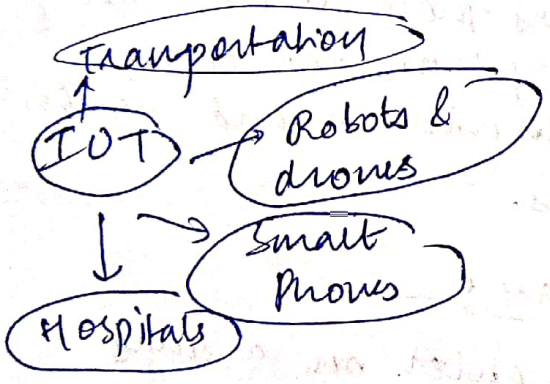
Unit I

(1) What is IOT?

- The Internet of Things (IOT) is the n/w of physical objects i.e. devices, vehicles, buildings and other items embedded with electronics, s/w, sensors, and n/w connectivity that enables object to collect & exchange data.
- The IOT refers to a wireless n/w between objects, usually the n/w will be wireless and self configuring, such as household appliances
- A phenomenon which connects a variety of things. Everything that has the ability to communicate.
- IOT is the intelligent ~~connective~~ connectivity of physical devices driving massive gains in efficiency, business growth and quality of life



- IOT refers to the capability of everyday devices to connect to other devices & people through existing Internet infrastructure. Devices connect & communicate in many ways. Ex:- Phones interact w other phones.

- IOT data differs from traditional computing. The data can be small in size & frequent in transmission.
- The smart object is building block of IOT vision. By putting intelligence into everyday objects, they are turned into smarter objects not only to collect info from environment & interact with physical world, but also to be interconnected, to each other through Internet to exchange data & info

Characteristics of IOT :-

① Interconnectivity :- Everything can be connected to global info and communication infrastructure.

② Heterogeneity :- Devices within IOT have diff hardware and use diff n/w but they can still interact with other devices through diff n/ws.

③ Things related services :- Provide things related services within the constraints of things, such as privacy and semantic consistency b/w physical & virtual thing

④ Dynamic changes :- The state of device can change dynamically

Component of IOT :-

- The Hardware utilized in IOT systems include device for a remote dashboard, devices for control, servers, a routing or bridge device and sensors. These devices manage key tasks and functions such as system activation, action specification, security communication and detection to support specific goals and actions.

Major components of IOT devices are :-

① Control units :- A small computer on a single integrated circuit containing processor core, memory and programmable I/O peripheral. It is responsible for the main operation.

② Sensor :- Devices that can ~~convert~~ measure a physical quantity and convert it into a signal which can be read & interpreted by microcontroller unit. These devices consist of energy modules, RF modules, power manag. modules and sensing modules. Most sensor fall in 2 categories :- Digital or analog

- Temperature sensor :- Accelerometers
- Image sensor :- gyroscopes
- Light sensor :- accoustic sensor
- Microflow sensor :- humidity sensor

(3) Communication Module :- These are the parts of devices & responsible for comm with rest of IoT platforms. They provide connectivity acc. to wireless or wired communication protocol they are designed. the comm b/w IOT device & Internet is performed in 2 ways :-

A) There is an Internet-enabled intermediate node acting as a gateway.

B) IOT device has direct comm with the Internet.

- Communication b/w main control unit and communication module uses serial protocol in most cases.

(4) Power Sources :- In small devices, current is usually produced by sources like battery, thermocouple, solar cells. Mobile devices are mostly powered by light weight batteries that can be recharged for a longer life duration.

(5) Communication Technology & Protocol :- IOT primarily exploits standard protocol and n/w technologies. However, the major enabling technologies and protocols of IOT are RFID, NFC, low energy Bluetooth, low energy radio protocols, LTE-A & wifi Direct. These tech support the specific n/wing functionality needed in an IOT system in contrast to standard uniform n/w of common system.

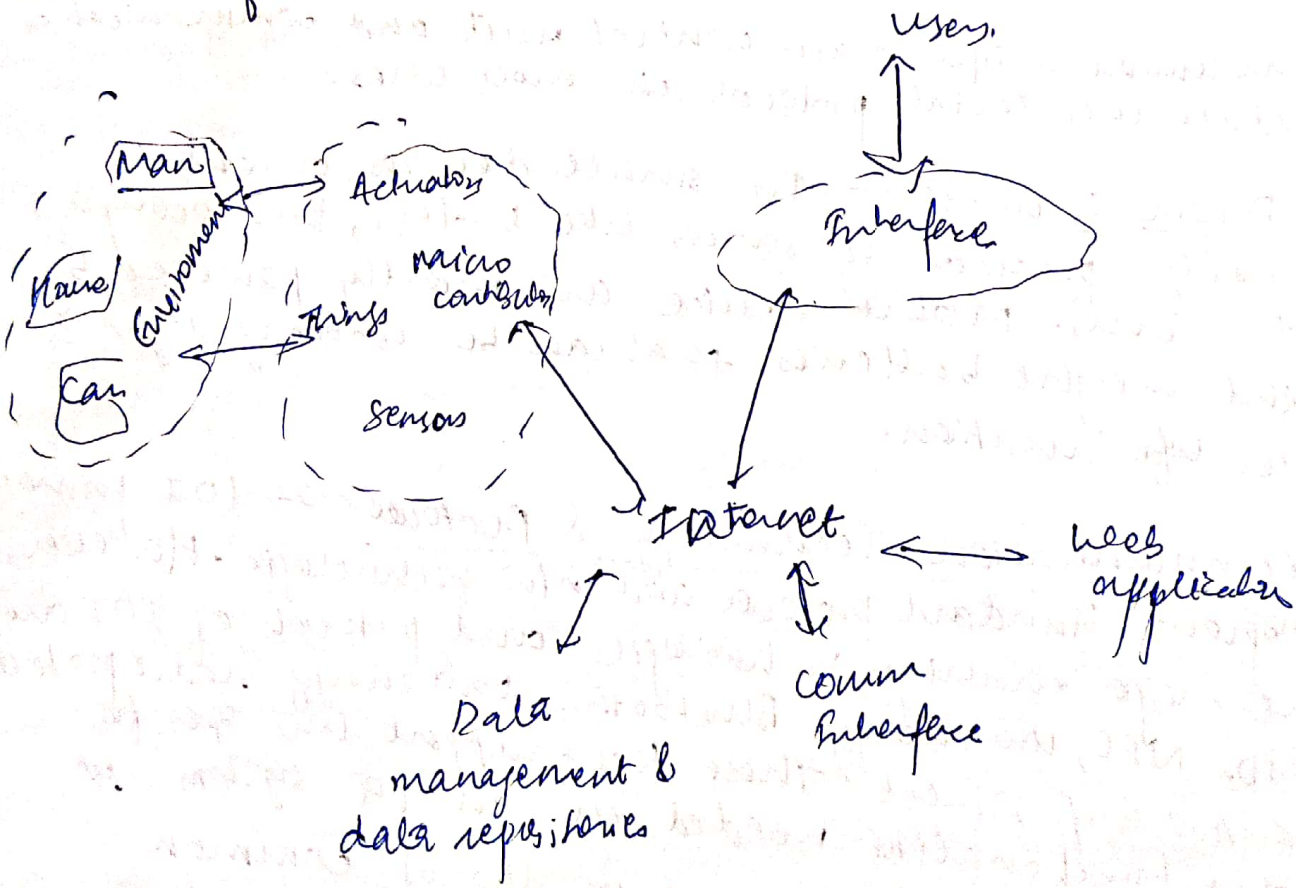
Working

① Collect and Transmit Data :- The device can sense the environment & collect info related to it & transmit it to a diff device or the Internet.

② Actuate Device Based On Triggers :- It can be programmed to actuate other devices based on conditions set by user.

③ Receive Info :- Device can also receive info from n/w

④ Communication Assistance :- It provides communication b/w 2 devices of same n/w or diff n/w



Adv. of IOT :-

- Improved customer engagement & Communication
- Support for technology optimization.
- Support wide Range of data collection
- Reduced Waste

Disadvantages of IOT:

- Loss of privacy and security:— As all household appliances, industrial machinery, etc are connected to Internet, a lot of info is available on it. The info is prone to attack by hackers.
- Flexibility:— many are concerned about the flexibility of an IOT system to integrate easily with others.
- Complexity:— The IOT is a diverse and complex h/w. Any failure or bugs in s/w or h/w could cause serious consequences. Even power failure can cause lot of inconvenience.
- Compatibility:— Currently, there are no international standard of compatibility for the tagging & monitoring equipment.
- Same time & memory [High cost].

Application of IOT:—

(1) Homes:— Building where people live. It controls home and security systems.

(2) Offices:— Energy management & security in office buildings, improved productivity, including for mobile employees.

(3) Factories:— Place with repetitive work routines including hospitals & farms; operating efficiencies, optimizing equipment & inventory.

(4) Vehicles:— Vehicle including car, truck, ship, trains; condition based maintenance, usage-based design, pre-sales analytics.

(5) Cities:— Public spaces & infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring.

(6) Worksites:— It's a custom production env. like mining oil and gas, construction, operating theatres maintenance, health & safety.

Motivation for IOT

The increased no of users (corporation, companies, SMEs) who use IOT can be explained by many benifits it offer such as:—

i) improving the ~~effcie~~ customer experience
ii) efficiency
3) access to data/collection of new data
4) reduction of labor cost/actual cost.
5) connectivity
6) saving time
7) new positioning at business level

History of IOT:—

- It was only in 1999 that the term "internet of things" was coined by Kelvin Ashton. Ashton used the phrase as the title of his ppt for a new sensor project he was working on & it stuck from there.
- While the phrase came about in 1999, the concept of connected devices date backs to 1832. when the first electromagnetic telegraph was designed, allowing direct comm. b/w 2 machines through the transfer of electrical signals.
- However the true IOT history began with the invention of Internet in late 1960s.

~~first~~

- The first IOT device was invented by Carnegie Melon University in early 1980s. A group of students from uni created a way to get their campus coca cola vending machine to report on its content through a n/w inorder to save them the trek if machine was out of coke. They installed micro-switches into machines to report on how many coke cans were available & if they were cold.
- In 1990, John Romkey connected a toaster to ~~IOT to~~ internet for the first time. A yr later group of students at Uni of Cambridge used a webcam to report on coffee They came up with the idea of to use the 1st web cam prototype to monitor the amount of coffee available in their computer labs coffee pot. They did this by programming the web cam to take photos 3 times/min of coffee pot. The photos were then sent to local computer so everyone could see if there was coffee available

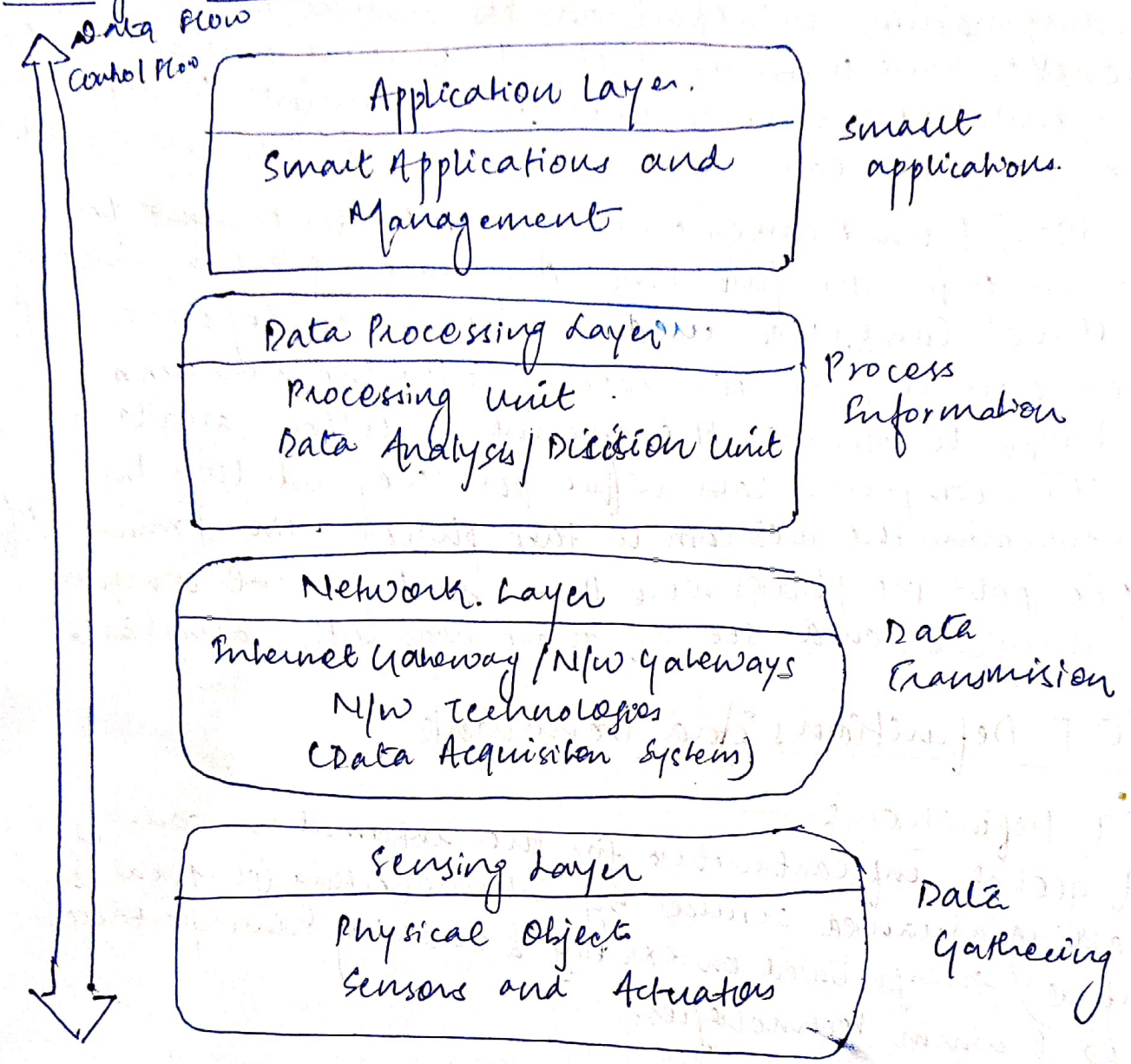
IOT Definitions And Framework

IOT Definitions:-

- A global infrastructure for the information society, enabling advanced services by interconnecting (physical & virtual) things based on existing & evolving interportable info & comm technologies.
- IoT :- It describes physical object that are embedded with sensors, processing ability, s/w & other tech. that connect and exchange data with either device and system over the Internet or other comm n/w.

Architecture of IOT :—

4-stage IOT architecture :—



There are 4 layers :—

1) Sensing Layer :— Sensors, actuators, devices are present in this sensing layer. These sensors or Actuators accepts data (physical environmental parameters), processes data and emits data over n/w.

2) N/w Layer :—
Internet / Network gateways, Data Acquisition System (DAS) are present in this layer. DAS performs data aggregation & conversion function.
- Collecting data & aggregating data after

converting analog data of sensors to digital data etc. Advanced gateways which mainly opens up connection b/w sensors n/w and Internet also performs many basic gateway functionalities like malware protection, & filtering also sometimes decision making based on inputted data & data management service.

3) Data Processing Layers —
This is the processing unit of IOT ecosystem. Here data is analyzed & pre processed before sending it to data center from where data is accessed by s/w applications often termed as business applications where data is monitored & managed & further actions are also prepared. So here edge IT or edge analytics comes into picture.

4) Application Layer: — This is the last layer of arch. Data center or cloud is management stage of data where data is managed & is used by end user application like agriculture, health, etc.

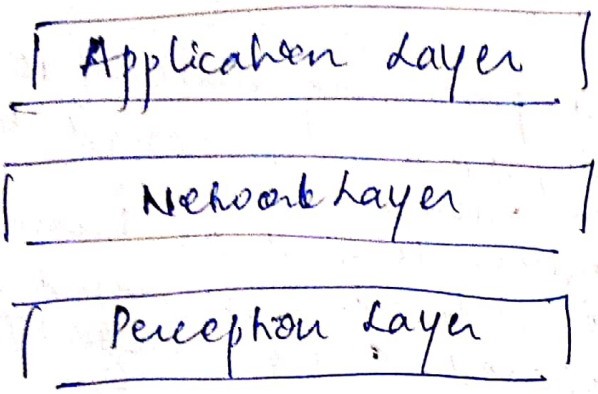
Below are 3 layers: —

1) Perception Layer : —
It is the physical layer, which has sensors for sensing and gathering info about the environment. It senses some physical parameters or identifies other smart object in environment.

2) The N/w Layers: —
It is responsible for connecting to other smart things, n/w devices and servers. Its features are also used for transmitting & processing sensor data.

3) The Application Layer :—

It is responsible for delivering application specific service to the user. It defines various applications in which IOT can be deployed.
Ex. – Smart Homes, smart cities, etc



The 3-layer arch is not sufficient for research on IOT because research often focus on finer aspects of IOT. That is why there are many more layer arch. One is 5-layer arch, which additionally includes processing & business layer.

5 layers are :– Perception, Transport, Processing, Application & Business layer.

Role of perception and application layer is same as architecture with 3 layer.

The remaining 3 layer :–

i) Transport layer ~~transports~~

It transfers the sensor data from perception layer to the processing layer & vice versa through n/w such as wireless, 3G, LAN, Bluetooth, RFID & NFC.

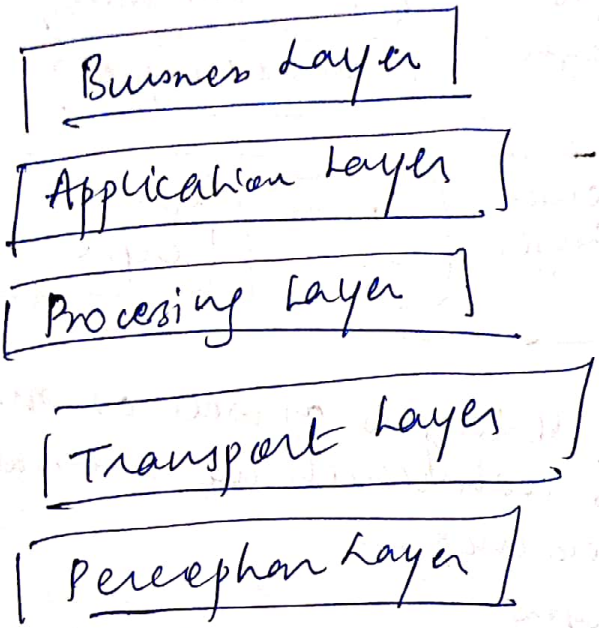
ii) Processing layer :→

It is also kfa middleware layer.

It stores, analyses and processes huge amount of data that comes from transport layer. It can manage & provide a diverse set of services to the lower layer. It employs many tech. such as database, cloud computing and big data processing module.

iii) The Business Layers —

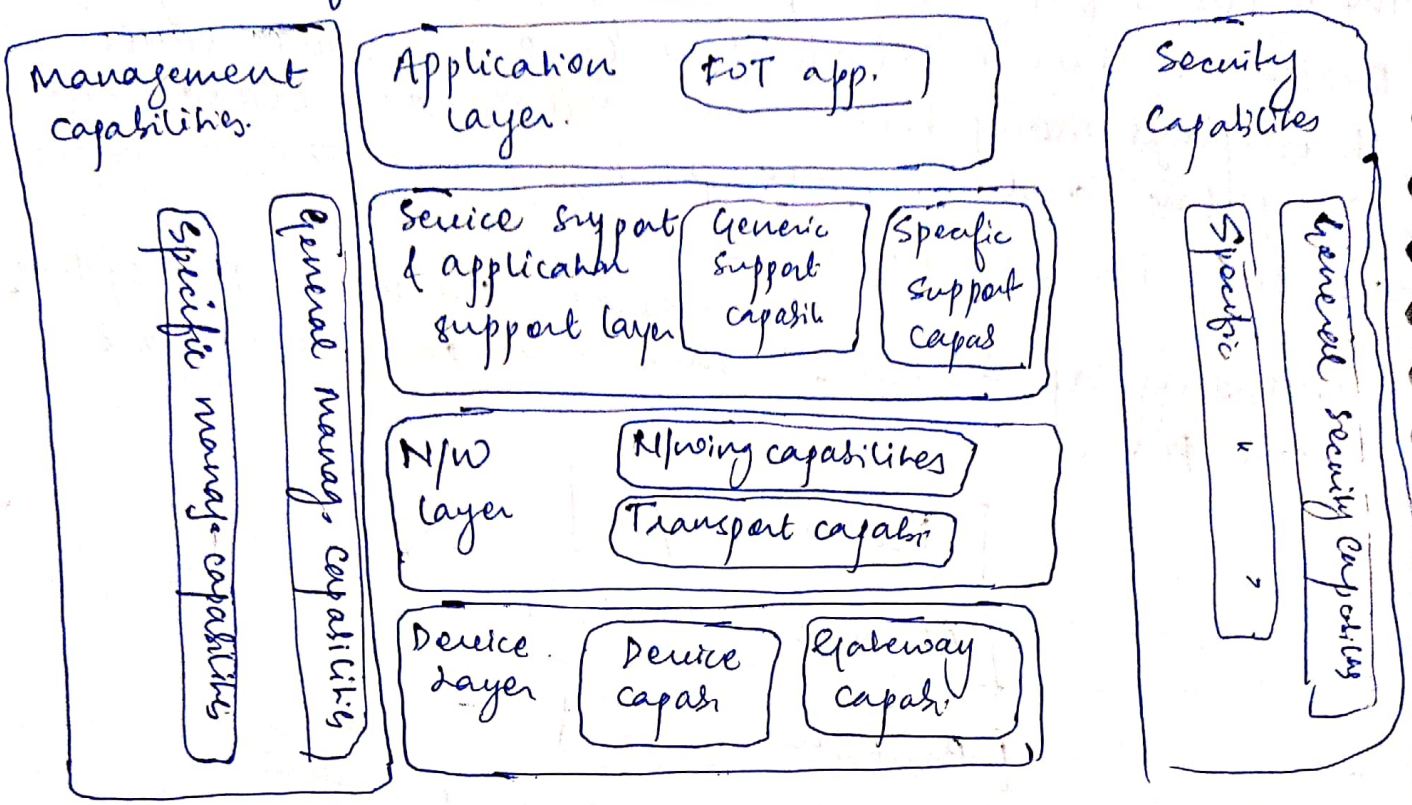
It manages the whole IOT system, including application, business and profit models & user's privacy



ITU-T View [International Telecommunication Union - Telecomm. sector view]

- The Telecommunication sector of International union [ITU-T] has been active on IOT standardization since 2005 with the Joint coordination Activity on N/w aspects of Identification System (JCA-NID), which was renamed to Joint Coordination Activity on IoT in 2011.
- The ITU-T IoT domain model includes a set of physical devices that connect directly or through gateway devices to a communication n/w that allows them to exchange info with other devices, services & applications.

ITU-T Reference model



- It is composed of 4 layers as well as management & security capabilities which are associated with 4 layers. The 4 layers are —
  - → Application layer
  - → Service support & Application support layer
  - → N/W layer
  - → Device layer
- Application layer :- It contains IOT applications
- Service and App. support Layer :- It consists of common capabilities which can be used by diff IoT applications & realizes detailed capability groupings, inorder to provide diff support functions to diff IoT applications
- N/W layer :- Provides relevant control functions of n/w connectivity and IOT services & applications transportation

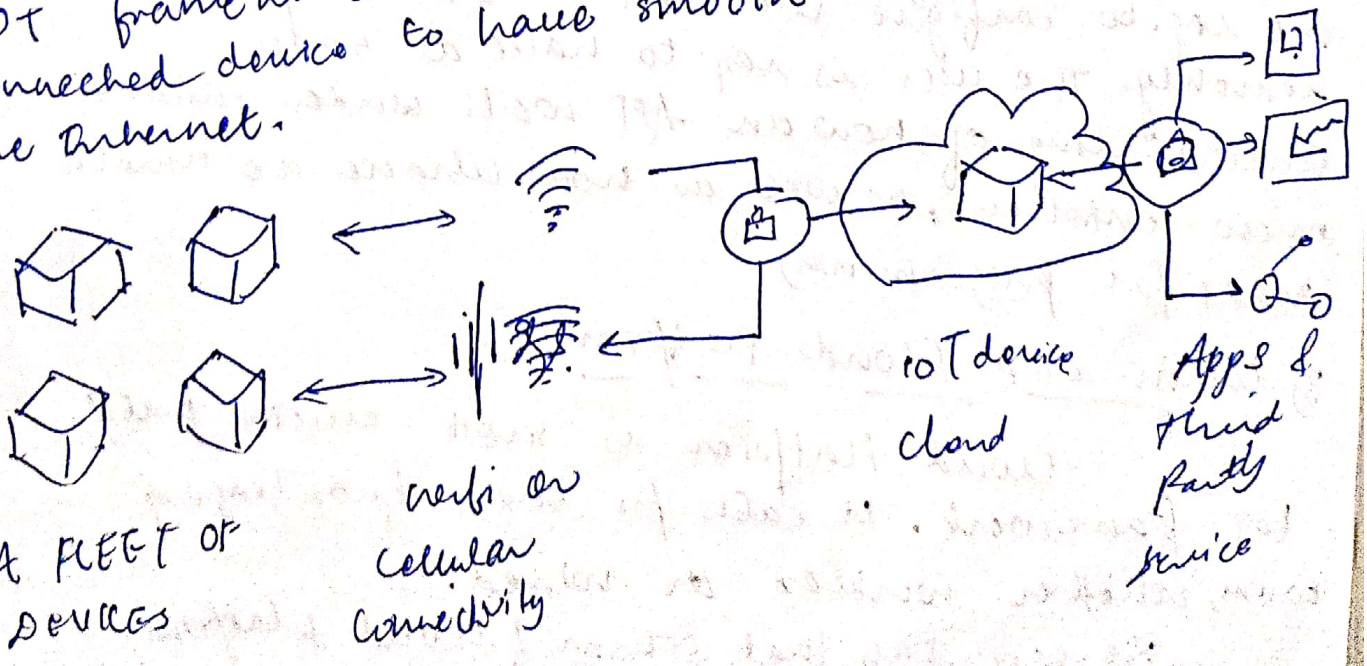
- Device Layer:— Includes direct / indirect device interaction with gateway and comm. n/w.
- Management Capabilities:— How to manage device, traffic, etc.
- Security Capabilities:— Includes authorization, authentication, application, data confidentiality & integrity protection, etc.

Advantages:—

- It provides language for everyone involved.
- ——— abstract but also rich view of domain.
- It can assist IoT project leaders in planning the work at hand & teams needed.

IoT framework:—

- The IoT framework can be described as being an ecosystem, comprising of several connected devices that communicate with each other, over the Internet. These connected devices usually work to transfer and sense data over the Internet, while requiring very little human intervention
- IoT framework is what makes it possible for the connected device to have smooth communication over the Internet.



IoT framework is very imp element of technology in modern world, finding applicaton in almost every sector. For ex:- one of major applicaton of IoT is in designing of smart homes.

- IoT framework concept is also applied in designing of diff physical obj, such as thermostats, electrical devices, security, etc.

Main Components of IoT frameworks —

IoT framework is comprised of 4 major comp:-

1) Device Hardware: —

The device H/w component of IoT framework req. some basic knowledge on architecture. The user is also req. to have an idea on working of diff micro-controllers, as well the sensors

Ex of hardware devices that form part of this IoT framework comp. are sensors, micro-controller & controller

2) Device Software: —

In order for device s/w of IoT framework to function properly, the included working applicatons are req. to configure the controller, then operate them remotely. The user is req. to have a basic understanding of how an APP works ~~under~~ inside the micro-controllers, as well as how libraries are usually made for programming

3) Comm. and Cloud platform: —

Cloud Platform is most crucial part of IoT framework. It calls for basic knowledge of comm, whether wireless or wired.

We can say that comm & cloud platform is where all communicaton happens.

4) Cloud Application:— It is a typ of S/W program, which mainly consist of components that can be accessed quite easier & faster. These comp. can be either local or even-cloud based. The cloud application works to improve the systems, such as that its max potential is realized.
In other words, cloud application can be defined as another application of IoT framework, that binds all local I/O devices as well as cloud-based devices.

Unit II :—

Structural Aspects of the IoT :—

Some key structural related desiderata are highlighted here, those issues ultimately may determine the extent & rapidity of deployment of IoT services & technologies. This list isn't exhaustive.

Environment Characteristics :—

such as but not limited to the foll: —

→ Low power [with the requirement that they will run potentially for yrs on batteries].

→ Low cost [total device cost on single digit dollars]

→ Significantly more devices than in a typ env.

→ Severely limited code & RAM space

Traffic Characteristics :—

The char of IoT comm is diff from other types of n/w or applications. For Ex:— cellular mobile n/w are designed for human comm. & comm. is connection centric; it entails interactive comm. b/w humans involving humans [file download, etc]. [video call, etc].

It follows that cellular n/w are optimized for traffic char of human based app. and comm.

There are 3 kinds of traffic generated :- event driven, query driven and period traffic.

Scalability :—

While some app (eg. smart grid, home automation, etc) may start out covering a small geographical area or small community of users, there invariably will be a desire

over time to expand, in order to make such services more cost-effective on per-unit basis, or to have sufficient critical mass for developers to be motivated to invest resources to add capabilities to service.

When contemplating expansion, one wants to be able to build on previously deployed tech w/o having to scrap the system & start from scratch. Also efficiency of large system should be better than efficiency of smaller system. This is what is meant by scalability

~~Interoperd~~

Interoperability :→

Because of plethora of app., technology suppliers and stakeholders, it is desirable to develop &/or re-use a core of common standards. To the degree possible, existing standards may prove advantageous to rapid & cost-effective deployment of tech. Product & service interoperability is of interest.

Security and Privacy :→

Unfortunately, security is chronically an after-thought when it comes to protocol development. almost invariably a protocol spec will have many pages of data format & operation procedures & only a short paragraph or two on security conditions when IoT relates to power distribution, goods dist, transport & traffic management, etc it is critical to maintain system wide confidentiality, identity integrity & trustworthiness.

Open Architectures —

The goal is to support a wide range of application using a common infrastructure, preferably based on service oriented architecture (SOA) over an open service platform, & utilizing overly n/w [these being logical n/w defined on top of physical infrastructure]. In an SOA environment, object expose their functionalities using a protocol such as SOAP or REST API. These devices may provide their functionality as a set that can in turn be used by other entities.

Key Technologies :—

There are a lot of new ~~things~~ technologies in the IOT, the key tech. of which is radio frequency identification technology (RFID), sensor technology, n/w comm. technology & cloud computing.

i) Working Principle & System composition of RFID :—

RFID is the abbreviation of radio frequency identification, also called electronic tags - RFID tech is an automation identification tech., it uses radio frequency signal through space coupling to realize the non contact info transmission, and achieve the purpose of identification through the info transmitted.

Its Principle — After the label enters the magnetic field, if it can receive the reader sending out the special frequency signal, the product info stored in the chip can be transmitted by energy of induced current.

The RFID should atleast include the foll parts, one is the reader, the other is electronic tag, in addition, antenna, host, etc. Acc to diff app purposes and app enu., RFID will be diff. But from work principle of RFID, the system is composed of signal transmitter, signal receiver & ~~signal~~ transmitter receiver.

Key Tech :-

ZigBee Technology :-

1) Wireless Sensor N/W's :-

A WSN comprises distributed ~~services~~ devices with sensors which are used to monitor the environmental & physical conditions. A wireless sensor n/w consist of end nodes, routers & coordinators. End nodes have several sensor attached to them where the data is passed to a coordinator with the help of routers. The coordinator acts as gateway that connects WSN to internet.

Ex:-
- Wealth monitoring systems
- Indoor air quality
- Soil moisture
- Health.

3) Cloud computing :-

It provides us mean by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations. With cloud computing, users can access any resources from anywhere like databases, web server and any S/W over internet.

Chara:-
- Broad n/w access
- On demand self-services
- Measured Service
- Rapid scalability
- Pay-per-use

Provides diff services, such as:—

- IaaS (Infrastructure as a service) :- provides online service such as physical machine, virtual machine, servers, networking, storage & data center space on pay per use basis. Major IaaS providers are google compute engine, Amazon web services etc. Ex:- Web Hosting.
- PaaS (Platform as service) :- provides cloud based env. with a very thing req to support the complete life cycle of building & delivering web based (cloud) applic- without the cost & complexity of buying & managing underlying hardware, s/w provisioning & hosting. Basically, it provides platform to develop app.

  Ex:- App cloud, Google app engine.
- SaaS (Software as service) :- It's a way of delivering applications over the Internet a service. Instead of installing & maintaining s/w, you simply access it via the internet, freeing yourself from complex s/w & h/w management.

  Ex:- Google Docs, Gmail, etc.

3) Big Data Analytics:-

It refers to method of studying massive volumes of data or big data. collection of data whose volume, velocity or variety is simply too massive or tough to store, control, process & examine the data using traditional DB.

Big data is gathered from a variety of sources including social n/w videos, digital images sensor & sales transaction records.

Steps involved in analyzing big data:—

- Data cleaning
- Munging
- Processing
- Visualization

Ex:- Bank transactions, E-commerce & ex Big-Basket, Health & fitness generated by IOT system such as fitness bands.

5) communication Protocols:-

They are backbone of IOT systems & enable n/w connectivity & linking to applications. communication protocols allow devices to exchange data over n/w. Multiple protocols often describes diff aspects of a single communication.

A group of protocols designed to work together is k/a protocol suite; when implemented in s/w they are protocol stack.

They are used in:-
Data encoding
Addressing schemes.

6) Embedded systems:-

It is a combination of H/w & S/w used to perform special tasks. It includs microcontroller & microprocessor memory, n/w units (Ethernet web Adapters), input output units (display key board etc) & storage devices (flash memory).

It collects data & send it to internet.

Embedded system used in:
ex → digital cameras
→ DVD player, music player
→ Industrial Robots
→ Wireless Router, etc.

Sensor Technology :—

Tech that uses sensors to acquire info by detecting the physical, chemical or biological properties & convert them into readable signals.

Sensors :— are used for sensing things & devices etc. A device that provides a usable o/p in response to a specified measurement. The sensor attains a physical para. here and converts it into a suitable signal for processing the characteristics of any device or material to detect the presence of a particular physical quantity. The o/p of sensor is a signal which is converted to human readable form like change in char., change in resistance, etc.

Sensor's Char:—

① Static ② Dynamic

① **Static characteristics** :—

It's about how the o/p of a sensor changes in response to an input change after steady state condition.

→ **Accuracy** :— capability of measuring instruments to give a result close to the true value of measured quantity

→ **Range** :— gives highest & lowest val of physical quantity within which sensor can actually sense.

→ **Resolution** :— higher the resolution, better the precision. Provides smaller changes in input that sensor is able to sense.

→ **Precision** :— capability of measuring instrument to give same reading when repeatedly measuring same quantity under same ~~prev~~ prescribed condition

→ Sensitivity:- Indicates the ratio of incremental change in response of the system and incremental change in input parameter.

→ Linearity:- Deviation of sensor value curve from particular straight line, it's determined by calibration curve.

→ Drift:- The diff in measurement of sensor from a specific reading when kept at that val for longer time.

→ Repeatability:- deviation b/w measurements in sequence under same conditions.

3) Dynamic Chars

Prop. of systems:-

- Zero order Systems:-

The O/p shows response to input signal with no delay. It doesn't include energy-storing element.
Ex:- Linear & Rotatory displacements.

- First order Systems:-

when the output approaches its final value gradually.
consist of energy storage & dissipation elements.

- Second order Systems:-

complex output response. The output response of sensor oscillates before steady state.

Sensor Classifications —

• Passive & Active • Analog & digital • Scalar & Vector

→ Passive Sensors: — Cannot independently sense the input. Ex:- Accelerometer

→ Active :- Independently sense the input. Ex:- Radar

→ Analog:- The response or output of sensor is some continuous function of its input parameter. Ex:- LDR

→ Digital :- Response in binary nature. Designed to overcome disadv. of analog sensors. Ex:- Passive Infrared.

→ Scalar:- Detects the input parameter only based on its magnitude. Ex:- Temprature, color & smoke sensor

→ Vector:- The response of sensor depends on magnitude of direction and orientation of input parameter. Ex:- Magnetic field.

RFID Technology :—

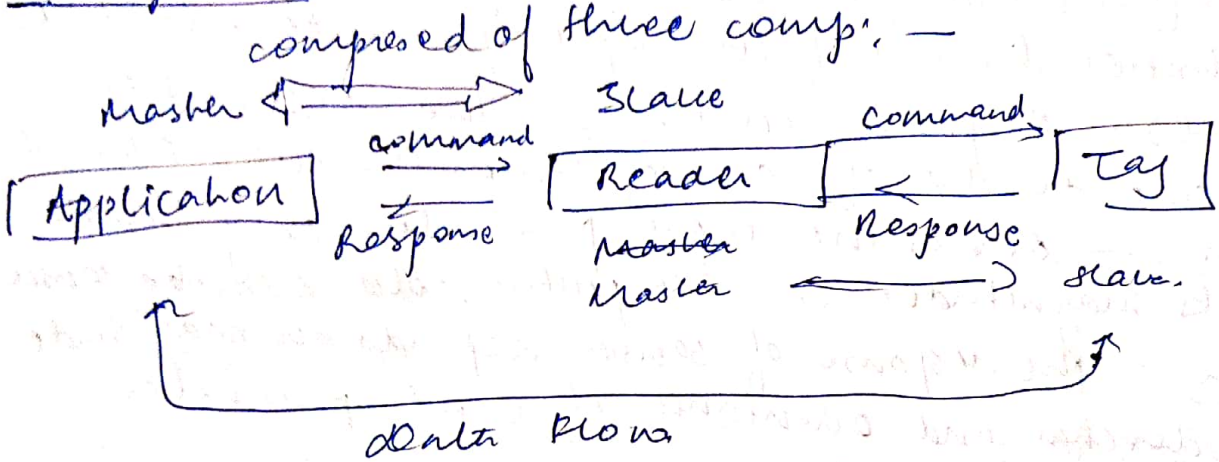
Radio frequency identification system is an automatic technology & aids machines or computers to identify objects, record metadata or control individual target through radio waves.

A typically RFID system is consisted of tags (transmitter/responder) and readers (transmitter/receiver).

Tag is a microchip connected with antenna, which can be attached to an object as the identifier of the object. The RFID reader communicates with RFID tag using radio waves.

When the RFID readers abided by appropriate comm protocols are connected to terminal of Internet, the reader throughout the world can identify, track and monitor the objects attached with tags globally, automatically & in real time if needed. This is so called IOT.

RFID Systems: —



RFID tags: — also k/a transponders are attached to object to counter identify. Tags could be either active or passive. Active tags are those who have capability to communicate with other tags, and can initiate a dialog of their own with the tag reader. Passive tags, do not need any internal power source but are powered up by a tag reader.

Tag mainly consist of coiled antenna & a microchip with main purpose of storing data.

Reader: —

Also k/a transceiver (transmitter/receiver) made up of a radio frequency interference (RFI) module & control unit. Its main function are to activate the tags, structure the common sequence with the tag & transfer data b/w app. s/w & tags.

- Application system:- also called processing system which can be an application or database, depending on DB. The app s/w initiates all reader & tag activities

Applications of RFID tech:—

The function of RFD system generally includes 3 aspects:- monitoring, tracking & supervising.

- Monitoring generally means to be aware of state of a system by repeated observing the particular conditions, especially to detect them and give warning of change.
- Tracking is observing persons or objects on move & supplying a timely ordered sequence of respective ~~data~~ location data to model.
- Supervising:- monitoring of behaviour, activies or other changing info.

→ the most interesting & successful app. includes these for supply chain management, production process control and objects tracking management.

→ RFID has been gradually used in folle fields:—

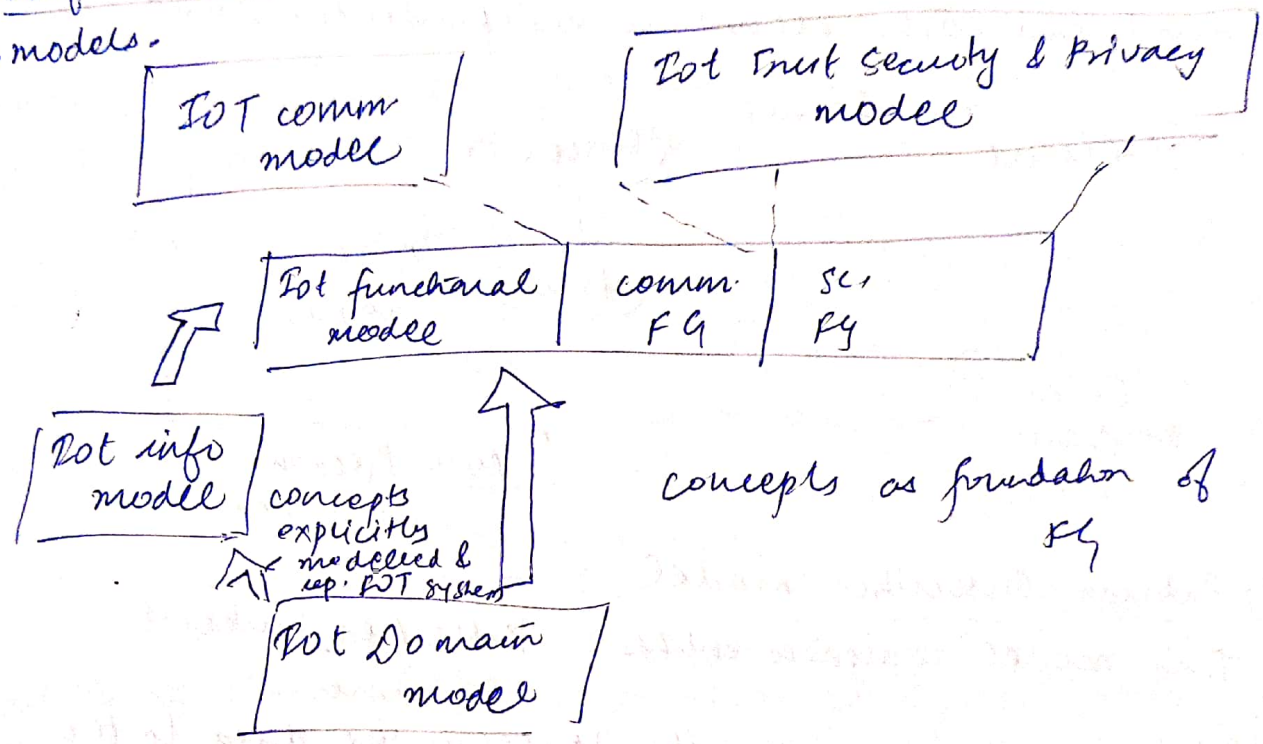
- Logistics & supply
- Manufacturing
- Agriculture management
- Military & Defense
- Health Care & medicine
- Payment Transaction
- Transportation & Retailing

Challenges: of RFID:—

- Collision Problem
- Security & Privacy Concerns

One M2M :- It is a broadband label that can be used to describe any tech that enables the n/w devices to exchange info and perform action w/o the manual assistance of humans. The main purpose of M2 techs is tap into sensor data & transmit it to an/cs

ii) IoT Reference model :- describes the domain using no of sub models.



Q Explain all app layer, transport layer, n/w layer & link layer protocol for IoT

Link Layer Protocols

i) Bluetooth :- It is a PAN or it is a short range wireless comm. ~~It is used for specific commercial & industrial app.~~ n/w for exchanging data b/w connected sensor.

ii) ZigBee :- It is low power personal comm n/w. It is used for specific commercial & industrial app.

iii) BLE (Bluetooth low Energy) :- Its range is similar to that of bluetooth but it consumes low power than Bluetooth

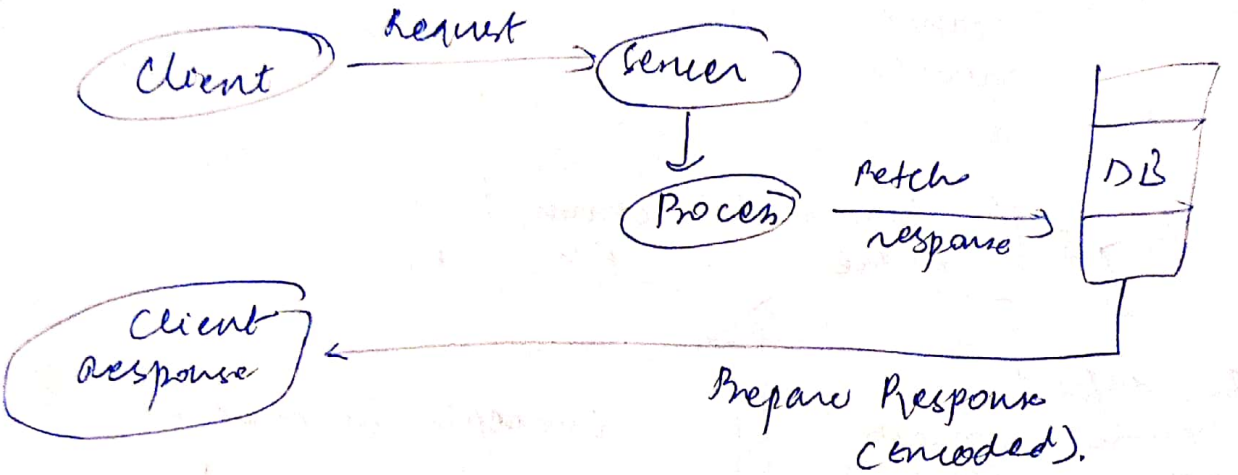
iv) Wi-Fi :- Wireless Fidelity It is a LAN there is no wired connection. It provides Internet access with Mid range

Q. Explain foll. comm model for IOT

i) Request-Request Model
ii) Publish/Subsc model
iii) Push/Pull model
iv) Exclusive pair mode

i) Request-Request Model

It follows client-server arch. This model is stateless since the data b/w the requests isn't retained and each request is independently handled

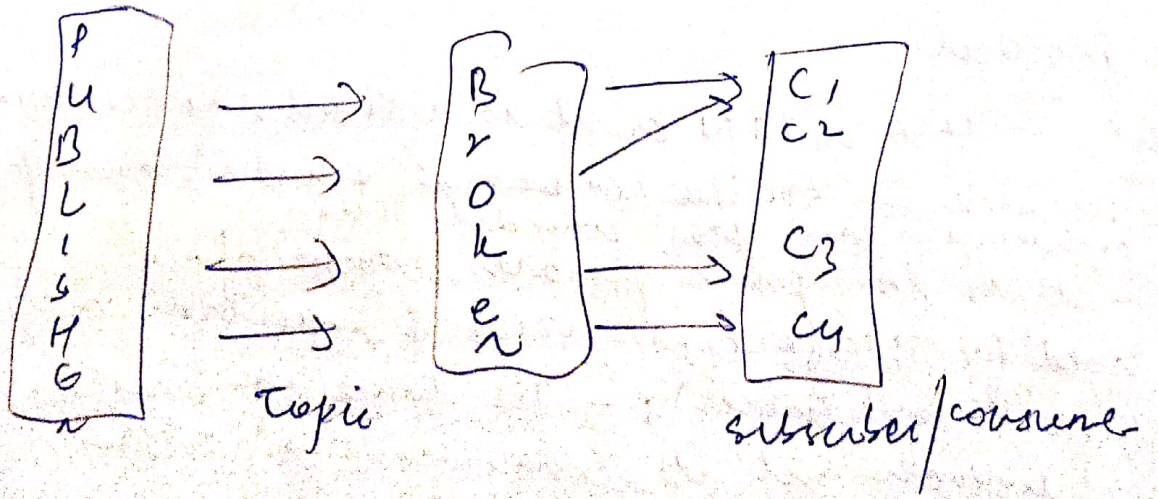


ii) Publish-Subscriber model →

This model comprises entities :- Publisher, broker & consumer

→ Publisher are source of data. It sends the data to the topic which are managed by broker.

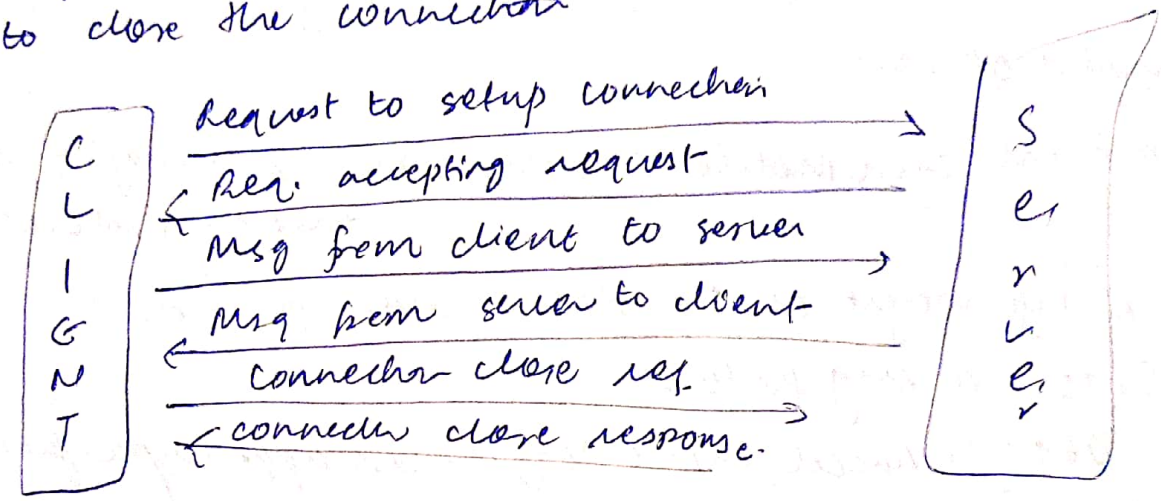
→ Consumer subscribe to the topics which are managed by broker



3) Push-Pull model:— consist data publishers, data consumers, and data queues.

→ Publishers publish their msg/data & push it into queue. Consumer on other side, pull data out of queue. Thus, queue act as a buffer for the msg when diff occurs in rate of push/pull of data on side of publisher & consumer.

4) Exclusive pair:— It is the bidirectional model, including full duplex comm. among clients & servers. The connection is constant & remains open till the client sends a request to close the connection



Q. Rest Based comm API:— It is a set of architectural principles by which you can design web services & web apis that focus on a system's resource & how resource's states are addressed & transferred. It follows request-response comm model.

Web Socket API:— allows bidirectional, full duplex comm b/w clients and servers. It follow exclusive pair comm model. This comm API doesn't require new connection to be set b/w clients & servers. Once the connection is setup the msg can be sent & received continuously w/o any interruptions. WebSocket APIs are suitable for IOT applications with low latency or high throughput req.

9) Explain Platform middleware for IOT i) Standards of M2M. ii) Framework for WSN

Middleware is s/w that serves as an interface b/w components of IOT, making comm. possible among elements that would not otherwise be capable.

middleware makes it easy for s/w developers to implement comm and input/output so that they can shift their focus to the specific purpose of their applications.

1) Standards of M2M

- OMA DM (Open Mobile Alliance Device manag) :- device manag protocol.
- OMA lightweight M2 :- device man protocol
- MQTT :- a msg protocol
- TR-069 (Technical Report 069) :- an app. layer protocol
- Hypercat :- data discovery protocol
- One M2M :- a comm protocol

2) Framework WSN :-

- A service model to describe services from both n/w
- A comm. infrastructure that enables their interoperability of WSN's & Internets services
- A advanced gateway which is responsible for providing the location & access transparency for services's comm.
- A service composition tool which enables the creation of logical regions in the WSN by just composing web services that are available on Internet.