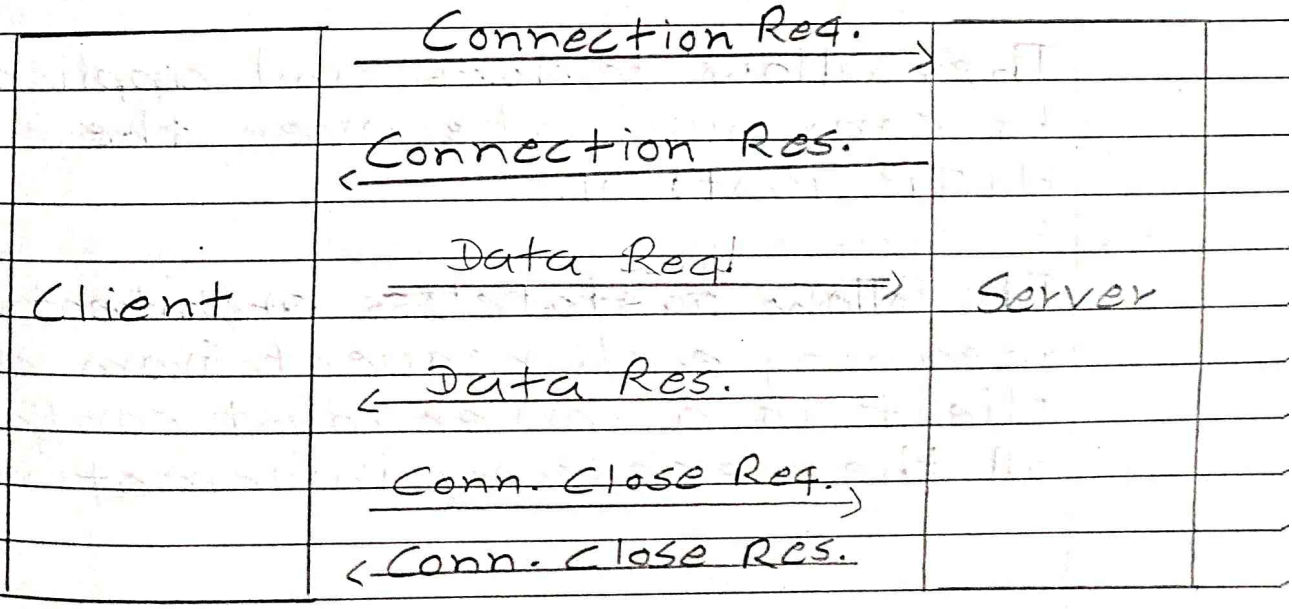
(4) Exclusive Pair Model :

It involves two main entities : the client and server.

-> Working :

1) Client send connection request to server and server response by accepting request.

2) Client and Server pass the data
3) Client send connection close request and server response.



C Communication APIs:

APIs plays a crucial role in IoT by enabling devices, applications and services to communicate efficiently.

Different API models define how data is shared, accessed and controlled in IoT ecosystem.

This are the communication APIs are used.

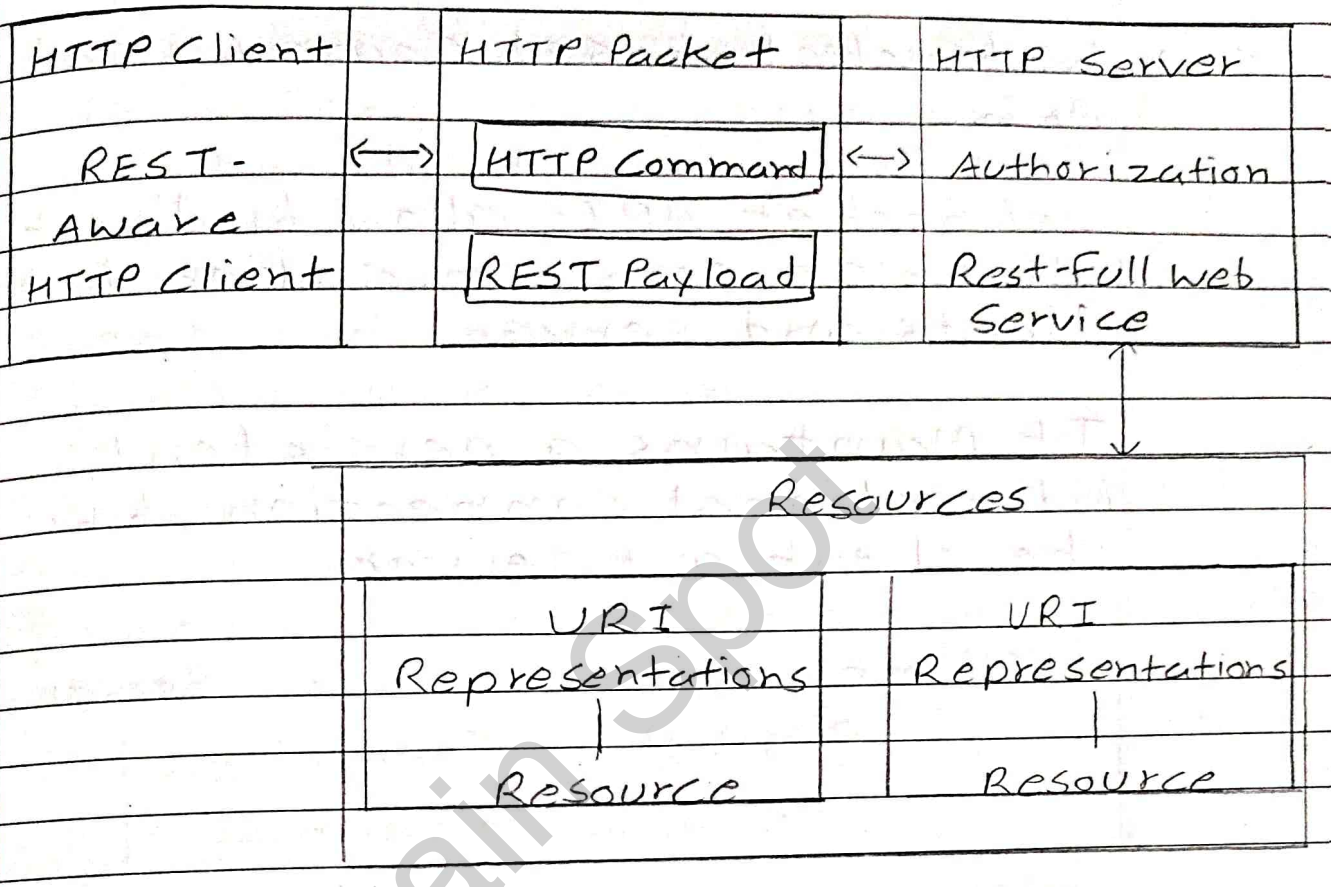
C1) RESTful APIs:

RESTful APIs are one of most widely used communication APIs in IoT.

They allow devices and application to communicate over the HTTP Protocol.

It follow a stateless architecture, meaning each request from a client to a server must contain all the necessary information.

SMVS
Page No.
Date : / /



It is work, based on HTTP methods like GET, POST, PUT, DELETE.

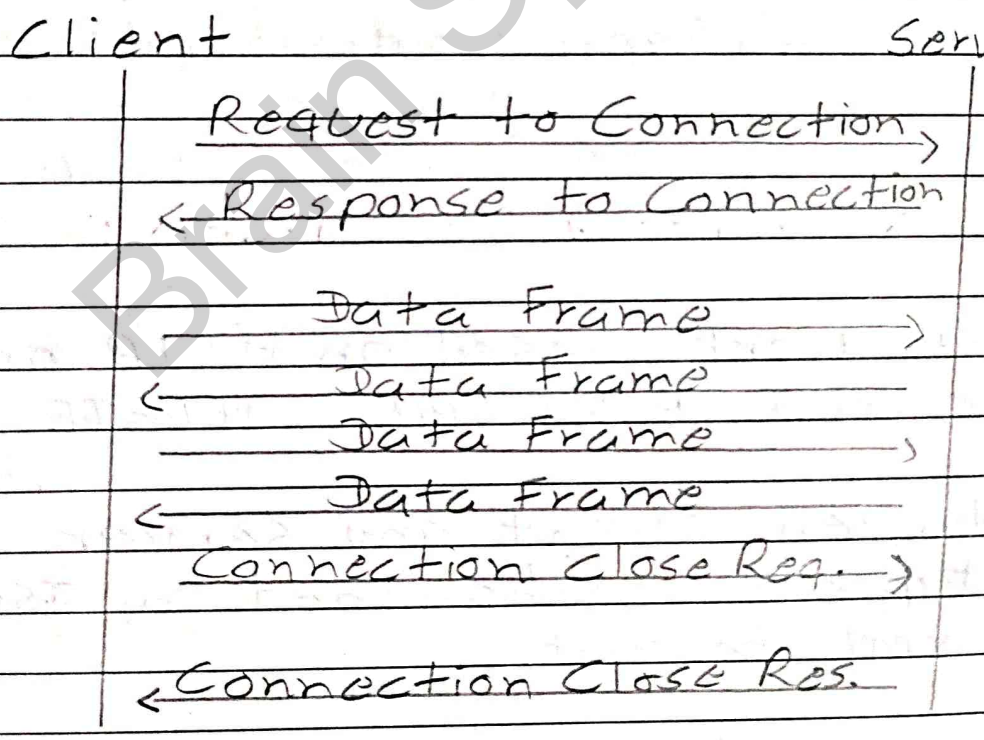
Between Client and Server, Data is typically exchanged in JSON or XML Format.

This API is easy to implement and works well with Cloud-based IoT services.

(2) WebSocket-based Communication APIs.

WebSocket APIs allow bi-directional Full duplex communication between clients and server.

It maintains a persistent, bidirectional connection b/w the client and server.



In this Communication, Do not require a new connection to be setup for each message to be sent.

SMVS
Page No.
Date : / /

WebSocket Communication begins with a Connection setup request sent by client to the server.

After the connection setup, the client and server can send data to each other.

It reduce the network traffic and latency as there is no overhead for connection setup and termination request for each message.

4 Explain Layered IoT Architecture.

=> The IoT is a concept where physical devices are embedded with sensors, software and connectivity to exchange data over the internet.

There are 4 Layer in IoT Architecture.

(1) Application Layer
(2) Data Processing Layer
(3) Network Layer
(4) Sensing Layer

(1) Sensing Layer: 1st Layer.

This Layer is responsible for data collection from the environm

It includes sensors and actuators to monitor parameter like temperature, light etc.

It uses wired or wireless commun cation protocol to send data to the network layer.

Application Layer	Smart Applicatio
Data Processing Layer	Process Informatio
Network Layer	Data Transmissio
Sensing Layer	Data Gathering

(2) Network Layer:

It manages communication and connectivity between the devices.

SMVS
Page No.
Date : / /

It includes gateways and routers to connect devices to the internet.

It also implement security features like encryption and authentication.

(3) Data Processing Layer:

This Layer handles data analysis and interpretation.

It collects raw data from devices and processes it for meaningful insights.

It uses data management systems, analytics platforms and machine Learning algorithms.

(4) Application Layer:

It is topmost layer interacting with end users.

Provides user-Friendly interfaces like mobile apps, web portal etc.

Also includes analytics tools for data visualization and decision-making.

SMVS
Page No.
Date : / /

5 What do you mean by IoT Gateway ? What is the role of a Gateway in IoT?

=> An IoT Gateway is a hardware device or software that acts as a bridge between IoT devices and the cloud or external network.

It facilitates communication by translating protocols, aggregating data before transmit data to the Network.

=> Role of IoT Gateway in IoT:

A Communication Bridge:

Connects to IoT devices with the cloud using different communication technologies.

B Protocol Translation:

Converts data from different IoT communication protocol into a standardized formate.

SMVS
Page No.
Date : / /

C Data Aggregation and Processing:

Collects and processes data from multiple IoT devices before sending it to the cloud.

D Security and Encryption:

Provides an additional security layer by encrypting and securing IoT device communications.

E Device Management and Diagnostics:

Monitors and controls multiple IoT devices remotely and performs devices diagnostics and updates to ensure smooth operation.

F Scalability and Network Management:

Supports a large number of IoT devices and balances network traffic efficiently.

Can be scaled up or down based on the number of connected devices.

Date : / /

=> Advantages :

- Protocol Translation
- Data Aggregation
- Edge Computing
- Security Enhancement
- Cost-Effective

=> Disadvantages :

- Single Point of Failure
- High Initial Cost
- Latency Issues
- Security Risks.

6 What is cloud ? What is the role of cloud platform in IoT ?

=> Cloud Computing is an internet-based computing model that provides on-demand access to shared computing resources such as server, storage, database Networking etc.

Users can provision resources automatically without human intervention.

SMVS
Page No.
Date : / /

=> Role of Cloud Platform in IoT:

A Centralized Data Storage and Management:

IoT devices generate massive amounts of data from sensors, cameras and other resources. So, cloud platform provide secure, scalable storage solution.

B Real-Time Data Processing and Analytics:

The cloud enables real-time data processing and analytics to make quick decisions.

C Scalability and Flexibility:

The cloud allows IoT networks to grow without additional infrastructure and resources are allocated dynamically based on demand.

D Security and Privacy:

Cloud platforms offers encryption, authentication and access control for IoT data security.

Date : / /

E Remote Access and Device Management:

IoT devices can be monitored and controlled from anywhere via cloud-hosted dashboards.

F Cost-Effectiveness and Resource Optimization:

Cloud Computing eliminates the need for on-premises infrastructure which reducing costs.

G IoT as a Service:

Many cloud providers offer IoT-as-a-Service, allowing businesses to deploy IoT solution quickly.

H Improved Connectivity and Interperability:

The cloud ensures seamless connectivity between IoT devices using REST APIs and WebSockets.

E Remote Access and Device management:

IoT devices can be monitored and controlled from anywhere via cloud-hosted dashboards.

F Cost-Effectiveness and Resource Optimization:

Cloud Computing eliminates the need for on-premises infrastructure which reducing costs.

G IoT as a Service:

Many cloud providers offer IoT-as-a-Service, allowing businesses to deploy IoT solution quickly.

H Improved Connectivity and Interperability:

The cloud ensures seamless connectivity between IoT devices using REST APIs and WebSockets.

SMVS
Page No.
Date : / /

* What is IoT and Characteristics of IoT.

=> The IoT is a concept where physical devices are embedded with sensors, software and connectivity to exchange data over the internet.

This enables seamless automation, monitoring and control of devices without human intervation.

IoT Follows standardized protocols to enable seamless communication b/w different device.

Each IoT device has a unique identity for data exchange.

=> Characteristics of IoT:

A Dynamic and Self-Adapting:

IoT systems dynamically adjust based on environments changes, user interactions and sensor inputs.

B Self-Configuring:

IoT devices can be plug-and-play meaning they can connect and configure automatically with minimal manual setup.

C Interperability:

IoT operates over multiple communication protocols such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN etc.

D Unique Identity:

Each IoT device has a unique identifier to ensures secure and efficient device management.

E Seamless Information Exchanges:

IoT devices collect and share real time data over networks, enabling automation and remote monitoring.

Page No.
Date : / /

E Security and Privacy:

IoT devices are prone to cyber threats, so they include encryption, authentication and security protocols.