UNIT-2.

Introduction to IOT

*Definition: The internet of things (IOT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices.

→ It has dynamic global network infrastructure with self configuring capabilities based on standard & interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual. Network and use intelligent interfaces.

* characteristics:

1. Dynamic & self adapting → IOT devices and system may have the capability to change dynamically depending upon the system and operating conditions or sensed environment. eg. the surveliance cameras can change their modes based on day or night.

2. Self configuring → IOT devices have self-configuring capability which allows large number of devices to work together to work provide certain functionality they can change their networking and update the software automatically. eg. weather monitoring system.

3. Interoperable communication protocol → IOT devices can communicate with number of interoperable communication protocols without any special effort.

4. Unique Identity → Each IOT device has an unique identity and a unique identifier. (such as IP address)

5. Integrated into Information Network → IOT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

* Applications of IOT:

Different applications of IOT include:

1. Home
   - smart lighting
   - smart appliances
   - Smoke / Gas detectors
2. Cities
   - Smart Parking
   - Smart roads
   - Emergency response
   - Health monitoring
3. Environment
   - weather monitoring
   - Air Pollution monitoring
   - Noise pollution "
   - forest fire detection
4. Agriculture
   - Smart irrigation
   - Green house control
5. Energy
   - Smart grids
   - Renewable energy systems
6. Health & Lifestyle
   - Health & fitness monitoring
   - wearables electronics
7. Retail
   - Inventory management
   - Smart payments
   - Smart vending machine

Physical Design of IOT:

The physical design of IOT consists of the things in IOT and IOT protocols.

1. Things in IOT →

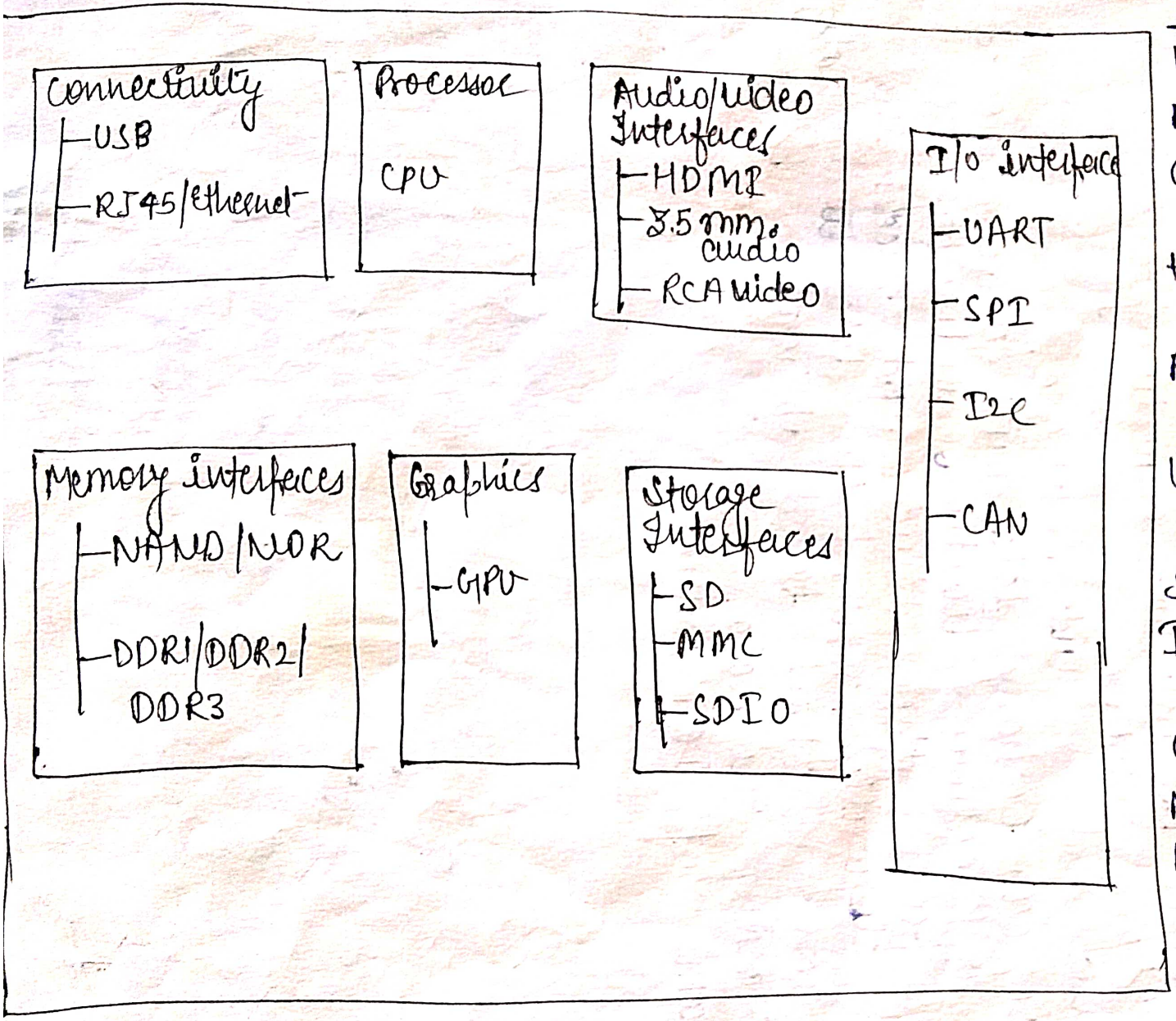
→ The things in IOT is usually refess to IOT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.

→ IOT devices consists of several interfaces for connecti n to other devices both ~~to~~ wired and wireless whic includes:

① I/O interfaces for sensors
② Interfaces for internet-connectivity
③ Memory & storage.
④ Audio and video interface.

→ IOT devices can exchange data with other connected devices and applications (directly or indirectly) or collect data from other devices and process the data either logically or send the data to centrali ed servers or Cloud based application back- ends for processing the data.

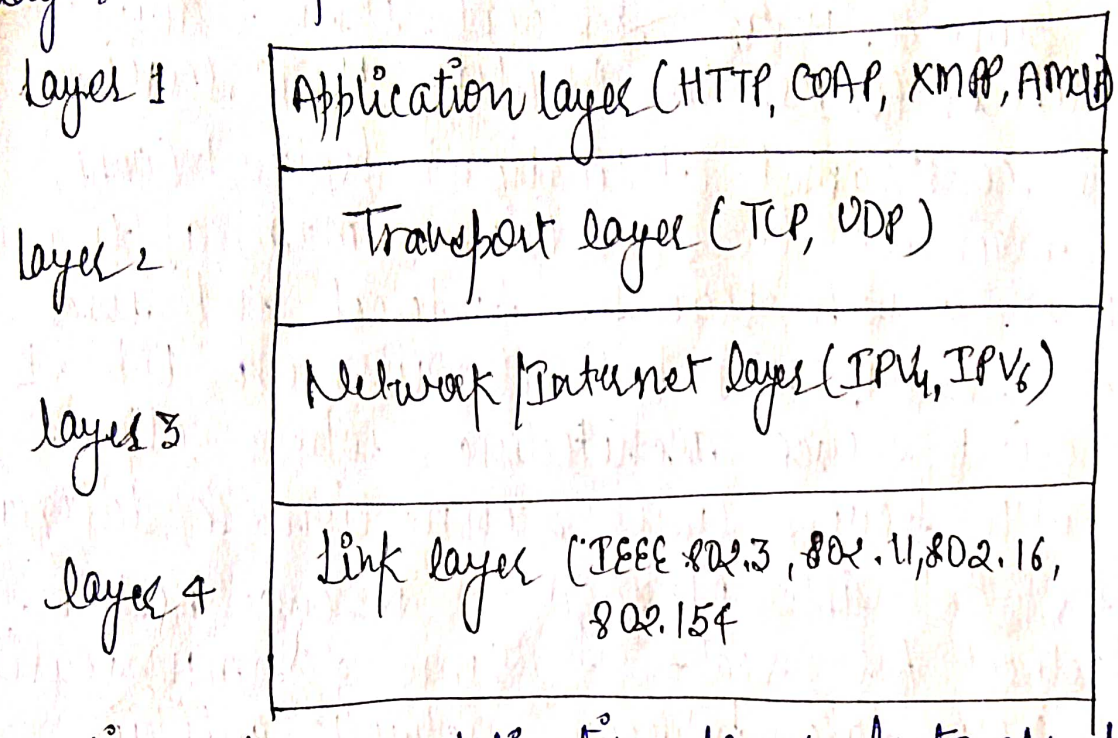
~~Diagram~~ of IOT Device.



Abbreviations:

USB - Universal Serial Bus
RJ45 - Registered Disk
CPU - Central Processing Unit
HDMI - High definition Multimedia Interface
RCA - Radio ~~corp~~ corporation of America.
UART - Universal Asynchronous Receiver Transmitter
SPI - Serial peripheral interface
I2C - Inter Integrated circuit
CAN - controller network.
NAND - a logic gate
NOR - a logic gate
DDR - Double data rate
GPU - Graphics processing unit
SD - Secure digital
MMC - Multi Media card
SDIO - Secure digital Input Output.

IOT layers & protocols: IOT has 4 layers: Application layer, Transport layer, Network, Internet layer. Each layer has some sort of functionality and each layer has protocols.



Application layer → application layer protocols define how the applications interface with the lower layer protocols to send the data over the network. The application data, typically in files, is encoded by the application layer protocol and encapsulated in transport layer protocol which provides connection. Port numbers are used for application addressing. (like port 80 HTTP, 22 for SSH etc.)

Websocket → This protocol allows full duplex communication over a single socket connection for sending messages between client & server. Websocket is based on TCP and allows streams of messages to be sent back & forth between client & server while keeping TCP connection open.

HTTP → stands for Hypertext Transfer Protocol which forms the foundation of the world wide web (www). The protocol follows a request-response model where a client sends requests to server using HTTP commands, HTTP is a stateless protocol. HTTP protocol uses Universal Resource Identifiers (URI's) to identify HTTP services.

CoAP → stands for constrained application protocol (CoAP) which helps machine to machine (M2M) applications. like HTTP CoAP is a web transfer protocol and uses request-response model. This protocol runs on top of UDP, CoAP uses client server architecture where clients communicate with servers using connectionless datagrams.

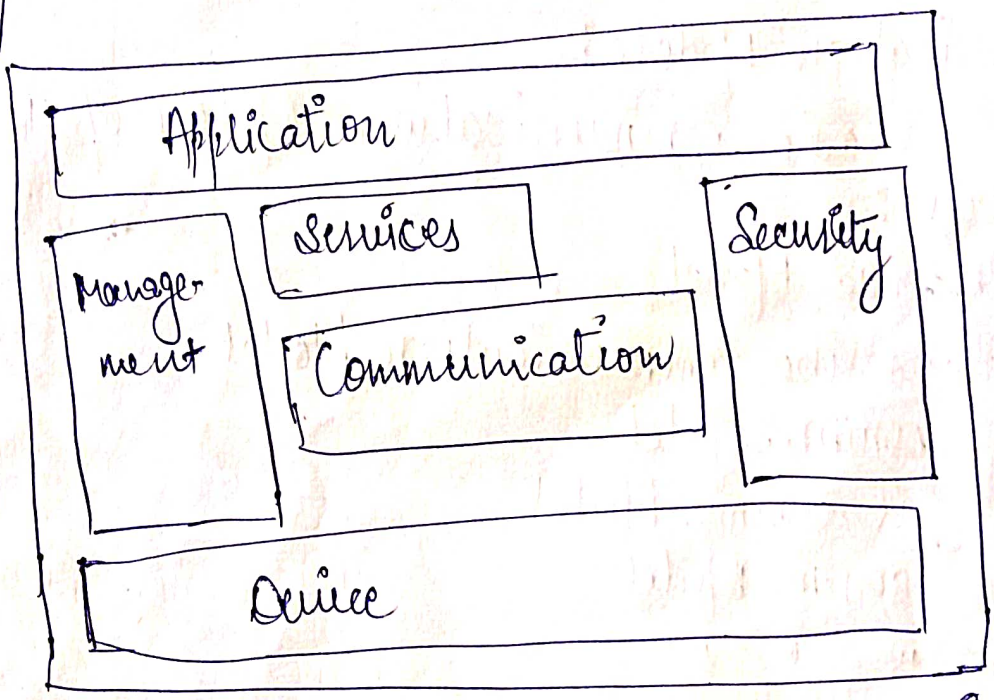
XMPP → stands for Extensible Messaging & Presence Protocol. It is a protocol for real-time communication and streaming XML data between network entities. XMPP powers wide range of applications including messaging, gaming, multi-party chat & voice/video calls.

MQTT → stands for Message Queue Telemetry Transport. It is an open application layer protocol for business messaging. MMQP supports both point to point and Publisher subscriber Models, routing and queing.

Logical Design of IOT :

→ abstract representation of the entities
→ processes without going into the low level specifics of the implementation.

IOT functional Block →
An IOT system consists of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication & management.



Application → IOT application provides an interface that the users can use to control & monitor various aspects of an IOT system.

Security → It secures the IOT system by providing functions such as authentication, authorization & data security.

Management → Management functional block provides various functions to govern the IOT system.

Services → An IOT system uses various types of IOT services such services for device monitoring, device control service, data publishing service & services for device discovery.

Communication → The communication block handles the communication for the IOT system

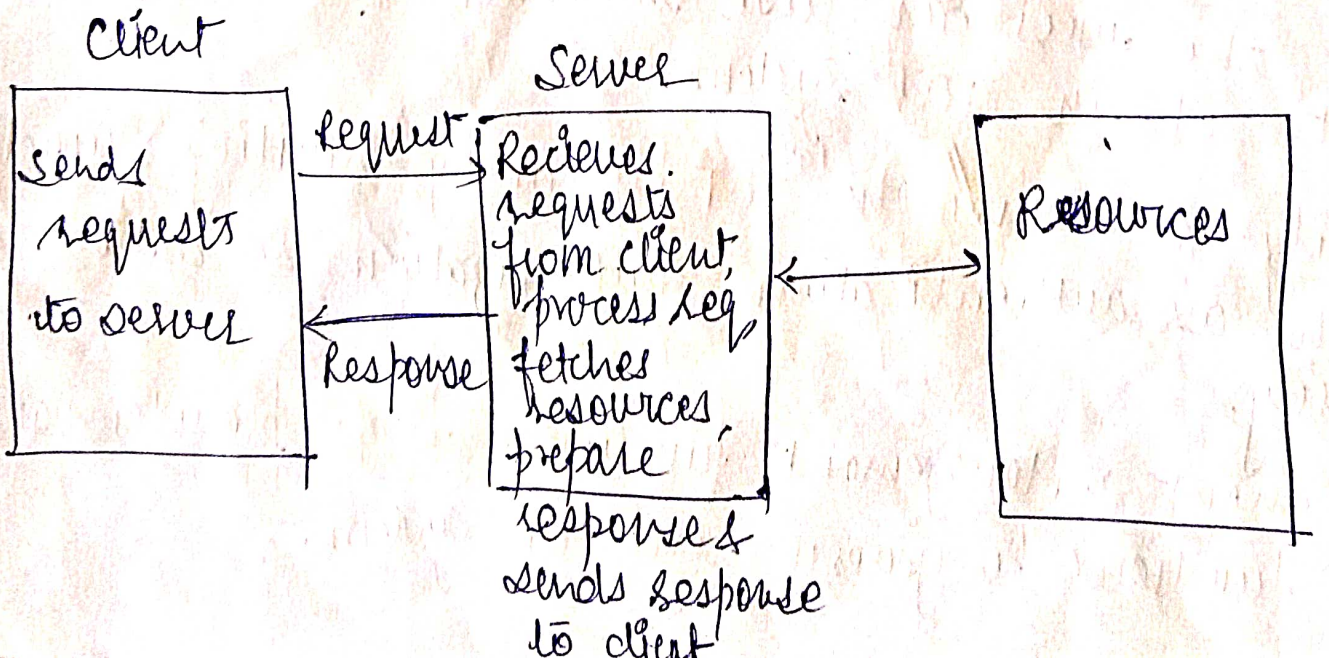
Device → An IOT system comprises of devices that provide sensing, actuation, monitoring and control functions.

IOT communication Models:

There are 6 basic communication Models of IOT exists. They are:

i) Request - Response Model
ii) Publish Subscribe communication Model
iii) Push - Pull comm. Model
iv) Exclusive pair comm. Model
v) REST - based comm. Model
vi) Websocket- " " "

1. Req. - Response Model:



2. Publish subscribe communication Model :

→ It is a communication model that involves publishers and consumers.

→ Publishers are the source of data. Publishers send to the topics which are managed by the broker. Publisher are not aware of the consumers.

→ consumers subscribe to the topics which are managed by brokes.

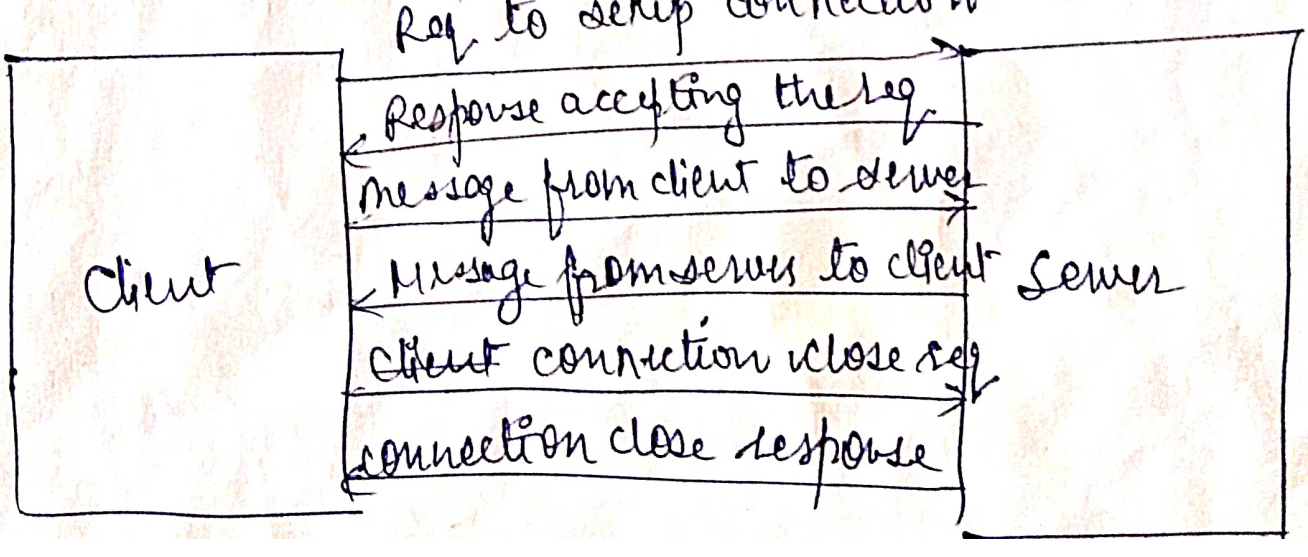
→ When the broker recieves data for a topic from the publisher, it sends the data to all the subscribed consumer.

3. Exclusive pair communication Model :

→ Exclusive pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and the server.

→ Once the connection is set up it remains open until the client sends a req. to close the connection.

→ Client & server can send messages to each other after connection setup.

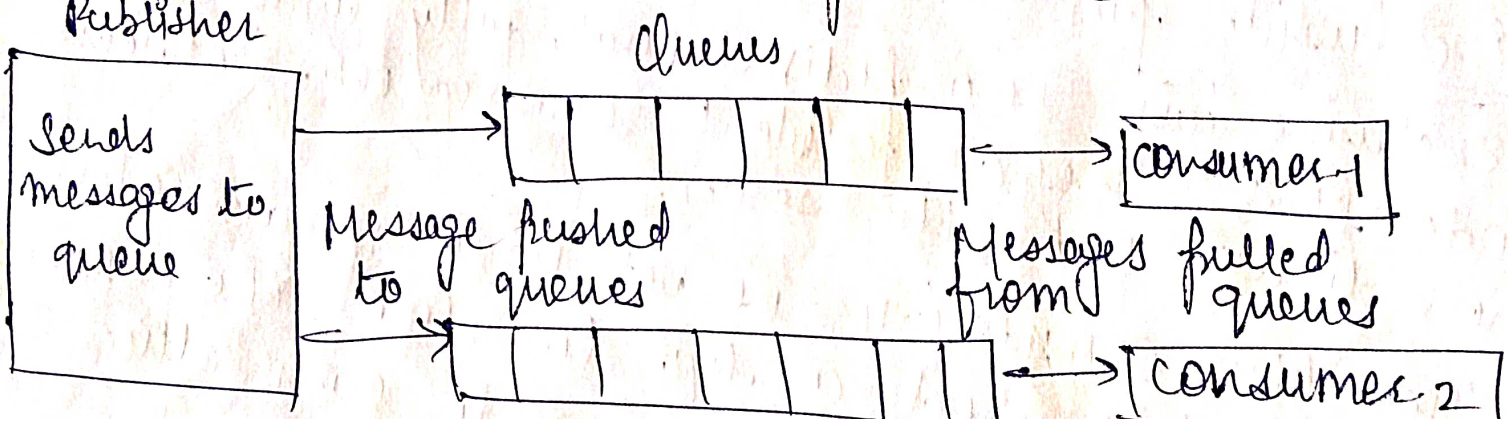


4. Push - Pull communication Model :

→ Push-pull is a communication model in which the data producers push the data to queues and the consumers pull the data from queues. Producers do not need to be aware of consumers.

→ Queues help in decoupling the messaging between the producers and consumers.

→ Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull data.

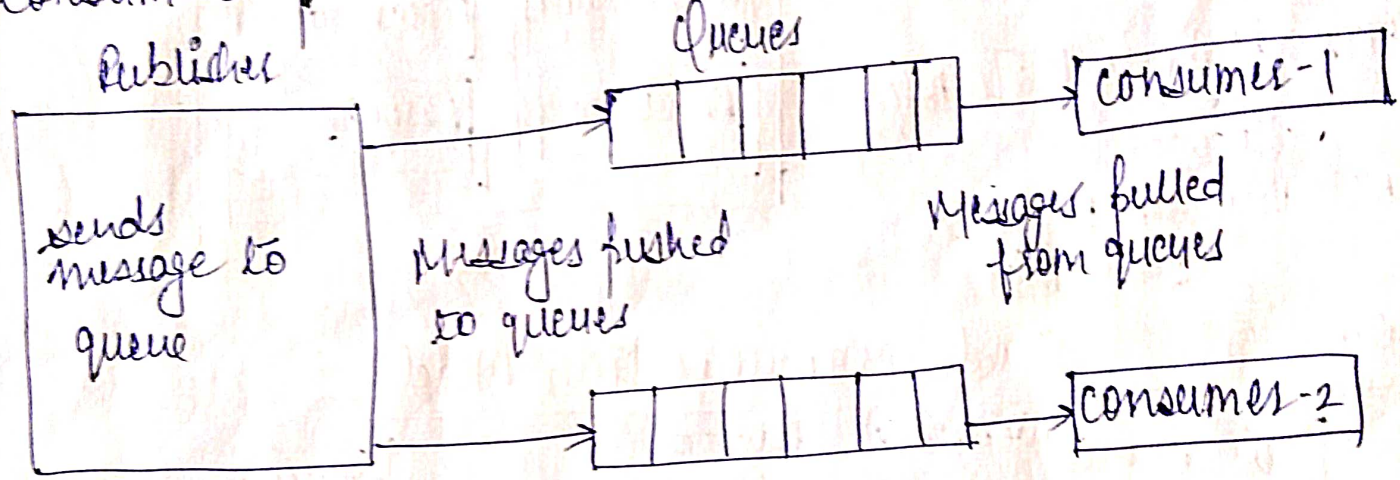


Push-Pull communication Model:

→ Push-pull is a communication model in which the data producers push the data to queues and the consumers pull the data from queues producers do not need to be aware of consumers.

→ Queues help in decoupling the messaging between the producers and consumers.

→ Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which consumers pull data.

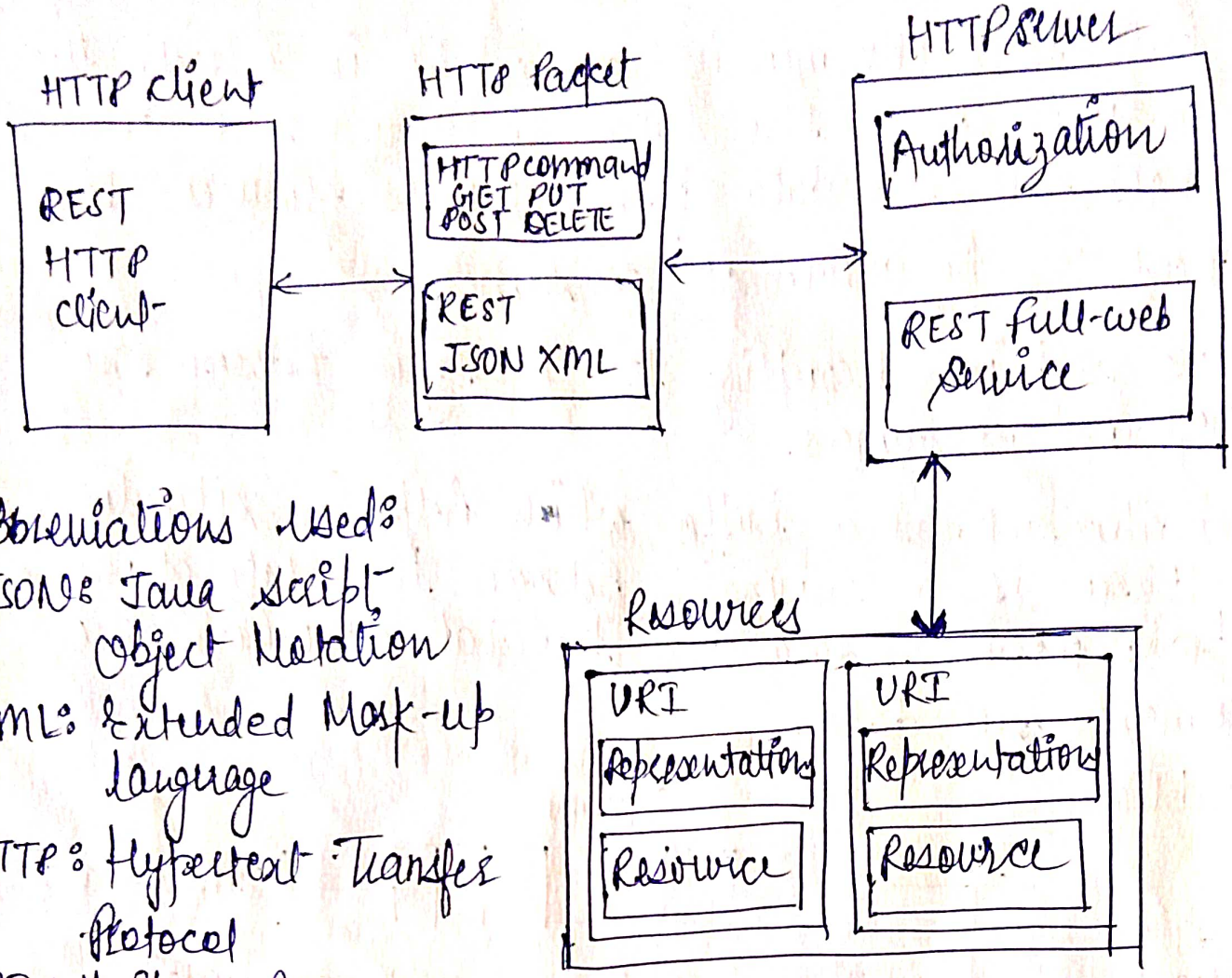


5. REST Based communication Model:

→ Representational State Transfer (REST) is the set of architectural principles by which we can design web services and web APIs (Application Programming Interfaces) that focus on system's resources and how resource states are addressed and transferred.

→ REST APIs follows the request-response communication model.

→ REST architectural constraints apply to the components, connectors and data elements within a distributed hypermedia system.



Abbreviations used:

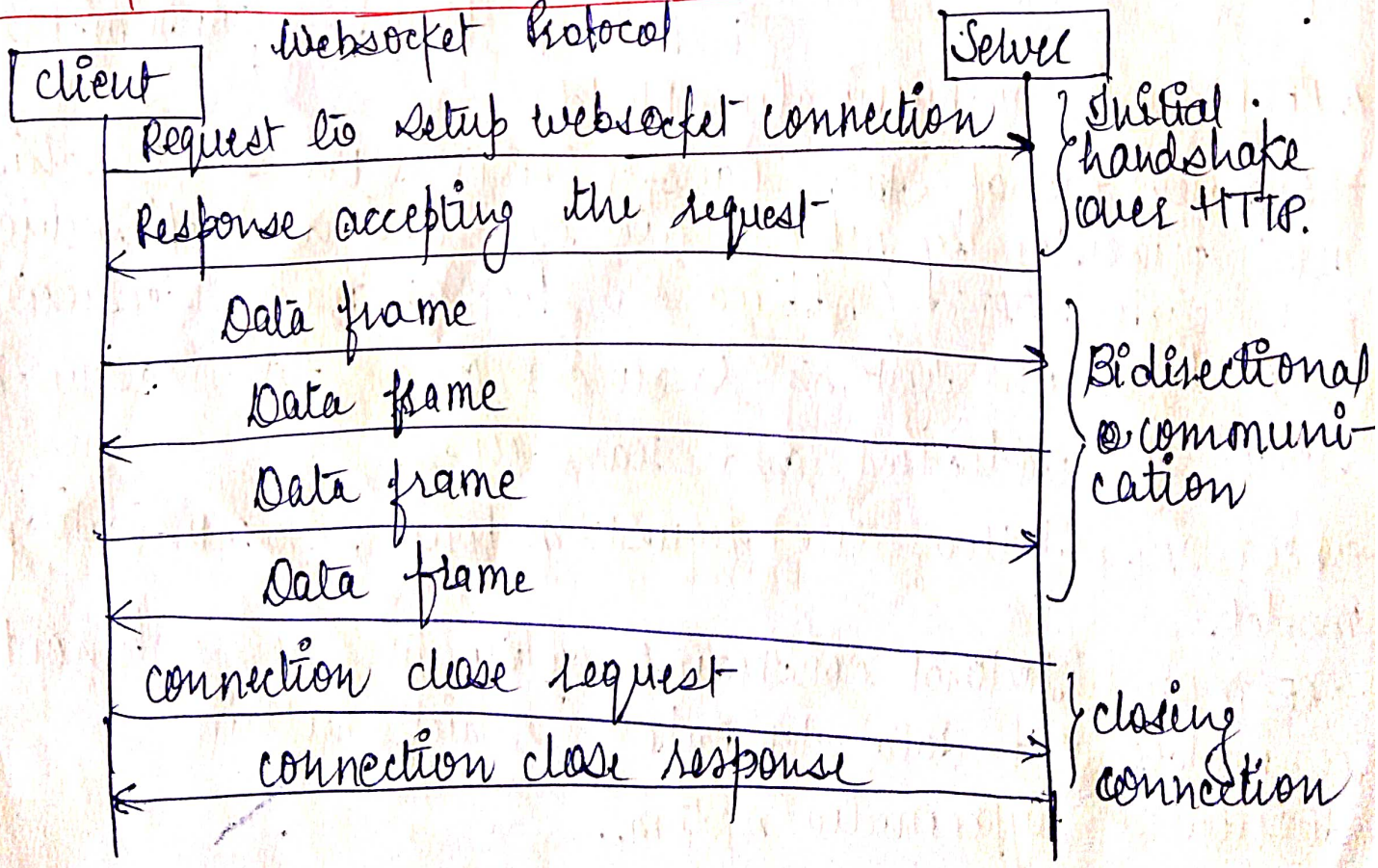
JSON: Java script Object Notation

XML: Extended Mark-up language

HTTP: Hypertext Transfer Protocol

URI: Uniform Resource Identifier

6. Web Socket - Based communication Model:



→ web socket APIs allows bidirectional, full duplex communication between clients and servers.
→ Web socket APIs follow the exclusive pair communication models.

* IOT enabling Technologies:

IOT is enabled by several technologies. They are:
i) Wireless sensor network
ii) cloud computing
iii) Big data analytics
iv) communication Protocols.
v) Embedded system

(i) Wireless Sensor Networks (WSN) →

→ A WSN comprises of distributed devices with sensors which are used to monitor the environmental & physical conditions.
→ A WSN consists of a number of end nodes, routers and co-ordinator.
→ End nodes have several sensors attached to them. Each nodes to can also acts as routers.
→ Routers are responsible for routing the data packets from end nodes to coordinater.
→ Co-ordinator collects the data from all the nodes, it also acts as a gateway that connects WSN to the internet.

Examples of WSN's used in IOT:

→ Weather monitoring systems are WSN in which the nodes collect temperature, humidity, rainfall etc.
→ Indoor air quality monitoring system are use WSNs

to collect data on the indoor air quality and concentration of various gases.

→ Soil moisture monitoring system use WSN to monit soil moisture at various locations.

→ Surveillance system use WSN's for surveillance data (such as motion detection data).

(ii) Cloud computing :→ Basically cloud computing is a distributed computing paradigm with ability to provide on demand services that focuses on providing a wide range of users with distributed access to scalable, virtualized hardware and/or software infrastructure over the Internet.

Moreover cloud computing provides us the attracting conventional services like software as a service (Saas) where end users can avail software and or services provided by saas without purchasing and monitoring overhead, Plat-form as a service (Paas) where end users can run and deploy their applications more easily which includes operating system support and software development and last but not the list Infrastructure as a service (Iaas) which demands provisioning of infrastructural resources usually in terms of virtual machines.

(iii) Big data analytics → Big data is defined as collections of data sets whose volume, velocity and variety is so large that it difficult to store, manage, process and analyze the data using traditional databases and data processing tools.
Generally big data analytics with advanced analytics and visualization techniques play a major role for effective decision making to figure out and uncover hidden patterns and unknown correlations in large data sets.
Some examples of big data generated by IOT systems are given as follows:
→ Sensors data generated by IOT systems such as weather monitoring stations.
→ Data generated by IOT systems for location and tracking of vehicles.
→ Data generated by retail inventory monitoring systems.
→ Machine sensor data collected from sensors embedded in industrial and energy systems.

(iv) Communication Protocols →

Communication protocols allow devices to exchange data over the internet. Protocols define the data exchange formats, data encoding, addressing schemes for devices & routing packets from source to destination. Other functions of the protocols include sequence control, flow control & retransmission of lost packet.

(V) Embedded Systems → A embedded system is a computer system that has computer hardware and software embedded to perform specific task.

→ Key components of embedded system include microprocessor or microcontroller, memory (RAM, ROM, Cache), networking units (Ethernet, wifi adaptors), input/output units (display, keyboard etc.), storage system (such as flash memory).

→ Some embedded systems have specialized processors such as digital signal processors, graphics processors and application specific processors.

* IOT levels →

A IOT system comprises of the following components:

(i) Device: An IOT device allows identification, remote sensing, actuating and remote monitoring capabilities.

(ii) Resource: Resources are software components an IOT device for accessing, processing and storing sensor information or for controlling actuators connected to the device. Resource also include the software components that enable network access for the device.

(iii) Controller Service: Controller service is a native service that runs on the device & interacts with the web services. Controller service sends data from device to the web service. & receives commands from the application (via web services) for controlling the device.

(iv) Database: Database can be either local or in the cloud and stores the data, generated by an IOT device.