Notes on Internet of Thing

by

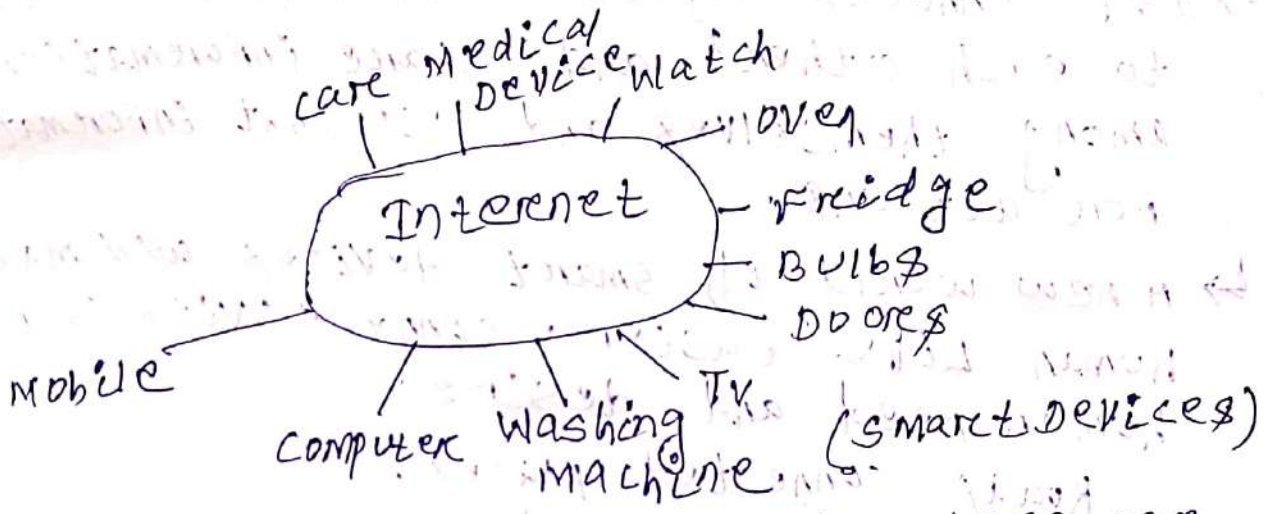
Satya Narayan Panigrahi

Lecturer in Electronics and Telecommunication Engineering

UGMIT, Rayagada

Interenet of Things (IOT)

- Things are objects like mobile, computers, washing machine, TV, watch, oven, fridge, bulbs, doors... appliances and devices that we use in our daily life.
- Things/objects accessible (or) connected through the Interenet, Then it is called Interenet of Things.



* Home Automation * Driverless car.

- IOT is a Term that refers to the connection of objects to each other and to Humans through the Interenet.
- IOT is a simple concept of basically controlling different devices by establishing a connection and communicating from Mobile Application (or) Web browser.
- Taking everyday Things, embadding them with electronics, software, sensors and then connecting them to Interenet & enabling them to collect and exchange data without human intervention is called as the IOT.

Goal of IOT :-

- To extend Internet connectivity from standared devices such as computers, mobile phone and electronic devices.
- IOT makes everything smart.
- The term I.O.T was invented by Kevin Ashton in 1999 while he was working with proctere & Gamble.
- IOT connects objects and make them 'Talk' to each other and share information among themselves and use that information for actions.
- A new world of smart devices will make human Life easiere. connectivity is a human need and desire.

  Roads connected places.
  Telephones connected people.
  Internet connected people and communities.
  IOT make entire world (every object) deeply and widely connected.
- IOT make every object — Addressable, Accessible, Actionable

ADVANTAGES OF IOT :-

① Minimize Human efforts :- As Devices interact and communicate with each other and do Lot of Task for us. It reduces the Human effort.

(2) Saves Time :- The IOT reduces the human efforts and hence it saves our Time instead of repeating the same tasks everyday, it enables people to do other creative jobs.

(3) Saves Money / Efficient resources utilization :-

If we know the Functionality and the way that how each device work we can increase the optimum utilization of energy and resources. Hence we can save money by using IOT Technology.

(4) Improving Quality of Life :-

As IOT Technology increased comfort, convenience and better management, Hence it improves the quality of Life.

(5) Better Monitoring of devices :-

The IOT allows us to automate & control the tasks that are done on a daily basis & reducing Human intervention. We can monitore the devices connected to IOT and take necessary action in case of emergencies.

(6) Ability To access information From anywhere at any time on any device.

DISADVANTAGES OF IOT :-

(1) Lack of security on privacy :- IOT devices First share data over the Internet, where the risk of Losing privacy increases because of hackers.

(2) complexity :- Designing, developing and maintaining IOT is complicated. Any error in the software or Hardware will have serious consequences.

power Failures (or) no Internet can cause a lot of inconvenience.

(3) Increasing unemployment :-

As daily activities getting automated, there will be fewer requirements of Human resources, especially workers and Less educated staff. So, IOT will create unemployment issue in society.

(4) Technology Takes control of Life :-

With IOT we are Losing control of our Life. We are dependent on Technology. We always want to do small tasks by doing minimum efforts. IOT devices makes this possible but it makes us dependent on Technology.

(5) compatibility :- Since There is no international standard of compatibility For IOT, it is difficult For devices From different manufactures to communicate with each other.

APPLICATIONS OF IOT :

① Smart Home :- With the use of IOT, the user can access the Home appliances like Lighting, Heating, security and entertainment remotely. IOT provides security, comfort and convenience to owners of House.

↳ Smart TVs that are connected to Internet allows us to browse various applications.

Refrigerators with LCD screen - It gives information of what's inside, food that's about to expire, ingredients you need to buy and also provide this information on your smartphone app.

↳ cameras and Home alarm systems - It provide safety to our own home.

↳ Detection of window and Door openings - It prevent intruders (Thieves) to enter in to home.

↳ Energy and Water supply consumption - It helps to save money.

② Wearables :- Virtual glasses, smart watches are the examples of IOT wearable tools.

↳ IOT wearables can display calls, text messages, social media updates and track fitness and health.

↳ IOT wearables are small and energy efficient devices, which are equipped with sensors, with the necessary hardware for measurements and readings and with software to collect and organize data and information about users.

③ Connected Health :- The use of wearables (or) sensors connected to patients, allows doctors to monitor a patient's condition outside the hospital and in real time.

↳ Integration of IOT Technology in to hospital beds, can collect and transfer health data like blood pressure, oxygen and blood sugar levels, weights and ECGs. This data is stored in the cloud and can be accessed by doctors when required.

④ Smart Retail :- This IOT application saves time of shoppers with the help of IOT apps, customers do not need to ~~stan~~ stand in long queues as the checkout system can easily read the tags from the products and deduct the total amount from the customer's mobile payment app.

⑤ Smart Farming :- As quality of soil is crucial to produce good crops. So IOT offers farmers the possibility to access detailed knowledge and valuable information of their soil condition.

↳ Information such as soil moisture, level of acidity, the presence of certain nutrients, temperature etc. helps farmers to control irrigation, make efficient use of water, specify the best times to start sowing and also discovers the presence of diseases in plants & soil.

So with the help of IOT, farmers will be able to reduce waste and increase productivity.

⑥ Industrial Automation:-

↳ IOT technology can automate manufacturing process remotely.

↳ With the help of IOT, we can manage the inventory and supply chain.

↳ We can diagnose if the machine require repaire and maintenance.

↳ We can monitor the emission of toxic gases to avoid damage to worker's health and the environment.

↳ This is possible by installing sensors inside equipment to monitore and send reports.

⑦ connected car:-

↳ car connected with IOT system will report to the user the condition of the car such as the fuel efficiency, advanced navigation, maintenance etc. It generate an alert of heavy traffic and other security alerts.

⑧ Smart Grid:-

↳ Smart Grid is used to monitore and manage everything remotely such as Lighting, traffic Lights, traffic jams, parking lights, road warnings etc.

↳ It also detects influx energy resulting from earthquakes and extreme situations weather. It can effectively avoid (or) reduce the damage of ~~natural~~ natural disaster and reduce the economic loss.

(9) Smart cities :-

↳ A smart city is a technically advanced region with advance information and communication Technologies.

The IOT can be used

(i) To monitor the vibrations of building bridges and monuments in case the building material is threatened (or) overloaded.

(ii) Manage traffic especially during traffic jams, peak hours, accidents and racing.

(iii) Manage street Lights - automatically switch them off in the presence of sunlight and switch them on at the onset of darkness.

(iv) Alerting the officials to empty the trash bins (dustbins) when filled with waste.

(v) Smart parking notifies uses for open spaces and when the parking time is expired.

CHARACTERISTICS OF IOT :-

(1) Connectivity :- In IOT, anything, anywhere, anytime should be connected to the infrastructure without connection nothing makes sense.

(2) Intelligence :- Extraction of knowledge from the generated data is important. sensor generate data and this data should be interpreted properly.

(3) Scalability :- The no. of devices that need to be managed and that communicate with each other will much largere than the devices connected to the current Internet. Hence, an IOT setup shall be able to handle the massive expansion (handling the growing things and the increase in data)

(4) Heterogeneity :- Devices in IOT are based on different hardware platforms and networks and can interact with other devices or service platforms through different networks. IOT architecture should support direct network connectivity between heterogeneous networks.

(5) Unique Identity :- Each IOT device has an I.P. address. This is helpful in tracking the equipment and at times to query its status.

(6) Dynamic & Self Adapting :- The IOT device must dynamically adopt itself to the changing context (temperature, Location, speed)

Example :- A camera meant for surevelliance may have to work in different conditions and at different Light sitvations (Morning, afternoon & night)

(7) Safety :- IOT devices are vulnerable to security threats. As our personal data is shared with the help of Internet, it can be tempered. If proper safety measures are not taken. So, the personal data of the

users needs to be secured from any data theft and security of expensive IOT things.

user needs to be secured from any data theft and security of expensive IOT things.

IOT conceptual Framework and Architectural Frame work :-

↳ Following Equation describes a simple conceptual Framework of IOT:

Physical object (Thing) + (controller, sensor, Actuators) + Internet = IOT

Actuator → supporting device which helps other devices to operate.
It is a device that makes something move (or) operate.

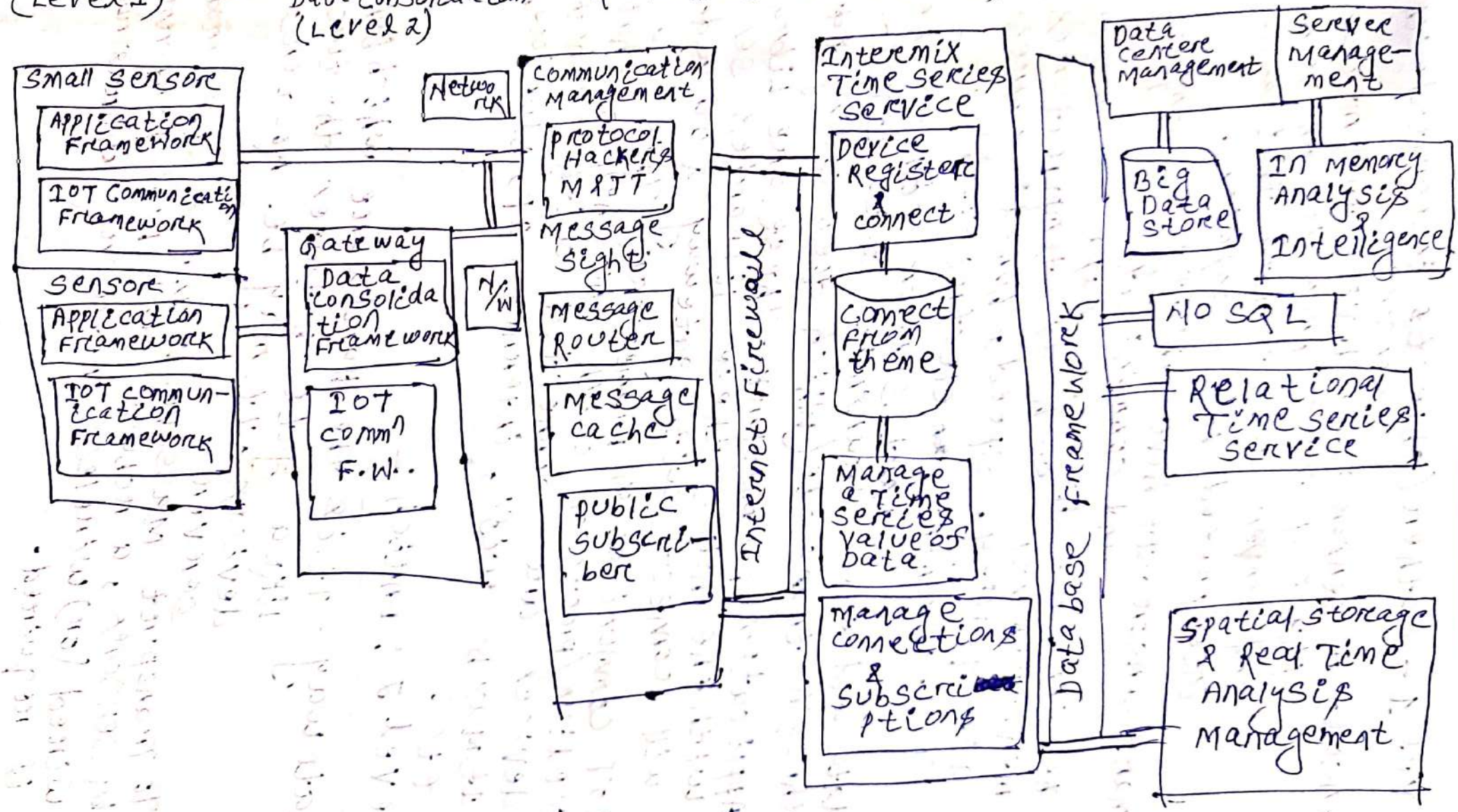
↳ IOT conceptual Framework for enterprise processes (IOT Architecture by oracle)

Gather + Enrich + stream + manage + Acquire + organize & Analyse = IOT

↳ complex IOT conceptual framework for cloud platform based processes & services.

Gather + Consolidate + connect + collect + Assemble + manage & Analyse = IOT

IBM IOT Conceptual Framework



Level 1 - Gather (objects integrated with sensors)

Sensor - A sensor is a device that measures physical input from its environment and convert it into data that can be interpreted by a computer.

↳ Smart sensor - It have ability to compute and communicate.

The sensors have the capacity to take measurements such as temperatures, air quality, speed, humidity, pressure, flow, movement, electricity etc.

Smart sensor collect the data and then transmit it to Level-2 through transcode (which does coding & decoding)

↳ Application Framework - These are Libraries, with the help of these libraries sensor will connect with gateway & other devices.

↳ IoT Communication Framework - This is a medium/protocol with the help of that devices are connected with eachother. It may be wifi, internet, IP, Bluetooth etc.

Level 2 : Enrich :-

Gateway - It is the Hardware which behave like a gate between the two devices. It may be Router, server.

To Transport massive volume of data produced by sensors, a robust and high performance wired (or) wireless network infrastructure is required.

Data from sensors come to Gateway after the encoding and when data go to the next Level from gateway decoding is done.

Level 3 : Stream :-

communication management is done here to send and receive the data streams.

protocol handlers - These are used to check whether the device connected in IOT has ability to access the Internet (or) not.

Message Router - If any device send the message then the router will decide to whom it will go.

Message cache - It stores the recently comes data.

Level 4 : Manage :-

Level 4 receive the device data. Here Device Management, Device Identity management and access Management receives devices data. The device/hardware which we are using should be registered. The registered device can only access the data.

Example:- Let two Mobile phones are connected to each other & if first mobile phone wants to communicate with second mobile phone, so the first mobile phone is registered & the data of this mobile is on Level-4 like data of device registers, device identity etc.

Level 5 : Acquire :- A Data store (or) database acquires data at Level-5.

Level 6: organize and Analyse:-

Data routed from previous Levels are organised and analysed at Level 6. Data is analysed for collecting business intelligence. Data is analysed & to check whether the data is authenticated sensitive (or) non sensitive.

IOT ARCHITECTURE:-

There are four Layers in IOT Architecture (or) IOT is based on 4 building blocks also called IOT architecture Layers.

Layer 1: sensing Layer:-

Application Layer
(Smart Application & management)

Data processing Layer
processing unit
(Data Analytics/Decision unit)

Network Layer
Internet & Network gateways
(Data Acquisition unit)

sensing Layer
(physical objects-sensors and actuators)

↳ sensing Layer is made up of physical objects integrated with sensors (smart devices/objects) & actuators. These sensors (or) actuators accept data from the atmosphere (or) place like

Temperature sensor senses Temperature from the room, process data and emit/share it through IOT gateway.

Layer 2 (Network Layer):-

↳ In this Layer, Internet/ Network gateways, Data Acquisition system (DAS) are present.

↳ DAS performs data aggregation (collection) and conversion function (analog data of sensors to digital data etc)

↳ Gateways acts as a carrier between the internal network of sensor nodes with the internet. Gateways also performs many functionalities like malware protection, filtering, data management services etc.

Layer 3 (Data processing Layer):-

↳ The data transmitted through the gateway is stored and processed securely with the cloud server (data center) from where data is accessed by software applications (termed as business applications).

↳ The processed data is used to perform intelligent actions that make all our devices smart Devices.

Layer 4 (Application Layer):-

↳ End user application (or) mobile apps will help end users to control & monitor this devices from remote locations.

↳ These apps takes important information from the cloud & display it on your smartphones, tablets etc. The main tasks here are

visualization & management of important information.

With the help of these applications, user sends commands to sensors to perform some actions like changing default temperature of air conditioner etc.

COMPONENTS OF IOT ECOSYSTEMS :-

Things (or) Devices $\xrightarrow[\text{Data}]{\text{Wireless Network}}$ Gateway $\xrightarrow[\text{Data}]{}$ Cloud $\xrightarrow[\text{Data}]{}$ Analytics $\xrightarrow[\text{Data}]{}$ User Interface

↳ IOT connect multiple devices at a time to the Internet thereby facilitating man to machine & machine to machine interactions.

↳ IOT ecosystem is not limited to a particular field, but has applications in home automation, vehicle automation, factory line automation, health care etc.

There are 4 fundamental components of IOT System which tells us how IOT works. These components are: ① sensors/devices ② Gateways ③ Data processing (cloud and Analytics) ④ user Interface

① sensors/devices :-

sensor is a Hardware device that takes the input from environment & gives to the system by converting it.

Sense Temperature → [Thermometer] $\xrightarrow[\text{signals}]{\text{Electrical}}$ [system]

Actuator – It is a device that converts the electrical signals into the physical events (or) characteristics.

– It takes the input from the system & gives output to the environment.

Environment ← Actuator ← system
(Heat/motion)

Example:- Motors, Heaters etc.

Smart Devices/sensors:-

↳ Devices & sensors are the components of the device connectivity Layer.

↳ Smart sensors are continuously collecting data from the environment and transmit the information to the next Layer (Gateway).

↳ Most Modern smart devices & sensors can be connected to Low power wireless networks like Wi-fi, Zigbee, Bluetooth etc.

Gateway:-

↳ It can be configured to perform preprocessing of the collected data from thousands of sensors locally before transmitting it to the next Layer (cloud Layer). It filters unnecessary data.

↳ It acts as a Middle Layer between devices and cloud to protect the system from malicious attacks and unauthorized access.

Cloud and Analytics :-

- IOT cloud offers tools to collect, process, manage and store huge amount of data created by devices, applications & users.
- Distributed database management systems are the most important components of IOT cloud.
- Analytics is the process of converting analog data from billion of smart devices and sensors in to useful insights which can be interpreted and used for detailed analysis.
- Big enterprises use the massive data collected from IOT device & utilize for their future business opportunities.

User Interface :-

- User Interface should be well designed, so that users can perform minimum efforts to operate the IOT devices through it.
- Like multicolore touch panels have replaced hand switches in our household appliances.

PHYSICAL DESIGN OF IOT :-

↳ It refers to IOT devices, IOT protocols.

IOT devices :-

↳ Things in IOT are IOT devices.

↳ They have unique identities.

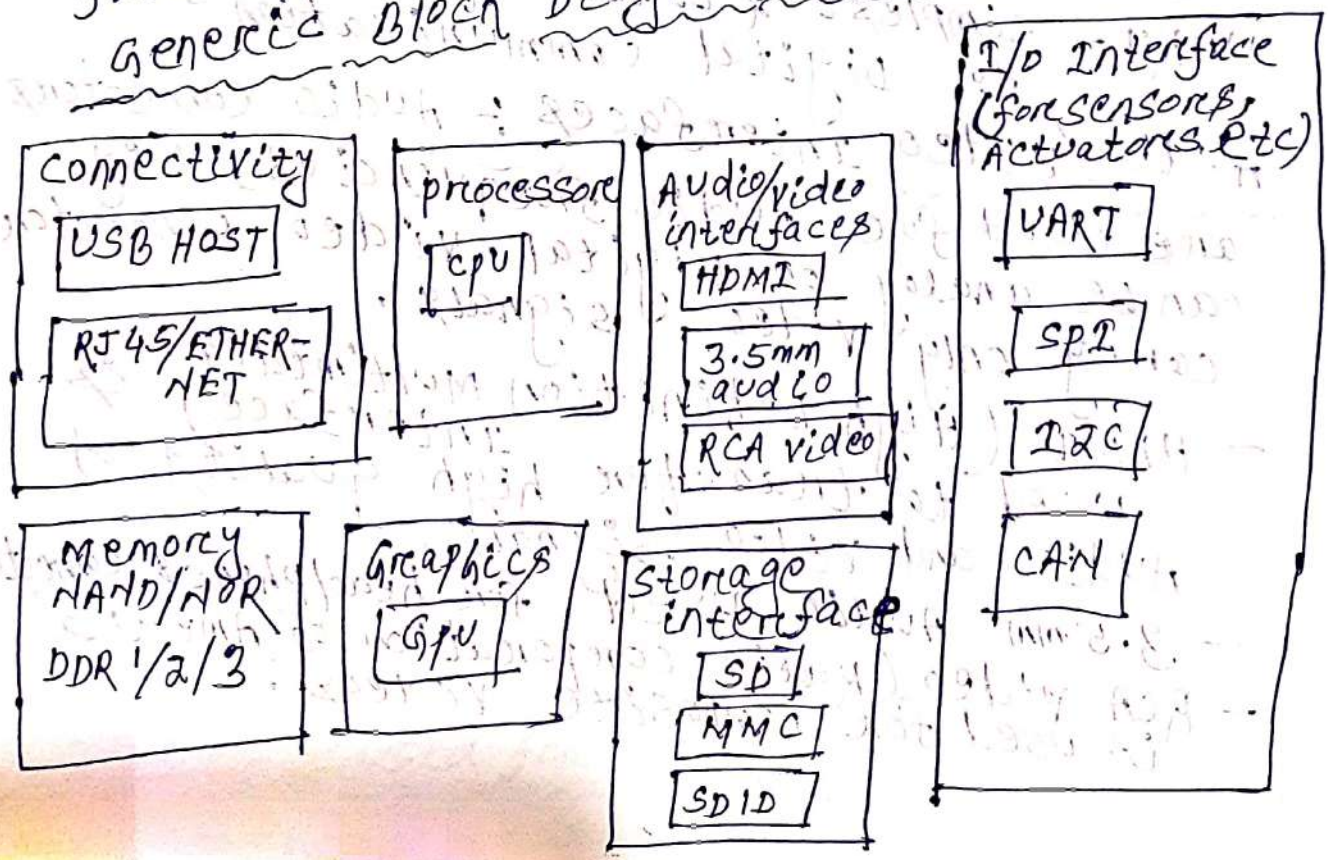
↳ They perform remote sensing, actuating and monitoring.

↳ Types of IOT devices :- sensing devices, smart watches, smart Electronic appliances, Wearable sensors, Automobiles, Industrial machines etc.

↳ Data generated by IOT devices processed by data analytics systems leads to useful information to guide further actions locally (or) remotely.

↳ IOT devices can exchange data with other connected devices and applications directly or indirectly, or collect data from other devices.

Generic Block Diagram of IOT Devices



↳ IOT Devices may consists of several interface for connection with other devices both wired & wireless like:-

(i) I/O interface for sensor & actuators.
(ii) Interface for internet connectivity.
(iii) Memory (or) storage interface.
(iv) Audio & video interface.
(v) process & graphic interface.

I/O interfaces (for sensors, actuators etc):-

- sensors and actuators will be connected to IOT devices through this interface.

Different types of I/O interfaces used in IOT devices:-

(i) UART (Universal Asynchronous Receiver & Transmitter)
(ii) SPI (serial peripheral Interface)
(iii) I2C (Inter Integrated circuit)
(iv) CAN (controller Area network)

UART - simplest & oldest form of digital to digital communication

Audio/video Interfaces :- Audio connectors are used for Audio frequencies, They can be analog or digital. video connector carry only video signals.

- HDMI (High Definition Multimedia Interface) is used to transfer high quality of Audio and video signals.
- 3.5 mm Audio used for headphones connection
- RCA video (Radio corporation of America) is used for composite videos.

Storage Interface

SD - Secure Digital (Memory card used to store data of smart phones, music players, camera etc)

MMC - Multimedia Card (Memory card)

SDIO - Secure Digital Input output (used for Input output devices)

Graphics - Images displayed on computer screen like Bar charts, pie charts, flow charts etc.

GPU - Graphics processing unit

Memory - It is used to store information

volatile memory (Temporary) & cache

Nonvolatile memory (permanent) - static [ROM, HDD]

NAND - NOT AND
NOR - NOT OR
] Logical Gates found in memory cards, smartphones, and USB devices.

DDR - Double Data Rate generation 1, 2, 3 - memory can send & receive data signal in double rate (Twice per clock cycle)

Connectivity :-

The network of connected "smart devices" that communicate over the Internet.

- It contains USB Host - Universal Serial Bus → system used to connect multiple USB clients.

RJ45/Ethernet - Registered Jack cable used for Ethernet Network.

PHYSICAL DESIGN OF IOT :-

IOT protocols

- IOT protocols help to establish communication between I/O devices and cloud based server over the Internet.
- It also helps to send commands to IOT device & receive data from an IOT device over the Internet.

IOT protocols used at Different Layers :-

Application Layer

HTTP COAP Websockets
MQTT XMPP DDS AMQP

Transport Layer

TCP UDP

Network Layer

IPV4 IPV6 6LOW PAN

Link Layer

802.3 - Ethernet 802.16 - WiMax 2G/3G/4G
802.11 - Wifi 802.15.4 - LR - WPAN

Application Layer protocols :-

HTTP (Hypertext Transfer protocol)

- It is a protocol for transmitting hypermedia documents such as HTML.
- It is a method for encoding and transporting information between a Web browser and a Web server.

- HTTP follows a classical client server model.
- HTTP is a stateless protocol.
- Server does not keep any data (state) between two requests.
- Generally use TCP connections to communicate with servers.

COAP (constrained Application protocol)

- It enables devices to communicate over the Internet.
- It is used for constrained devices such as 8-bits micro controller, Low power sensors that can't run on HTTP.
- It is used for machine to machine communication.
- It is a simplification of HTTP protocol running on UDP instead of TCP, that helps save bandwidth.
- It is designed for use
  (i) Between devices on the same constrained network like Low-power, Lossy networks,
  (ii) Between devices and general nodes on the Internet,
  (iii) Between devices on different constrained networks both join by an internet.
- It is also being used via other mechanisms such as SMS on mobile communication Network.

Websocket - It is a Low level web friendly communication mechanism (FB, messenger, Mozilla).

- It is a full duplex communication over a single socket connection for sending messages between client & server.
- client can be a browser, IOT device (or) a mobile application.

MQTT (Message Queuing Telemetry Transport):-

- M2M / IOT connectivity protocol.
- It is a publish subscribe based messaging protocol used in IOT.
- It runs over TCP/IP.
- MQTT broker is a server & clients are the connected devices.
publisher-server, client-subscribers (or) customers

XMPP (Extensible Messaging & presence protocol):-

→ It is a communication protocol for message oriented middleware based on XML.
- It is suitable for voice/video calls, chats, messaging, gaming, multiparty chat, IOT applications such as smart grid and serial networking services etc.

DDS (Data Distribution Service)

- IOT protocol developed for M2M communication by object management group communications.
- It enables data exchange via publish-subscribe methodology.
- It integrates the components of a system together providing low latency data connectivity.

extreme reliability and a scalable architecture that business & mission critical IOT applications need.

AMQP (Advanced message queuing protocol) :-

- It is an open standard application Layer protocol for message oriented middleware.
- Messages are pushed by the brokers (or) pulled by the consumers.
- used for business messaging.
- Three Additings Bindings — states the connection between MQ & Exchange

Exchange → Message queues

Receives messages from publishers & routes them to message queues.

queues stores messages until completely processed by client software.

Transport Layer protocols :-

- Transport Layer provide functions such as error control, segmentation, flow control & congestion control.
- so, Transport Layer protocol provide end to end message transfer capability independent of the underlying network.

Transmission control protocol (TCP) :-

- It is a connection oriented protocol (ex:- FTP {File Transfer protocol}, SMPT {Simple Mail Transfer protocol})
- It defines how to establish and maintain a network conversation through which application programs can exchange data.

- TCP works with the IP (Internet protocol) which defines how computer send packets of data to each other.
- It helps in exchange of messages between computing devices in a network.

User Datagram protocol (UDP) :-

- It is a connectionless protocol (example: DNS {Domain name server}, online multi-player games)
- It is unreliable and connectionless protocol. So there is need to establish connection prior to data transfer.
- Suitable for multicasting as UDP supports packet switching.

Network Layer protocols :-

- This Layer is responsible for sending of IP datagrams from the source network to the destination network.
- This Layer performs the host addressing and packet routing.
- IPV4 & IPV6 are used for Host identification. There are hierarchical IP addressing schemes.

IPV4	IPV6
- It defines an IP address as a 32-bit number. (2^{32} addresses)	- It defines an IP address as a 128-bit (2^{128} addresses)

- It is a numeric address, separated by a dot.	- It is an alphanumeric address, separated by a colon (:)
Ex: 12.244.133.165	3001:1ab6:0000:00001

6LOWPAN :- (IPV6 over Low power wireless personal Area Network)

- This protocol allows smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
- 6LOWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network like WiFi.

Link Layer protocols :-

- Link Layer protocols determine how data is physically sent over the networks physical Layer (or) medium Link Layer protocols are :-

802.3 Ethernet :-

- Ethernet is a set of Technologies & protocols that are used primarily in LANs.
- It was first standardized in 1980 by IEEE 802.3 standard.
- Ethernet is classified in to 2 categories:

classic Ethernet	switched Ethernet
- original form of Ethernet.	- used switches to connect to the stations in the LAN.
- Data Rate between 3 To 10 Mbps.	

802.11 - Wifi :-

- It defines an interface between 2 wireless clients.
- IEEE 802.11 standard is used to provide secure end to end communication for WLANs.
- Wifi computer communication in various frequencies including 2.4 GHz, 5GHz, 6GHz & 60 GHz frequency bands.

80.2.16 WiMax :-

- The standard for WiMax technology is a standard for wireless Metetropolitan Area Networks (WMANs) that has been developed by working group number 16 of IEEE 802, specializing in point to multipoint broadband wireless access.
- WiMax can provide at home (or) mobile Internet access across whole cities (or) countries.

802-15.4 - LR - WPAN - (Low Rate Wireless personal Area Networks)

EX:- Zigbee

- LR WPAN focuses on low cost, low speed communication between devices.
- WPANs is the importance of achieving extremely low manufacturing operation costs and technological simplicity without sacrificing flexibility.

2G/3G/4G - Mobile communication

- These are different types of telecommunication generations.
- IOT devices are based on these standards can communicate over the cellular networks.

	2G	3G	4G
Speed of	up to 250 Kbps	200 Kbps to 3 Mbps	up to 100 Mbps for mobile access

2G/3G/4G - Mobile communication

- These are different types of telecommunication generations.
- IOT devices are based on these standards can communicate over the cellular networks.

	2G	3G	4G
Speed of	up to 250Kbps	200Kbps to 3Mbps	up to 100Mbps for mobile access

Logical Design of IOT :-

↳ Logical Design of IOT system refers to an abstract representation of the entities (devices) and processes without going into the low level specifics of implementations.

↳ Terms used for understanding of logical design are

1. IOT functional blocks.
2. IOT communication modules.
3. IOT communication APIs.

IOT Functional Blocks :-

- IOT system consists of many functional blocks that provide the system:
  - (i) capability for identification
  - (ii) sensing
  - (iii) Actuation
  - (iv) communication
  - (v) Management

Functional Blocks :-

① Device :- IOT system devices provides sensing, actuation, monitoring & control function.

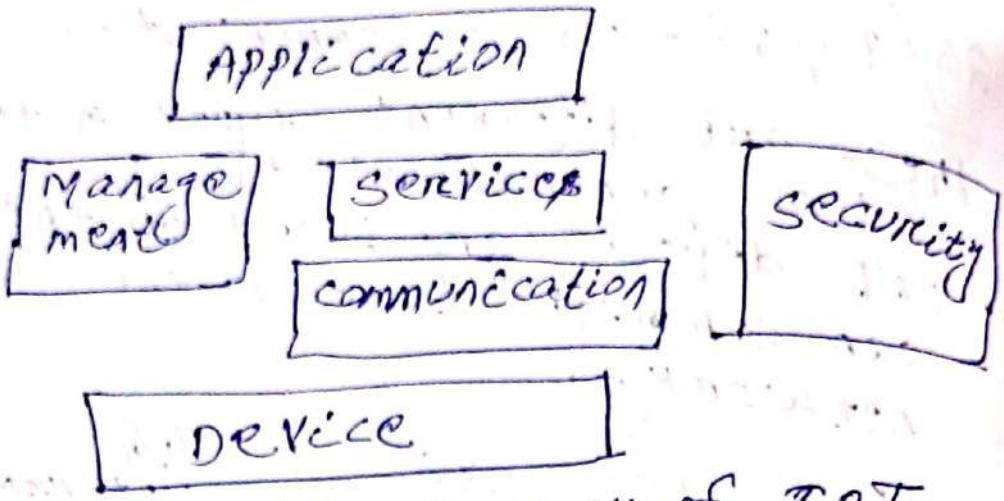


Fig: Functional block of IOT

Communication :- Handles communication for IOT system.

Services :- provides services for device monitoring, device control services, data publishing services & services for device discovery.

Management - It provides various functions to govern the IOT system.

Security - This block secures the IOT system, by providing functions such as authentical, authorization, message & content integrity & data security.

Application :-

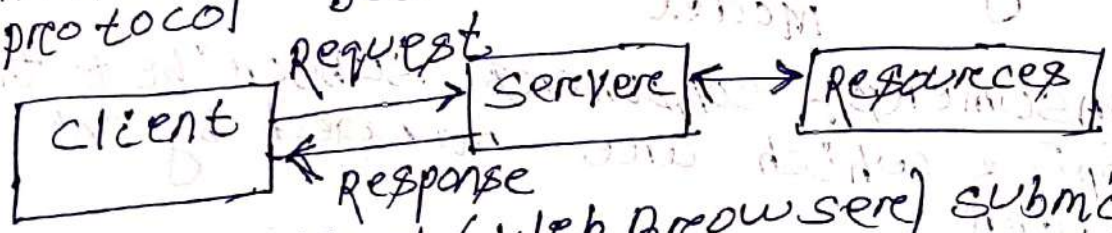
- This is an interface that the users can use to control & monitor various aspects of the IOT system.
- It also allow users to view the system status & view (or) analyze the processed data.

IOT communication models

1. Request Response model.
2. publish subscribe model.
3. push pull model.
4. Exclusive pair model.

1. Request Response model :-

- It is a communication model in which the client sends requests to the server & the server responds to the requests.
- The request may be for Transfer of data or upload of data.
- The server may be remote (or) local & can handle requests of multiple clients.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representation, prepares the response & then sends the response to the client.
- ~~Req~~ It is a stateless communication model & each request-response pair is independent of others.
- HTTP works as a request response protocol between a client & server.



Example :- A client (Web Browser) submits an HTTP request to the server, then the server returns a response to the client.

- The response contains status information about the request & may also contain the requested content.

② Publish subscribe model :-

- publish subscribe is a communication model that involves publishers, brokers & consumers.

Publisher :- publishers are the source of data. They send the data to the topics which are managed by the broker.

- publishers are not aware of the consumers.

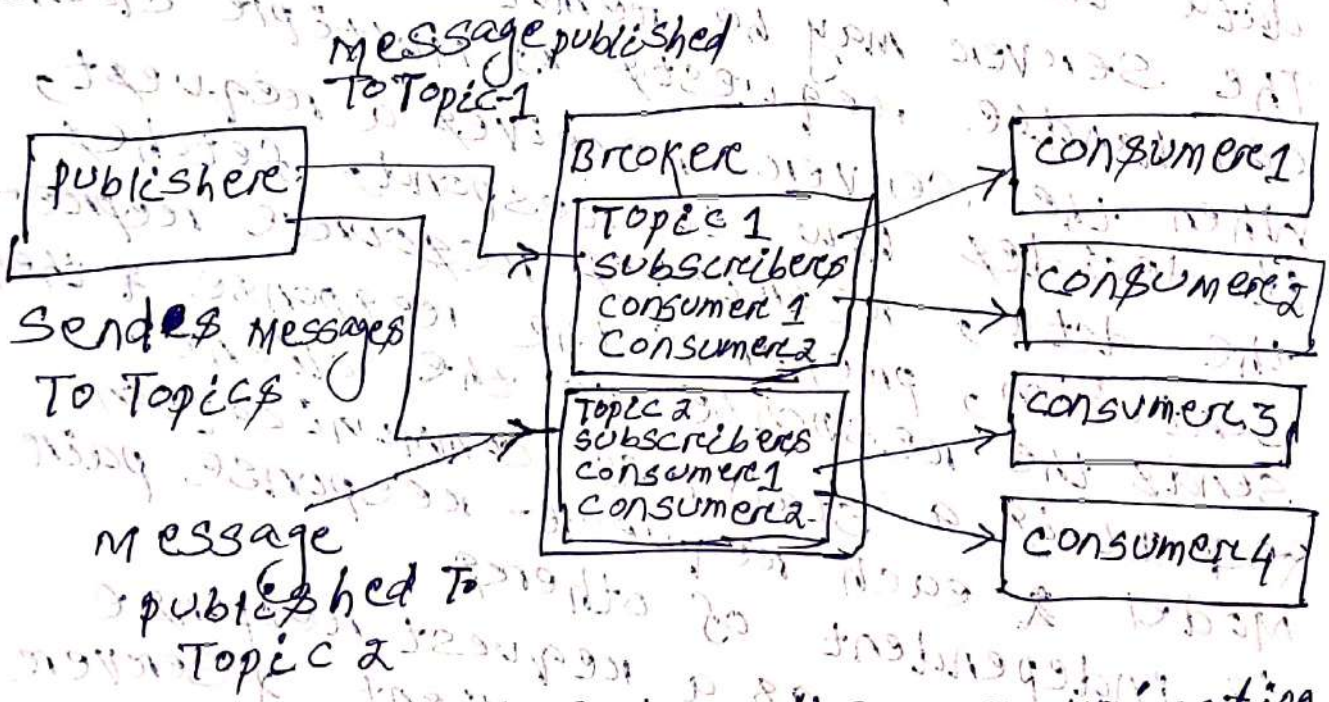


Fig: publish subscribe communication model

Consumers :- consumers subscribe to the topics which are managed by the broker.

Brokers :- When the broker receive data for a topic from the publisher, it sends the data to all the subscribed consumers.

- Brokers responsibility is to accept data from publishers and send it to the appropriate consumer.

③ push-pull model :-

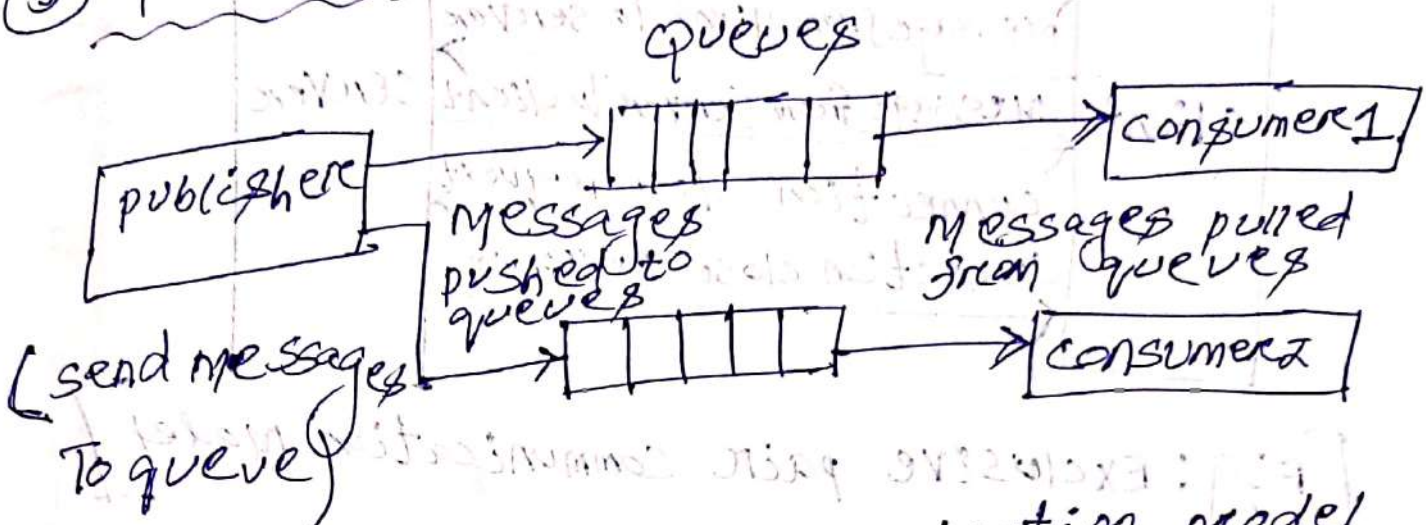
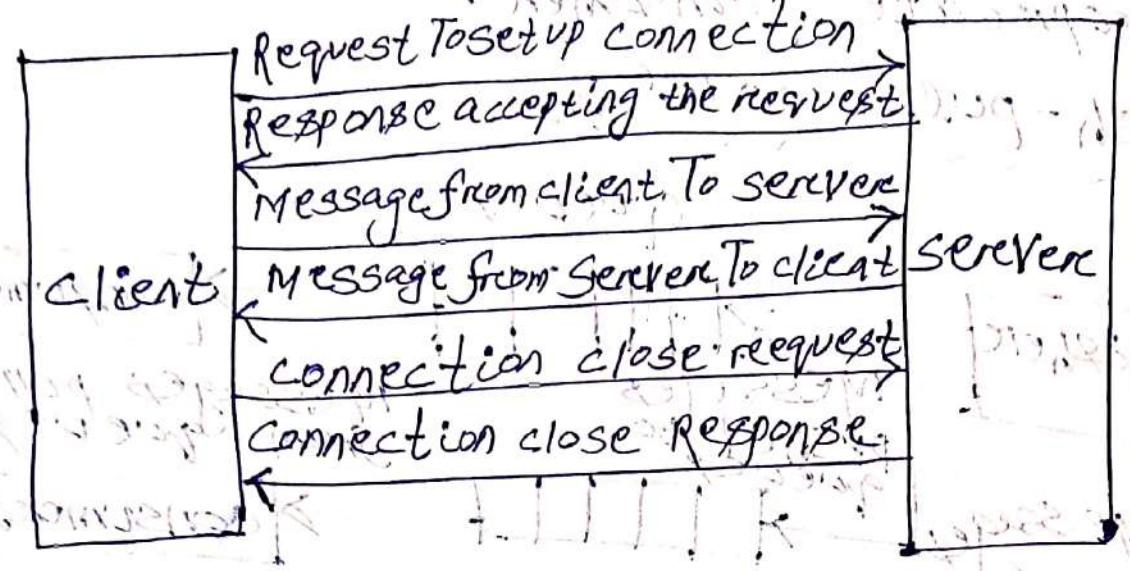


Fig: push-pull communication model

- push pull is a communication model, in which the data producers 'push' the data to queues & the consumers 'pull' the data from queues.
- producers & consumers are not aware of each other.
- queues act as buffers & are useful when there is a mismatch between the rate at which the producers push data & the data rate at which the consumers pull data.

④ Exclusive pair communication Model :-

- Exclusive pair is bidirectional, full duplex communication model that uses a persistent connection between client & server.



[Fig: Exclusive pair communication model]

- The connection is persistent & remains open till client sends a request to close the connection.
- This is a stateful connection model & server is aware of all open connections.
- Client & Server can send messages to each other after connection setup.

IOT communication APIs :-

API :- set of functions, protocols, routines & tools used fore building application software.
→ (Application programming Interfaces)

Generally There are 2 APIs used fore IOT communications :-

① REST - based communication APIs.
② Web socket based communication APIs.

① REST based communication APIs :-

- Representational state Transfer (REST) is a set of architectural principles by which you ~~and~~ can design Web-services & Web APIs that focus on a system resources & how system resource states are addressed & transferred.
- REST APIs follow the request response communication model.
- The following REST architectural constraints applied to the components, connectors & data elements within a hypermedia system :-

① client server :- The principle behind the client server constraints is the separation of concerns.

Example :- - clients should not concerned about storage, it is concern of server.
- server should not concern about user interface. It is concern of clients.

so, this separation allows clients & server to be independently developed & uploaded.

② Stateless :- Each communication should be independent of others.
- Each request from client should be include all the information required to understand the request.

③ Cacheable :- cache constraints requires that the data within a response to a request be implicitly (or) explicitly labeled as cacheable (or) non cacheable. If it is cacheable then the client is given right to reuse that response for later for equivalent requests.

④ Layered system :- Layered system constraints, constraints the behavior of components, such that each component can't see beyond the intermediate layers during interaction

Example :- A client can't tell if it is directly connected to server (or) intermediatary along the way.

⑤ Uniform Interface :- Interface constraints requires that the method of communication between a client & a server must be uniform.

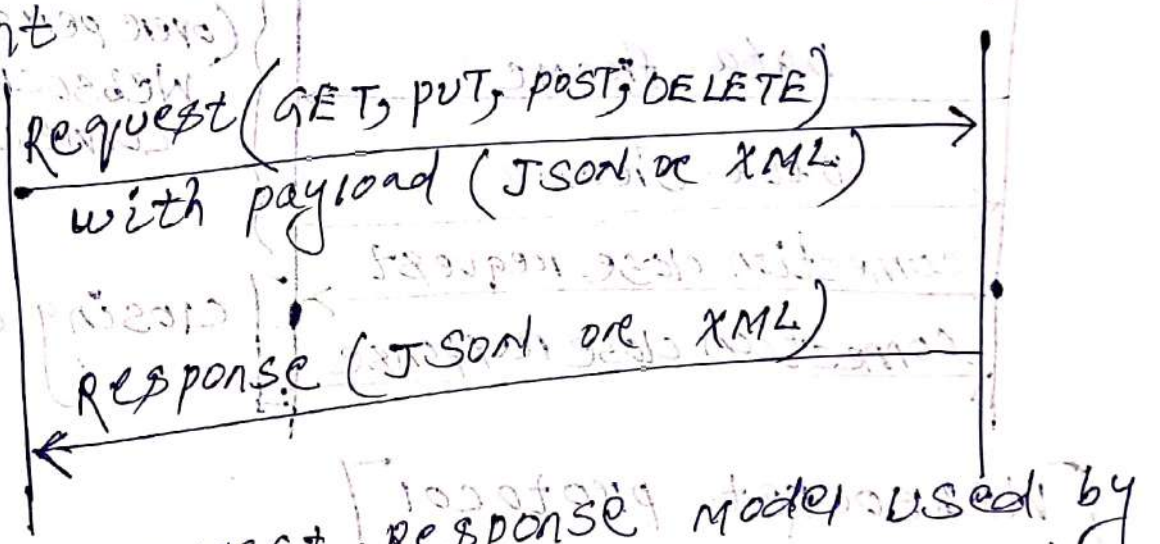
⑥ client $\xrightarrow{URI}$ server

⑥ Code on Demand (optional):-

Servers can provide executable code (or) scripts for clients to execute in their context.

communication between client & server using REST API:

* Resources are represented by URI.
- clients send request to those URIs using method defined by HTTP protocol (like GET, PUT, POST, DELETE)



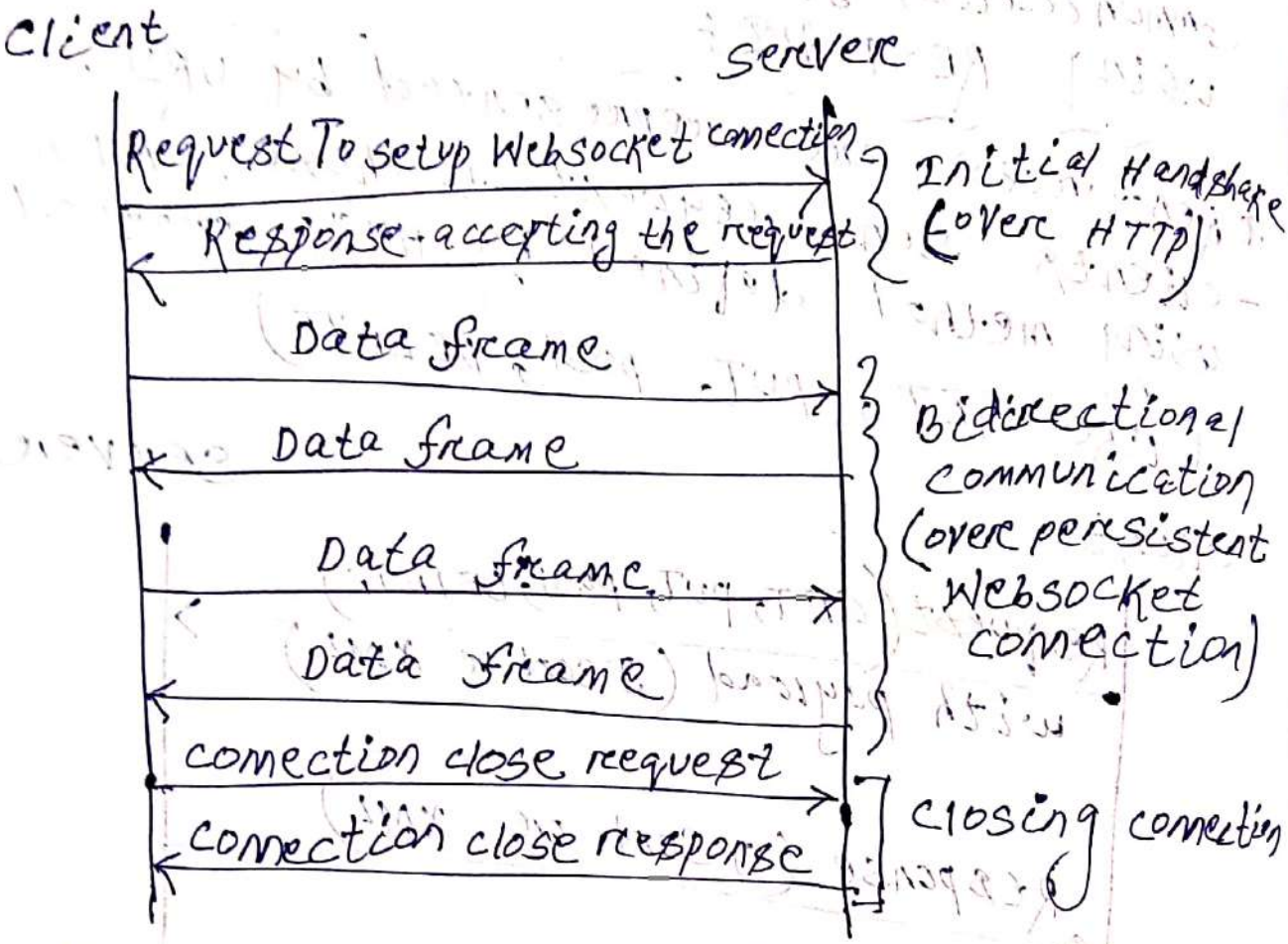
[Fig: Request Response model used by REST]

JSON → Java script object notification.
XML → Extensible markup Language.

② Websocket based communication APIs:-

- Websocket APIs allow bidirectional, Full duplex communication between clients & servers.
- It follows Exclusive pair communication model.

- It doesnot require a new connection to be setup for each message sent.
- Websocket suitable for IOT applications that have low latency (or) High throughput requirements.



[Websocket protocol]

[Fig: Request response model used by REST]

② Websocket based communication APIs :-

- Websocket APIs allow bidirectional, Full duplex communication between clients and servers.
- It follows Exclusive pair communication model.

- It doesnot require a new connection to be set up for each message sent.
- Websocket APIs reduce the network traffic and latency as there is no overhead for connection setup and termination requests for each message.
- Websocket suitable for IOT applications that have low latency (or) high throughput requirement.

Difference Between IOT & M2M :-

(Machine To Machine) M2M	Internet of Things (IOT)
- In M2M, two (or) more machines can communicate with each other & carry out certain functions without human intervention.	- IOT means Internet of Things a network of internet connected devices able to sense, collect & exchange information.
- Devices do not necessarily require internet connections.	- Devices require internet connections.
- It supports point to point communication.	- It supports cloud communication.
- It communicates through a proprietary cellular (or) wired network.	- It communicates in standard based IP networks.
- M2M use proprietary & non IP based communication protocols. Ex:- zigbee, Bluetooth, mobiles, IEEE 802.15.4	- IOT uses IP protocols Ex:- HTTP, COAP, DDS etc.

Machine To machine communication (M2M):

- In M2M communication, objects/devices/machines can talk to each other without human intervention.
- M2M means two machines communicating (or) exchange data without human interaction.
- Like IOT, M2M allows virtually any sensors to communicate which opens up the possibility of systems monitoring themselves and automatically responding to changes in the environment, with a reduced need for human involvement.

Example - vending machine

① Sensor detects that the vending machine is out of cold drinks → ② Message is automatically sent to the warehouse. → ③ Route driver is notified that machine at given location needs to be refilled.

- M2M is typically more emphasized on embedded hardware.
- Data collected is not shared with other applications.
- Less scalable than IOT.
- M2M communication is used for monitoring & control of one (or) few infrastructure or assets.
- M2M is mostly hardware based Technology.
- Machines normally communicate with a single machine at a time.
- M2M applications include vending machines, ATMs, smart meters.
- Isolated systems of devices using same standard.

- IOT is more focused on sensors & interfacing various components of IOT systems are sensors, internet & networking infrastructures.
- Data is shared with other applications (like weather forecasts, social media etc). It improve end users experience.
- More scalable due to cloud based architecture.
- IOT is used to address everyday needs of humans.
- IOT is both Hardware & software based Technology.
- Many users can access at one time over the Internet.
- IOT applications include smart cities, offices, homes, Telehealth, connected car, Wearables etc.
- Integrates devices, data & applications across varying standards.

- Machines communicating with machine.
- It is only for B2B (Business To Business) business Type.
- M2M systems typically have homogeneous machine types within an M2M area network.
- M2M data is collected in point solutions & can be accessed by on-premises applications such as diagnosis applications, service management applications & on premised enterprise applications.
- M2M is Typically more emphasized on embedded hardware.

- Machines communicating with machines, humans with machine & machines with humans.
- It is for B2B and B2C business type. (B2C: Business To consumer)
- Things in IOT refers to physical objects that have unique identifiers & can sense & communicate with their external environment (and used applications) or their internal physical states.
- IOT data is collected in the cloud & can be accessed by cloud applications such as analytic applications, enterprise applications, remote diagnosis & management applications.
- IOT is more focused on sensors & interfacing. various components of IOT systems are sensors, internet & networking infrastructures.

- Linear Value chain.

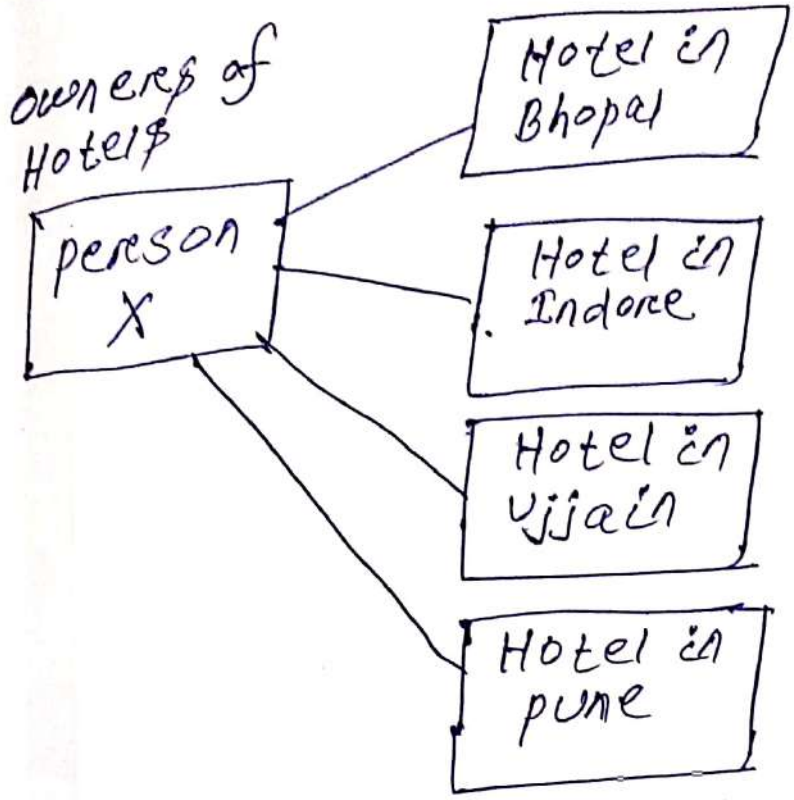
- non Linear Value chain:

Mobile — AC
— car
can operate — Lights

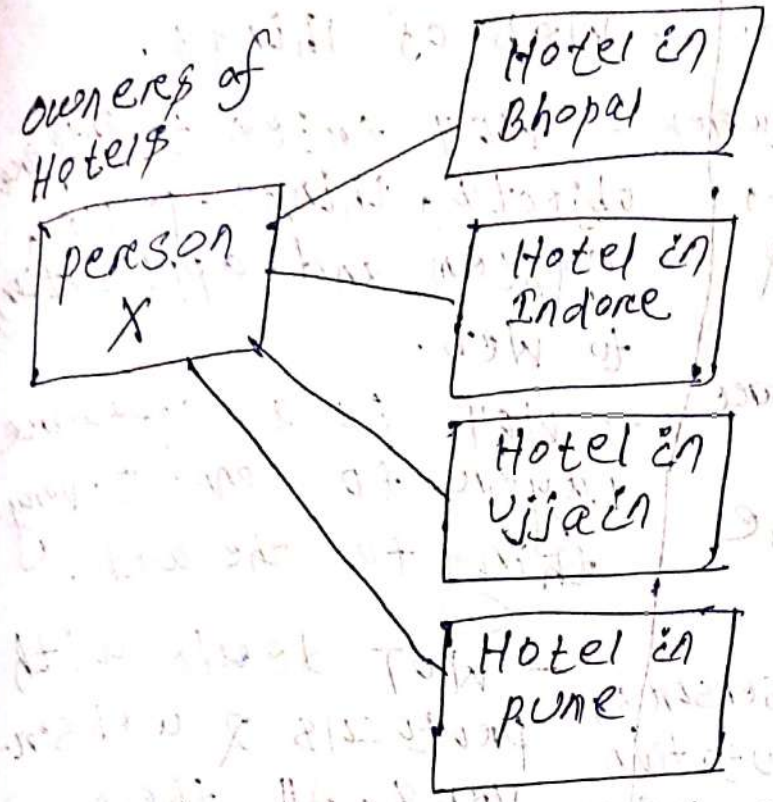
IOT Limitations:-

- IOT allows us to interact with different devices through Internet with the help of smartphones (or) computers, thus creating a personal network.
- But here to interact with n no. of different devices we need to install n different applications which is inconvenient for users.
- It is challenging (time consumely) to build a single communication platform where all devices can communicate effectively with one another in different ways.
- Wouldn't it be convenient to have one interface to connect all the devices?
- We know that Web is already being used as a system to communicate with each other.
- So Web can also be used in such a way that all things can communicate with each other in the most efficient manner by integrating them together.

- WOT (Web of Things) allows the use of web services to connect anything in the physical world, besides human identities on web.
- WOT is a term used to describe approaches, software architecture styles and programming patterns that allow real world objects to be part of the world wide web.
- WOT provides an application layer that simplifies the creation of the Internet of Things.
- WOT enables access & control over IOT resources & applications using mainstream web technologies such as HTML 5.0, Java script, Ajax, etc.
- The approach to building WOT is therefore based on RESTful principles & REST APIs, which enables both developers and deployers to benefit from the popularity & maturity of web technologies.



- person X can connect all the appliances in all the rooms of his hotels, so that he is able to monitor, control & improve the management of his hotels from any place using a single web based application "hotel control center".



- person X can connect all the appliances in all the rooms of his hotels, so that he is able to monitor, control & improve the management of his hotels from any place using a single web based application "hotel control center".

IOT limitation :-

- It is very difficult to establish an effective communication between different machines of different vendors. Due to this limitations in IOT, WOT comes in picture.
- WOT focused on reusing the already established web system to help every-day connected devices (IOT devices) connect to one single application i.e. on web. so that they can store information & communicate with each other.

IOT	WOT
- Internet of Things.	- Web of Things.
- IOT creating a network of objects, things, people, system & applications.	- WOT tries to integrate objects, things, people, system and applications to web.
- IOT is a hardware Layer to connect everything to the Internet.	- WOT is a software Layer to connect everything to the web.
- IOT deals with sensors, actuators, computation & communication interfaces. From a box of apples with a RFID tag, to smart city and to everything in between, all these digitally augmented objects make up the IOT. (RFID - Radio Frequency Identification)	- WOT deals with protocols & web servers. All those applications for IOT devices make up the WOT.
- For each & every IOT devices there is a different protocol.	- WOT makes it easy by using single protocol for multiple IOT devices.
- Communication over network Layer (IP) RFID, Zigbee, Bluetooth, COAP, LowPAN.	- Communication over application Layer (HTTP). HTTP, REST, URI, HTML 5.0

- In IOT, hundreds of incompatible protocols co exit, this makes the integration of data and services from various devices extremely complex & costly.
- IOT is usually focusing on the Lower Layer of the OSI stack.
- Lack of standard communication protocol.
- Identifiable things are RFID, QR-code.
- IOT standards & prototypes are privately Funded & are not publicly accessible.
- IOT platforms are hard to program due to multiple protocols.
- IOT is tightly coupled between the applications & networks.

- In WOT, any device can be accessed using standard web protocols connecting heterogeneous devices to the web makes the integration across systems and applications much simpler.
- WOT only deals with the OSI Layer 7 which is Application Layer, which handles Applications services and data.
- Communication through RESTful API.
- Things are identified by URI.
- WOT is free for anyone & can be accessed anywhere, anytime.
- Due to common APIs to handle the protocol WOT programming is easiere.
- WOT in application Layer is loosely coupled.

SENSORS :-

- As we know that Human beings collect information of the surroundings using their sense organs (sensors), namely eyes, ears, nose, skin etc. In order to perform various tasks.
- Similarly, systems must interact with their environment to do useful tasks. So they use sensors and actuators.
- Without the use of sensors, there would be no automation.
- Sensors can be embedded in our bodies, automobiles, airplanes, cellular Telephones, radios, chemical plants, industrial plants and many other applications.

sensor - It is a device/module/machine subsystem.

purpose : To detect events (or) changes in its environment and send the information to other electronic devices.

- sensor is a device that measures a physical variable (Ex:- force, pressure, Temperature, velocity, flow rate etc) & converts the physical quantity into another form (Electrical form)

which can be read by an observer (or) by an instrument.

Example :- → Heat is converted to electrical signals in a Temperature sensor.

→ Atmospheric pressure is converted to electrical signals in a barometer.

→ A Thermocouple converts Temperature to an output voltage which can be read by a voltmeter.

properties / Features of sensors

① It is only sensitive to the measured property.

Example :- A Temperature sensor senses the ambient temperature of a room.

② It is insensitive to any other property likely to be encountered in its application.

Example :- A Temperature sensor does not bother about light (or) pressure while sensing the Temperature.

③ It does not influence the measured property.

Example :- Measuring the temperature does not reduce (or) increase the temperature.

CHARACTERISTICS OF SENSORS :-

① High sensitivity :- sensitivity indicates how much the output of the device changes with unit change in input (quantity to be measured)

② Linearity :- The output should change linearly with the input.

③ High Resolution :- Resolution is the smallest change in the input that the device can detect.

④ Less noise and disturbance.

⑤ Less powere consumption.

⑥ Range - Difference between the maximum and minimum values of the input that can be measured.

⑦ Responses - should be capable of responding to the changes in minimum time.

⑧ Accuracy - No deviation from exact quantity.

⑨ sensitivity - change in output / change in input.

⑩ Repeatability - Deviation from reading to reading, ~~The ability of the sensor~~ when these are taken for a number of times under identical conditions.

i.e. The ability of the sensor to output the same value for the same input over a number of trials.

components of a sensor node:-

↓ sensing unit ↓ processing unit ↓ Transceiver ↓ power unit

- sensor is a device that is used to gather information about a physical process (Temperature, pressure, light, sound, motion, flow, humidity, radiation etc) and translate it into electrical signals that can be processed, measured and analysed.
- A Wireless sensor network consists of sensor nodes that are deployed in high density and often in large quantities and support sensing, data processing, embedded computing and connectivity.

sensor node:- A sensor node in Wireless sensor network consists of 4 basic components ① power supply ② sensor ③ processing unit ④ communication system.

sensing unit:- It is usually composed of two subunits. ⓐ sensors ⓑ Analog To Digital converters.

The sensor collects the analog data from the physical world and an ADC converts this data to digital data. Then these digital data/signals are fed in to processing unit.

processing unit :- The main processing unit which is usually a microprocessor (or) a microcontroller, performs an intelligent data processing and manipulation.

- It is generally associated with a small storage unit.

communication unit/Transceiver :-

- It connects the node to the network. communication unit consists of radio system, usually a short range radio for data transmission and reception.

power unit :- As all the components are low power devices, a small battery like CR-2302 is used to power the entire system.

- A sensor node can only be equipped with limited power source (< 0.5Ah, 1.2 Volt)
- There are some other subunits of a sensor node that are application dependent.

Location Finding System :-

↳ Location finding system is commonly required because most of the sensor network routing techniques and sensing tasks require knowledge of location with high accuracy.

Mobilizer :- A mobilizer needed to move sensor nodes when it is required to carry out the assigned tasks.

Sensor classes

- Based on output
  - Analog sensors
  - Digital sensors
- Based on data type
  - Scalar sensors
  - Vector/multimedia

Examples :- Accelerometers, pressure sensors, temperature sensors.

- Based on External power
  - Active sensor
  - passive sensor

Analog sensors :-

- sensors that produce continuous analog output signal are analog sensors.
- Analog sensors senses the external parameter (like wind speed, solare radiation, Light intensity etc) and gives analog voltage as an output. Thus the output voltage may be in the range of 0 to 5 volt.
- Examples of analog sensors are accelerometer, pressure sensors, Light sensors, Sound sensors, Temperature sensors and so on.
- The Temperature of a liquid can be measured using a Thermometer (or) Thermocouple (example in geysers) which continuously responds to temperature changes as the liquid is heated up (or) ~~called~~ cooled down.

pressure Sensor :- It will produce an analog output signal that is proportional to the amount of applied pressure.

Accelerometers :- sensors that detect changes in position, velocity, orientation, vibration and tilt by

sensing motion are called as accelerometers.

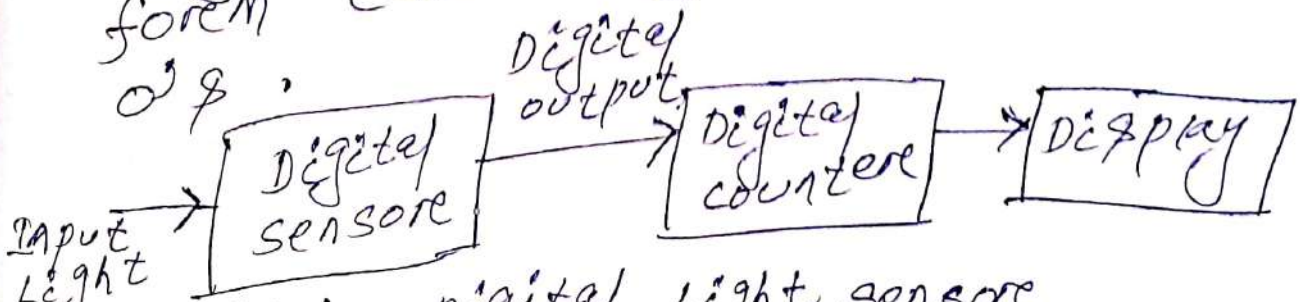
Light sensors :- sensors that are used for detecting the amount of light striking the sensors are called as light sensors.

Example :- LDR (Light dependent Resistor).

Analog Temperature Sensor :- Thermistor is a thermally sensitive resistor that is used for detecting changes in temperature. If the temperature increases, then the electrical resistance of thermistor increases. Similarly if temperature decreases, then resistance decreases.

Digital Sensor :-

- The sensors which produces discrete output (0's and 1's) is known as digital sensor.
- It generates output in binary digital form consisting of binary 1's and 0's.



ex :- Digital Light sensore

- Digital Light sensor uses rotating disc to generate output pulse with Logic 0 and Logic 1.
- These pulses are counted by the digital counter and final output is displayed on the numeric display.
- Digital sensors are capable of overcoming the drawbacks of analog sensors.
- Digital sensor produce discrete values (0 & 1). Discrete values often called digital (binary) signals in digital communication.
- Analog signals are much affected by external noise and create errors in the output signal. But digital signals are susceptible to noisy environments and hence digital sensors are preferred over analog ones.

— x —

Difference between Analog and Digital sensors :-

Analog Sensors

- It gives an output that varies continuously as the input changes. i.e. output is analog signal.
- output can have infinite number of values within sensor's range.
- It requires analog to digital conversion before feeding to the digital controller.
- More prone to noise.
- Analog sensors ideal for reading continuous varying parameters such as temperature, pressure, humidity etc.
- Examples of Analog sensors: Thermocouple, pressure sensor, Accelerometer, Light sensors.

Digital Sensors

- It generates output in binary digital form consisting of 0's and 1's i.e. output is digital.
- As output varies in discrete steps (or) levels, so it have a finite number of values.
- Digital sensors produce digital outputs that can be directly interfaced with the digital controller.
- Less prone to noise.
- Digital sensors is ideal for reading discrete values (i.e. binary values 1 & 0) such as push bottom switch.
- Examples of Digital sensors: Digital Light sensor, push button, distance sensor, Line Follower sensor.

- Accuracy in reading the output is low.	- Accuracy in reading the output is high.
- Analog sensor consists of amplifiers, ADC.	- Digital sensor consists of cable and transmitter.
- cheap compared to Digital sensors.	- Expensive.
- Response time is Low.	- Response time is high.

Scalar sensor (vs.) vector sensor

Scalar sensor	vector sensor
- These sensors produce output signal (or) voltage which is generally proportional to the magnitude of the quantity being measured.	- vector sensors produce output signal (or) voltage which is generally proportional to the magnitude direction as well as the orientation of the quantity being measured.
- physical quantities such as temperature, colour, pressure etc. are all scalar quantities as only there magnitude is sufficient to convey an information.	- physical quantities such as sound, image, velocity, acceleration, orientation etc. are all vector quantities, as only their magnitude is not sufficient to convey the complete information.

Example :- The temperature of a room can be measured using a thermometer (or) thermocouple which respond to temperature changes irrespective of the orientation of the sensor (or) its direction.

Example :- The acceleration of a body can be measured using an accelerometer which gives the components of acceleration of the body with respect to the x, y, z co-ordinate axes.

Active sensor	passive Sensor
- It does not need the external power supply for operation.	- It needs external power supply for operation.
- They are self generating sensors.	- They are not self generating sensors.
Example :- Thermocouple, photocell, piezoelectric	Example :- Thermistor, LDR, LVDT etc.

SENSOR TYPES :-

- sensors are helpful in making things done without human intervention.
- sensors are devices which can be used to sense/detect the physical quantity like force, pressure, strain, light etc. & then convert it into desired output like the electrical signal to measure the applied physical quantity.

- There are different types of sensors available in the market. We need to select the desired sensor based on our project (or) application.
- mostly used sensors by IOT Applications are:-

Temperature sensors	chemical sensor	Level sensors
proximity sensor	Gas Sensor	Image sensors
pressure sensor	smoke sensor	motion detection sensors
Water quality sensor.	IR sensors	Accelerometer sensors

① Temperature sensor :-

- It is a device which is used for measuring the temperature of anything (or) anyplace.
- A device which gives temperature measurement as an electrical signal (electrical voltage) is called as temperature sensor.
- Before IOT technology, these are mostly used in computers, AC, refrigerators and similar devices used for environment control, but with the advent of IOT world, they found their role in manufacturing processes, agriculture and health industry.

Example of Temperature Sensors :-

Thermocouples	Resistor Temperature Detector (RTD)	Thermistors	IC semiconductor sensor
- Voltage Devices that indicate temperature measuring with a change in voltage. - As Temperature goes up the o/p voltage of the thermocouple rises.	- The Resistance of the device is directly proportional to the Temperature, increase in a positive direction when the temperature rises resistance goes up.	- Temperature sensitive resistor that change its physical resistance with change in Temperature. - (-ve) direction Temp↑ ⇒ Resistance ↓	- Linear devices where the conductivity of the semiconductor increases linearly. - provide direct Temperature reading in digital form.

Infrared Sensors :-

- It detects temperature by interrupting a portion of emitted infrared energy of the object (or) substance and sensing its intensity, can be used to measure temperature of solids and liquids only.

(2) proximity sensors :-

- A device that detects the presence (or) absence of a nearby object (or) properties of that object & converts it into signal which can be easily read by user (or) a simple electronic instrument without getting contact with them.
- used for parking availability in places such as malls, stadiums (or) airports.
- used in retail industry, as they can detect motions & the correlation between the customer & ~~the~~ product they might be interested in. A user is immediately notified of discounts and special offers of nearby products.

Example :- Inductive sensors, capacitive sensors, photo electric sensors, ultrasonic sensors.

pressure sensor :-

- A pressure sensor is a device that senses pressure & converts it into an electric signal. Here the amount depends upon the level of pressure applied.
- There are many devices that rely on liquid (or) other forms of pressure.
- pressure sensors make it possible to create IOT systems that monitor systems and devices that are pressure propelled.
- With any deviation from the standard pressure range, the device notifies the system administrator about any problem that should be fixed.

Water quality sensor :-

- It is used to detect the water quality used in variety of industries.
- Most common used water sensors are:-

chlorine Residual sensor :-

- It measures chlorine residuals in water and most widely used as disinfectant because of its efficiency.

Total organic carbo sensor :-

- It is used to measure organic element in water.

Conductivity sensor:- It is used to obtain information on Total ionic concentrations (i.e. dissolved components) in water solutions.

pH Sensor :- It measures pH value of water.

Oxygen Reduction potential Sensor:-

- The ORP measurement provides insights into the Level of oxidation reduction reaction occuring in the solution.

Chemical Sensors :-

- These are used to indicate changes in liquid or to find out air chemical changes.
- It is mostly used in Industrial environment monitoring & process control, intentionally or accidentally released harmful chemical detection, explosive and radioactive detection etc.

Most commonly used chemical sensors are :-

chemical field effect Transistor, pH glass electrode, Fluorecent chloride sensor, electrochemical gas sensor etc.

Gas sensor :- It is used to monitor changes in the air quality and detect the presence of various gases.

- used in numerous industries such as agriculture, health.
- used for air quality monitoring, detection of toxic or combustible gas, hazardous gas monitoring in coal mines, oil & gas industries etc.

Examples :- Air pollution sensor, CO_2 sensor, oxygen sensor etc.

Smoke sensor :-

- It is a device that senses smoke and its level.
- With the development of IOT, These sensors are now plugged in to a system that immediately notifies the user about any problem that occurs in different industries.
- Expensively used to detect fire & gas incidences and helps to protect people working in dangerous environments.

Examples :- optical smoke sensor, Ionization smoke sensor.

IR sensors :- It is used to sense certain characteristics of its surroundings by either emitting (or) detecting infrared radiations.

- It is also capable of measuring the heat emitted by the objects.

- used in health care to make monitoring of blood flow & bp.
- used in smart devices such as smart watches & smartphones.
- It is a great tool for ensuring high level security in your home.

Level sensors :- It is used to determine the level or amount of fluids / liquids or other substances that flow in open or closed system.
- used in sea level monitoring & Tsunami warning, medical equipments, compressors etc.

Image sensors :- These are instruments used to convert optical images into electronic signals for displaying or storing electronically.
- It is used in digital camera, medical imaging, Thermal imaging devices, radar etc.

Motion detection sensors :- It is an electronic device used to detect the physical movement (motion) in a given area & it transforms motion into an electric signal, motion of any object or motion of human beings. It is used for security purpose like automatic door control, smart camera

(i.e. motion based capture/video recording), automatic parking systems, ACs etc.

Accelerometer Sensors:-

↳ Accelerometer detect an object's acceleration i.e. The rate of change of the object's velocity with respect to time.

↳ This is great for monitoring your driving fleet or using a smart pedometer.

↳ Widely used in cellular & media devices, vibration measurement, movement detection etc.

Humidity sensors:-

- It is defined as the amount of water vapor in an atmosphere of air (or) other gases.
- Humidity sensors measure the humidity commonly found in heating, vents & air conditional (HAVC) system in both industrial & residential domains.
- Also used in hospitals & meterology stations to report and predict weather.

SENSOR ERRORS :-

- A main challenge to using sensors in activity recognition is the different types of errors and noises their measurements or signals suffer from.
- Such errors can mislead an activity recognition module from recognizing which activity the sensor signals measured correspond or do not correspond to.

↳ There are different types of deterministic errors in sensors which can be estimated & compensated through Laboratory calibration.

Some errors are :-

1. offset error or bias
2. Drift
3. Hysteresis error
4. Quantization.

Input - refers to actual true quantity

output - refers to the measurement reading of the sensor.

1. offset error or Bias :-

It is the value of the constant non zero output when the input is zero

(or)

If the output signals differs from the correct value by a constant, the sensor has an offset error (or) bias.

(2) Drift :-

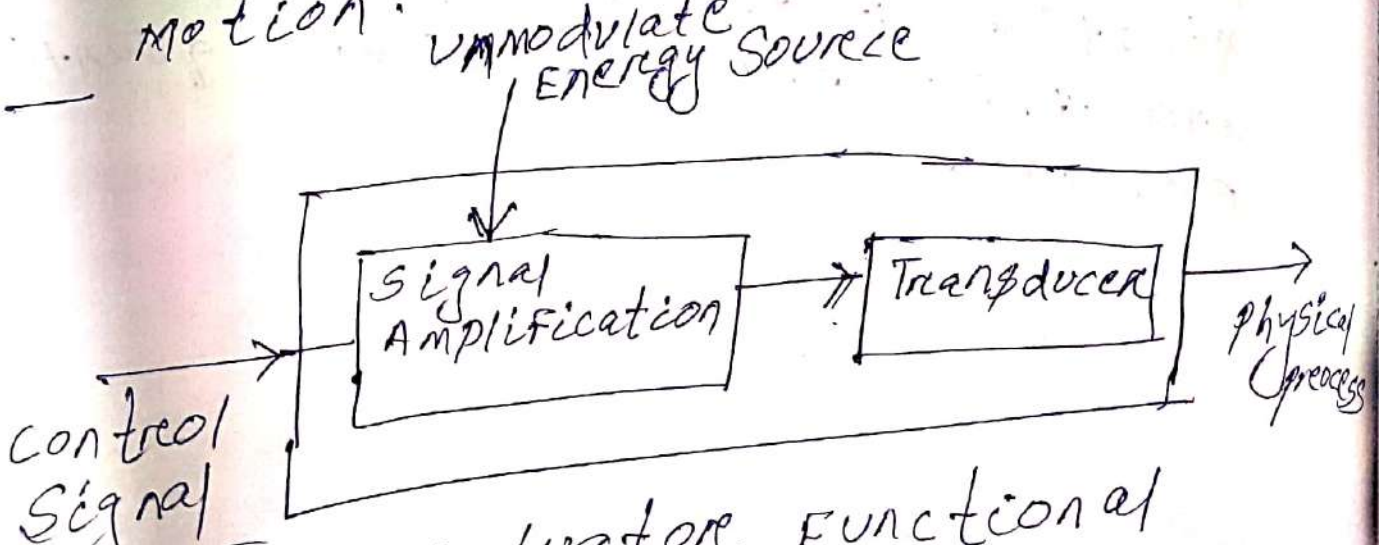
- If the output signal slowly changes independent of the measured property this is defined as drift.
- Long term drift over month (or) years is coursed by physical changes in the sensor.

(3) Hysteresis :- It is an error in which sensor's output for the same input value changes depending on whether the input is increasing (or) decreasing
- It is actually exists in magnetic compasses & pressure sensors.

(4) quantization error :- It exists in digital systems and it is caused by the conversion from analog to digital values.
- If the sensor has digital output, the output is essentially an approximation of the measured property and this error is called quantization error.

ACTUATOR :-

- These are devices used to produce action or motion.
- It is a device that starts (or) stops mechanical equipment with the help of Hydraulic fluid, Electric current, air (or) other sources.
- Actuators are usually used in automation to control the motion of a moving member in any machine.
- An actuator requires a control signal & a source of energy.
- After receiving a control signal, the actuator responds by converting the energy in to mechanical motion.
- After receiving a control signal, the actuator responds by converting the energy in to mechanical motion.
-



[Fig: Actuator Functional Diagram]

- Amplifier converts the (Low power) control signal in to a high power signal.
- Transducer converts the energy of the amplified control signal in to work.
- Depending on the source of power, actuators can be categorized in to following types :-

① Hydraulic Actuator ② pneumatic Actuator ③ Electrical Actuator.
④ Thermal / Magnetic Actuator.
⑤ Mechanical Actuator.
⑥ Soft Actuator.

Hydraulic Actuator :-

- These actuators utilize Hydraulic Energy for automation.
- A Hydraulic actuator consists of a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation.
- The mechanical motion is converted to linear, rotatory (or) oscillatory motion.
- So, hydraulic actuators can produce rotatory, linear or oscillatory motion.
- They have high force capabilities and are preferred to conditions where heavy equipments are to be moved.

- These actuators can generate a large output force for very small input force & are also able to maintain its mechanical stiffness.
- Applications of hydraulic sensors are in
  (i) close loop velocity controlling.
  (ii) High precise positioning for heavy loads.
- Typical Hydraulic Actuator consists of a hollow cylinder & piston arrangement.
- The piston can execute reciprocating motions by pressurizing and depressurizing the cylinder, to move the mechanical system.

Pneumatic Actuator :-

↳ A pneumatic actuator converts energy formed by vaccum (or) compressed air at high pressure in to either linear (or) Rotatory motion.

↳ Similar to hydraulic actuators pneumatic actuators also contain a piston cylinder arrangement, but they also have valves or ports to control the inflow & outflow of air to increase or decrease the pressure.

- The size of those valves greatly determines the power delivery capacity of pneumatic actuators.
- pneumatic rade and pinion actuators are used for valve control of water pipes.
- pneumatic energy quickly responds to starting & stopping signals.
- The power source does not need to be stored in reserve for operation.
- pneumatic actuators enable large forces to be produced from relatively small pressure changes.

Ex:- pneumatic brakes are very responsive to small changes in pressure applied by the driver.

- It is responsible for converting pressure in to force.
- Here the proper sealing is necessary to avoid any Leakage.

Electrical Actuator:-

- These actuators are powered by electric source.
- Electric Actuator is actuated by motor that converts electrical energy in to mechanical Torque.
- The electrical energy is used to actuate equipment such as solenoid valves which

control the flow of water in pipes in response to electrical signals.

- Electric actuator consists of electric motor, speed reducer, position limit mechanism and over torque protection mechanism & position feedback device.
- These actuators are commonly used in control systems. Because they can be easily interfaced with controlling equipments & electric energy is easier to control & use.
- No leakage issue with these actuators but electrical short circuiting can cause fire accidents.
- Electric actuators are considered as one of the cheapest, cleanest & speedy actuator types available.

Thermal/Magnetic Actuators:-

- These actuators are actuated by applying thermal or magnetic energy.
- These use shape memory materials like shape memory alloys (or) magnetic shape memory alloys.
- They tend to be compact, light weight, economical & with high power density.
- In MEMS (Micro Electro Mechanical) system thermal actuator where small amount of thermal expansion of one part of the device translates to a large amount of deflection of the overall device.

- MEMS magnetic Actuator is a device that use MEMS to convert an electric current in to a mechanical output.

Mechanical Actuator :-

- A mechanical actuator converts rotary motion in to Lineare motion to execute some movement.
- It involves gears, pulleys, chains & other device to operate.
- The main advantage of these actuator is that small input force can produce very large output force.

Examples :- screw-Jack, Wheel & axle, rack & pinion.

Soft Actuators :-

- soft actuators (ex:- polymer based) are designed to handle feagile objects like fruit harvesting in agriculture (or) manipulating the internal organs in biomedicine.
- They produce flexible motion due to the integration of microscopic changes at the molecular level into a macroscopic deformation of the actuator meterials.

IOT Service oriented Architecture :-

- IOT aims to connect different things over the networks.
- As a key technology in integrating heterogeneous systems (or) devices, SOA (software oriented Architecture) can be applied to support IOT.
- SOA efficiently combines individual unit of software to provide higher level of functionality.
- Service oriented Architecture is an architecture based on reuseble well defined services implemented by IT components.
- SOA provides platform, technology & language independence.
- A service is a function that is well defined, self contained & does not depend on the context or state of other services.

IOT SOA consists of following 4 layers :-

① Sensing Layer :- This Layer is integrated with existing hardware (RFID, sensors, actuators etc) to sense/control the physical world & acquire data.

- In the sensing layer, the wireless smart systems with tags or sensors are now able to automatically sense & exchange

information among different devices.
- It is used to gather data from various sensor objects/devices.
- This Layer consist of sensor connected devices, these are the small memory constrained, often battery operated electronic devices with onboard sensors & actuators.
- These devices could either function as standalone sensing devices or be embedded as part of a bigger machinery for sensing & control.
- This Layer acquires information with respect to basic resources (names, addresses & so on) & related attributes of objects by means of automatic identification & perception technologies such as RFID, wireless sensors & satellite positioning.
- sensors, RFID tags & all other uniquely identifiable objects/things acquire real time information (data).

② Network Layer :-

- It provides basic networking support & data transfer over wireless (or) wired network.
- The role of this Layer is to connect all things together & allow things to share the information with other connected things.

- To design the networking layer in IOT, designers need to address issues such as network management technologies for heterogeneous network (such as fixed, wireless, mobile etc), energy efficiency in networks, QOS (quality of service) requirements, service discovery & retrieval, data & signal processing, security & privacy.
- This layer provides the infrastructure to support over wired (or) wireless connection among things.
- The various IOT devices of sensing layer to be connected to the internet via a more powerful computing device called the IOT gateway (networking device)
- Gateway aggregates data from numerous sensing devices & relays it to the cloud.
- IOT gateways are equipped with multiple communication capabilities like bluetooth, Zigbee, Low Range Wide Area Network etc to talk to the IOT devices on one end & a connection to the IP (Internet) based network on the other side over wifi, Ethernet (or) cellular network.

- The data that is collected by Layer 1 devices need to be transmitted & processed. That is the network Layer's Job.
- Network Layer connect these devices to other smart objects, servers & network devices.
- It also handles the transmission of all of the data.
- To design the networking Layer in IOT, designers need to address issues such as network management technologies for heterogeneous network (such as fixed, wireless, mobile etc); energy efficiency in networks, QOS requirements, service discovery & retrieval, data & signal processing, security & privacy.

③ Service Layer :-

- service Layer creates & manages services.
- It provides services to satisfy user needs.
- It relies on the middleware technology that provides functionalities to seamlessly integrate services & applications in IOT.
- The middleware Technology provides the IOT with a cost efficient platform, where the hardware & software platforms can be reused.
- This is a software middleware sitting between processing communication hardware & IOT applications providing a rich set of functions needed by many IOT applications.

- A main activity in the service layer involves the service specifications for middleware, which are being developed by various organizations.
- This layer includes the following components :-
  1. service discovery - It find objects that can offer the needed services & information in an efficient way.
  2. service composition - It enables the interaction & communication among connected things.

     It schedule or recreate more suitable services in order to acquire the most reliable services to meet the request.
- This layer tackles the information heterogeneity issues by intelligent interfaces.
- The functional solutions of this layer mainly consists of
  1. Data storage (Database & mass storage Technology)
  2. Heterogeneous data retrieval (search engine)
  3. Data Mining, 4. Data security
  5. privacy protection.
- The SOA layer is built on top of the network layer. It is used to handle heterogeneous data from the sensor layer.

(4) Application Layer :-

- This Layer provides the interaction methods with user application.
- The application Layer is what the user interacts with.
- This Layer is responsible for delivering application specific services to the user.
- Example when user Tap a button in the mobile app, coffee machine will turn on.
- various IOT applications include Home Automation, E-health, E-Government etc.
- The application Layer serves to a specific user request utilizing the information from the three Layers.

IEEE 802.15.4 :-

- The Institute of Electrical & Electronics Engineers (IEEE) supports many working groups to develop & maintain wireless and wired communication standards.

802.3 is wired Ethernet.
802.11 is for wireless LAN (WLANs/WiFi)
802.15 group of standards specifies a variety of wireless personal area network (WPANs) for different applications.
802.15.1 is Bluetooth
802.15.3 - High Data rate category for ultra wide band technologies.

802.15.6 is for Body Area Networks (BAN)
802.15.4 - Largest standard for Low data rate WPANs.

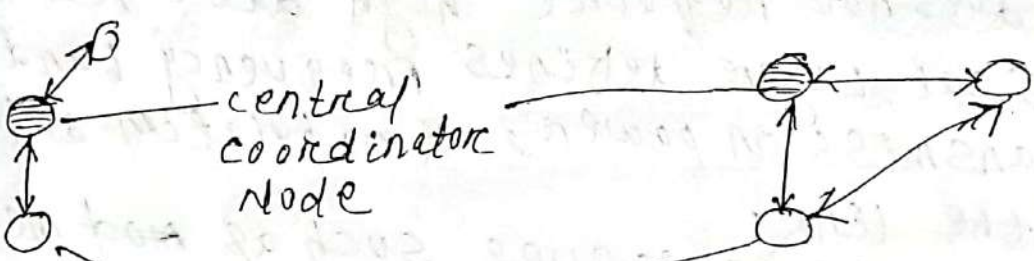
- IEEE 802.15.4 is the standard which is the basis for many Low power wireless connectivity solutions including Zigbee, 6LOWPAN & many more.
- It provides a framework & the lower layers (physical & MAC) in the OSI model for low cash, low power wireless connectivity networks (PAN).
- Low power is one of the key elements of 802.15.4 as it is used in many area where remote sensors need to operate on battery power, possibly for years without attention.
- used for Low power, Low cost & Low speed communication between devices (Device distance is 0.75mtr).
- The IEEE standard 802.15.4 is for Low Rate wireless personal Area Network (LR-WPAN)
- LR-WPAN includes Home Automation, Health care monitoring, environmental surveilance, smart cities etc.
- IEEE standard 802.15.4 defines the characteristics of physical & MAC Layer for the wireless communication systems

that does not require high data rate.
- physical layer defines frequency band, transmission power, & modulation scheme of the link.
- MAC defines issues such as ~~mod~~ medium access & flow control (frames)
- IEEE 802.15.4 utilizes Direct sequence spread spectrum (DSSS) coding scheme to transmit information.
- DSSS uses phase shift keying modulation to encode information.

BPSK - 868/915 MHZ data transmission rate 20/40 KBps respectively

OQPSK - 2.4 GHZ, data transmission rate 250 Kbps.

- DSSS scheme makes the standard highly tolerant to noise & interference & thereby improving link reliability.
- The preferable nature of Transmission is line of sight (LOS).
- The standard range of Transmission is 10 to 75 mtre.
- The transmission of data uses CSMA-CA scheme. (carrier sense multiple access with collision avoidance)
- Transmission occur in infrequent short packets for duty cycle (< 1%), thus reducing consumption of power.
- Two topologies are used. ① star network topology. ② peer to peer network topology.



[Star Topology]

[peer To peer Topology]

6 LOWPAN [IPV6 over Low power Wireless personal Area Network] :-

- It combines the latest version of the Internet protocol (IPV6) and Low power wireless personal Area Networks.
- Therefore 6 LowPAN allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol IPV6.
- 6LowPAN is low cost, short range, Low memory usage, Low bit rate & comprises of edge router & sensor nodes.
- Using 6 LowPAN, the smallest of the IOT device can now be part of the network & can talk to the outside world. (Ex: LED street lights almost zero power)
- 6LowPAN Technology is nothing but a simple wireless mesh Technology that makes the individual nodes IP enabled.

- Edge router is the core of 6LOWPAN network that link 6LOWPAN network to the other IP internet. It is responsible for routing 6LOWPAN packet to the IPV6 packet and assigning IPV6 prefixes in the 6LOWPAN network.
- 6LOWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi.
- 6LOWPAN uses AES-128 link layer security which is defined in IEEE 802.15.4 and this provides link authentication & encryption. (Advance Encryption standard)
- Basic requirements for 6LOWPAN are:-
  (i) The device must have sleep mode in order to support battery saving.
  (ii) Minimal memory requirements.
  (iii) Routing overhead should be lower.

Features:- (i) It is used with IEEE 802.15.4 in 2.4 GHZ band.
(ii) outdoor range : ~ 200 meters (maximum)
(iii) Data rate : 250Kbps (maximum)
(iv) Maximum nodes : ~ 100

Advantages of 6LOWPAN:-
(i) It is a mesh network which is robust, scalable & self healing.
(ii) It delivers low cost & secure communication in IOT devices.
(iii) It uses IPV6 protocol & hence can be routed directly to cloud platforms.

(iv) It offers one to many & many to one routing.

(v) Works efficiently with open IP standards like UDP, TCP, CoAP, HTTP, MQTT & Web sockets.

(vi) In this network leaf node can be in sleep mode for a long duration of time.

(vii) It offers large network which can be used by million of devices.

(viii) It offers end to end addressable nodes which don't require any gateway only a router which can connect this network to IP.

Disadvantages :-

① Less secure than zigbee.

② It has less immunity to interference than WiFi (or) Bluetooth devices.

③ It supports short range without mesh topology.

Applications :- ① used in Home Automation (Lighting). (ii) used in smart Agriculture.

(iii) Industrial monitoring.

(iv) Smart meters & smart grid are the most popular applications for the 6LoWPAN technology.

ZigBee & its Types :-

- It is created by the ZigBee Alliance.
- ZigBee is a wireless Technology developed as an open global standard to address the unique needs of Low cost, Low power wireless IOT networks (such as for home automation, medical device data collection etc)
- It is based on IEEE 802.15.4 standard that defines the physical (PHY) and medium Access control (MAC) Layer for ZigBee.
- It is simpler and less expensive than other wireless personal Area Networks (WPAN) such as Bluetooth, or WiFi.
- operates in unlicensed bands including 2.4GHZ, 915MHZ & 868MHZ.
- It is used in Low data rate applications that require Long battery Life & secure networking.
- Applications of ZigBee are in Wireless light switches, home energy monitors, Traffic management systems & other consumer & industrial equipment that requires short range, Low rate wireless data transfer.
- ZigBee has a shorter range of about 10 To 20mtr indoors because it uses less power & this increases battery Life for ZigBee devices. Maximum outdoore range ~ 500mtr.

maximum data rate ~ 250 Kbps.

- Zigbee supports a wide range of network topologies. (1) star (2) peer to peer (3) cluster free
- Zigbee specifies 3 different device types :-
  (1) zigBee coordinator. (2) ZigBee Router/ Full Function Device. (3) ZigBee End device/ Reduced Function Device.

Zigbee coordinator Node :-

- A ZigBee network has exactly one ZigBee coordinator device.
- It is able to store information about the network.
- It controls the network & it is the central node in star Topology, the root in a tree (or) cluster topology & may be located anywhere in peer to peer network.
- The coordinator serves as the centre point of network, where we can set permission.
- ZCs & ZRs have a higher power requirement than ZEDs. ZCs & ZRs can not be battery powered.

Zigbee Router & Full Function Device :-

- It is an intermediatory router transmitting data from other devices.
- It needs less memory than ZC node.
- It has lesser manufacturing cost.
- It can operate on all topologies.

- It can also act as a coordinator.
- It repeat the network signals.

ZigBee End Device / Reduced Function Device :-

- It is cheaper than ZigBee Router.
- It has lesser memory.
- It has lower power requirement & achieves a long life-time on batteries.
- ZEDs communicate only with their ZR.
- ZEDs are off most of time, thus they are not able to receive any traffic sent to them.
- Instead ZEDs periodically wakeup & check for messages at the ZR with which they are associated.
- The ZR buffers data sent to their ZED nodes & sends those data whenever they get a poll request from a ZED.
- The ZED transmits data to the ZR at any time, since ZR is always awake.
- The number of ZEDs associated with a ZR is limited.
- Mesh networking also means 'self healing networks' because they are multiple routers.
- With a standard WiFi network, if router goes offline all devices also go offline.
- ZigBee protocols automatically close the gap & 'self-heal' so devices continue to perform.

- As long as another routing device remains with in range, network will simply reroute & stay up.

- Advantages of ZigBee:-
  - It is easy to install & implement.
  - It has a very low cost, long battery life & low power consumption.
  - It supports large number of nodes (~6500).
  - It is more reliable & self healing.

Disadvantages:-
- It has low data transmission rate.
- It is not secure like Wifi based secured system.
- ZigBee network requires additional devices which increase cost.
- Appliances running ZigBee are incompatible with other network protocols such as Wifi.
- It lacks Internet protocol support.

- ZigBee & 6LoWPAN protocols are widely used for low power wireless sensor network that are being deployed in factories for monitoring the states of their devices & the environment.

Difference between 6LoWPAN & ZigBee

6LoWPAN	ZigBee
- 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on IP network like WiFi (or) Ethernet with a simple bridge device.	- ZigBee devices can not easily communicate with other protocols. Bridging between ZigBee & non ZigBee networks requires a more complex application layer gateway.
- 6LoWPAN protocol is an adaption layer allowing to transport IPV6 packets over 802.15.4 links.	- ZigBee network layer uses IEEE 802.15.4 address.
- Nearest competitor is ZigBee.	- ZigBee is the most popular, Low cost, Low power, wireless mesh networking standard on the market right now.
- The servers can collect data directly from the end devices.	- Coordinators are used which must perform application Layer protocol translations & send data to servers.
- No need of coordinators nodes directly communicate with their IP address & hence more reliable.	- If coordinators fail, the ZigBee network can not communicate with the internet.
- Data Transmission is very fast.	- Data transmission is very slow.
- Overall security in 6LoWPAN is a work in progress.	- ZigBee has a more robust & tested security protocol.
- 6LoWPAN communicates better with other protocols compared to ZigBee.	

RFID (Radio Frequency Identification) :-

- RFID is a form of wireless communication that uses radio waves to identify & track objects (like books, vehicles, money etc)
- RFID uses electromagnetic fields to automatically identify & track tags attached to objects.
- RFID can also be used to track animals & birds by implanting RFID tags into them.
- RFID tags contains electronically stored information.

Applications of RFID :-

(1) RFID tags are used in many industries. RFID tag attached to an automobile during production can be used to track its progress through the assembly line.

(2) people Tracking :- Hospital uses RFID tags for tracking their special patients. using RFID Technology, in emergency patient & other essential equipment can easily track.

(3) Animals :- RFID can be useful to track the movement & health of animals on a farm.

(4) security (Jewellery Tracking) :- With item level tagging of jewellery with RFID, it is possible to track the jewellery from factory to the distribution centres & then to the store.

(5) Library systems :- using RFID tags in books, librarian can scan it from multiple angles, which makes the issue & submission of books faster than of a barcode which requires proper positioning & line of sight.

(6) Inventory management (monitoring, controlling storing & using the materials for the sell of a product) :- several RFID tag items can be scanned at a time. So this property of RFID help to speed up the inventory management process & reduces human errors, thus providing highly accurate inventory records.

(7) Laundry Automation :- In large companies where they have a huge number of employee uniforms, RFID can be useful in creating a laundary management system. It can track the uniforms that were assigned to an employee, the number of times it was washed, age of uniforms & identifies the missing uniform.

(8) Document Tracking :- RFID enables high speed identification of documents, track & track of documents.

(9) Defense :- RFID can be used for tracking weapon movement & soldiers movement tracking.

(10) RFID tag used in electronic toll collection at highways.

Basic components of a RFID system :-

(1) RFID Reader (2) RFID Tag (3) Antenna (4) Software.

(1) RFID Tags :-

- RFID tag contains a microchip that is encoded with information about the object being tagged.
- RFID tag is a transponder which receives a radio signal & in response to it sends out a radio signal.
- It consists of an antenna (used to transmit & receive signals) & a small chip that stores a small amount of data & process the information.
- There are Two types of tags. passive & Active tags

(1) passive Tag :-

↳ Most common type of tag.
↳ Do not operate with batteries.
→ passive tags get power from a reader.
↳ Readers send electromagnetic waves that produce a current in the tags antenna which then powers the microchips circuits.

↳ Less expensive.
↳ passive tags read range is approximately 30 feets.

(ii) Active Tags:-

↳ Highly expensive than the passive Tags.
↳ It operate with a battery, hence it has higher range & efficiency.
↳ Data Transmission rate is high.
↳ Allow a read range of about 100 feet.
↳ useful in location Tracking applications.

(2) RFID Reader/Interrogator:-

↳ It consists of an interrogatore (Two way radio transmitted receiver, also known as a Transceiver)
↳ Transceiver is used to transmit an encoded signal that activates the tag.
↳ It collect data from RFID tags.
↳ The readere has a scanning antenna that emits radio waves & the tag responds by sending back its data.
It has a transceiver with a decodere to intereupt the data.

↳ Readers —
→ Fixed Readers - Mounted in specific locations & are used to track items as they move from one place to another. works without human Involvement.
→ Mobile Reader - Hand held. use to scan individual items (or) a pallet of items on the go.

- Flexible.
- use in retail environment

③ Antennas :- RFID tags & readers both have antennas that allow them to communicate with each other.

④ Software :- To process the data & running of the device, Three different types of softwares are used in RFID.

(i) Firmware :- It is the software that resides on the RFID hardware itself.
It is responsible for running the device.

(ii) Application software :- It use RFID collected data to address a particular business need.
↳ It can be anything from an inventory management software application to an employee time & attendance application.

(iii) Middleware :- It is the software between firmware & application.
→ It gathers raw RFID data & serves as a vehicle for sharing this data with application software.
→ It offer the ability to control & monitor RFID hardware & overall system health.

→ It is a communication link between RFID components & applications.

Advantages of RFID Technology:-

(i) RFID tags are very simple to install/inject inside the body of animals, thus helping to keep a track on them.

(ii) The RFID tags can store data up to 2 KB.

(iii) It cannot be easily replicated & therefore it increases the security of the product.

(iv) It is non contact, non line of sight nature of the technology.

(v) Hundred of tags can be read in seconds.

Disadvantages:-

(1) It is difficult for an RFID reader to read the information incase of RFID tags installed in liquids & metal products.

(2) Expensive than barcode system.

(3) Impacted by environmental factor and hardware interference.

(4) Not totally secured can be hacked or bypassed by hackers.

Near Field communication (NFC) :-

- NFC is the technology driving the adaption of the IOT.
- RFID helps at tracking inventory before the sale, while NFC is aimed at becoming part of a product's utility after the sale.
- NFC tags are small, inexpensive & embedded in to products at the item level for use by consumers.
- NFC operates at a shorter distance, provide secure communication and allows for bidirectional communication (peer to peer)
- NFC - enabled devices can be reader or cards.

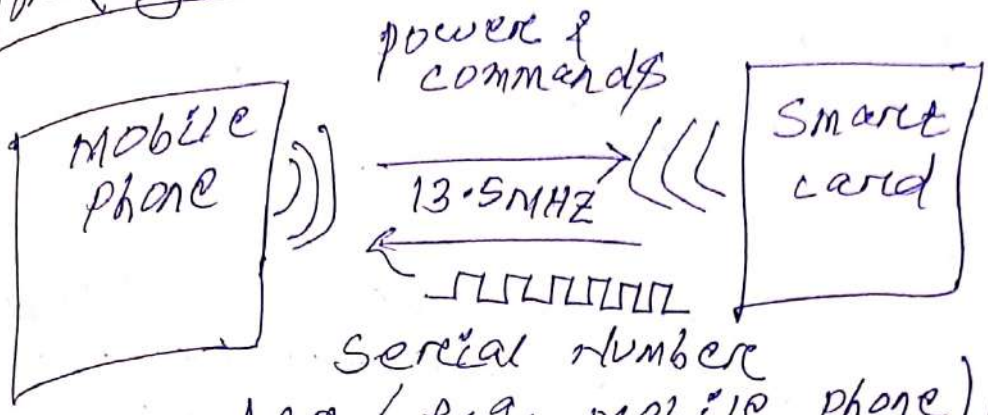
For example:- When we use NFC to exchange information between two smartphones, the first smartphone begin by acting as a reader and the second acts as a card.

After the initial information exchange, they reverse roles. Now the first smartphone is a card and the second smartphone is a reader.

But NFC tags can't act as readers. They are passive (no power source) so they always act as information sources.

NFC enabled device sends power & commands to the tag, which then responds with data.

Working :-



NFC reader (e.g. mobile phone) provides power, initiates radio frequency communications & captures data from the tag (or program data into the tag)

- NFC enabled device (like smartphone) can be used to write data to a tag using a special commands. That means NFC tags can be updated when needed to hold new information.

In peer to peer node, it is possible to transfer information between two NFC devices.

NFC systems operate on the same frequency as HF RFID (13.5 MHZ) systems. Therefore there are only short read range limitations. So, devices have to be in very close proximity (usually no more than a few centimeter). Therefore it has become a

popular choice for secure communication between consumer devices such as smartphones.

- As NFC device is able to act both as a reader & as a tag. NFC is a popular choice for contactless payment so, mobile industry including NFC in newer smartphones.
- NFC builds upon the standards of the HF RFID and turns the limitations of its operating frequency into a unique feature of NFC.

Advantages of NFC

1. Data exchange between two mobiles.
2. Health care.
3. contactless payment.
4. Transport cards.
5. Ticketing.
6. IOT
7. Access control
8. parking access management.

NFC integrated smart cards can be used for fast payments & at grocery shops, parking tickets, adding shopping points,

- Service providers can integrate payment option into smartphones using as NFC tag embedded in to the device.

Apple pay, Google Wallet & Samsung pay are the most popular among smartphone payment systems.

Attendance Tracking - NFC tags are frequently used in ID cards & badges for attendance tracking & record keeping.

Wireless pairing :- NFC Tags can be used to allow for quick pairing between a Bluetooth device (with an NFC Tag) & an NFC capable Bluetooth device, such as Andreoid phone.

—x—x—

RFID	NFC
- It stands for Radio Frequency Identification.	- It stands for Near Field communication.
- RFID is a wireless Technology mainly used to transfere data, identify & track automatically a tag attached to an object.	- NFC is a short range high frequency wireless Technology that enables devices & smartphones to establish a communication with each othere by touching them togethere or bring them in to proximity.
- RFID operate at 3 frequencies. LF - (125 TO 134 KHZ) HF - (13.56 MHZ) UHF - 856 MHZ TO 960 MHZ	- NFC is a branch of High Frequency HF(RFID) operate at 13.6 MHZ frequency.

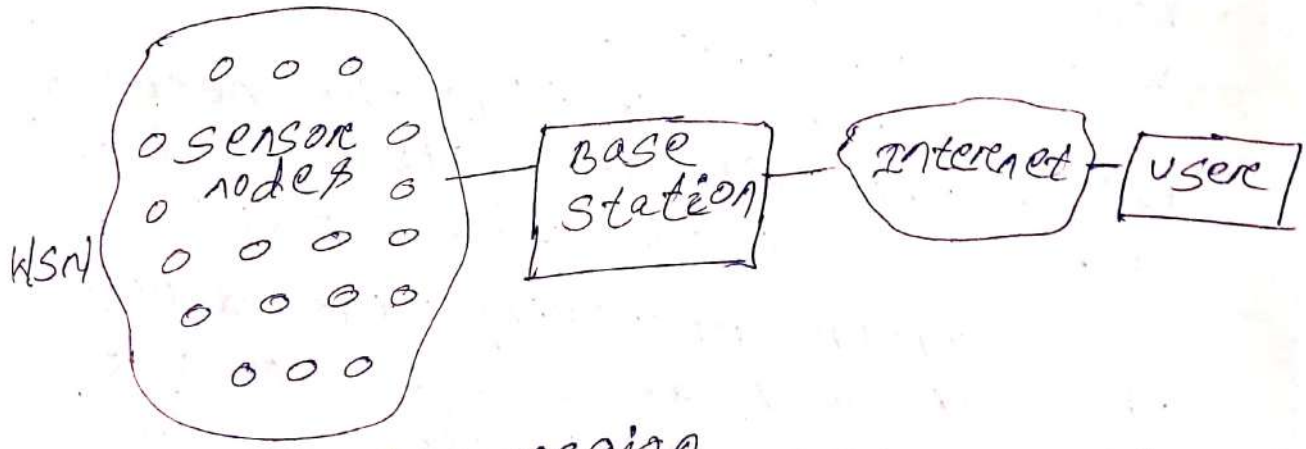
- RFID have separate RFID reader & RFID tags.	- NFC device is capable of being both an NFC reader & an NFC Tag.
- RFID Tags can be active, passive.	- NFC Tags are passive in nature.
- RFID tags are used for tracking wild animals by placing the tags inside their body. This reduce risk of putting human life in danger. commonly used in asset tracking.	- NFC tags is used for automating task in your smartphone, mobile payment, sharing data quickly.
- Multiple RFID tags can be scanned at a time from RFID reader.	- only one NFC tag can be scanned at a time.
- RFID Technology need both RFID reader & RFID tags Infrastructure.	- Most moderen mobile devices are now NFC enabled & can be used as mobile reader device, so no extra reader infrastructure is necessary.

—x—x—x—

Wireless sensor Network and Its Applications :-

- A Wireless sensor network (WSN) is a wireless network consisting of Large number of heterogeneous sensor node devices spread over a large field to monitor physical (or) environmental conditions such as Temperature, Sound, vibration, pressure etc.

- A WSN is a network of many tiny disposable lower power devices (nodes) that communicate through wireless channels for information sharing.
- A wireless sensor network consists of 3 major elements :-
  1. sensor unit :- used to take measurement.
  2. computing unit :- used to process data.
  3. communication unit :- It is used to enable communication among the wireless nodes.
- In wireless sensor network (WSN) different radio technologies can be used for communication such as ZigBee, WiFi, Bluetooth etc.



- In WSN a large number of sensor nodes are deployed in a large area to cooperatively monitor a physical environment.
- Sensor node consists of not only the sensing component but also other important

features like processing, communication & storage units. sensor node is responsible for physical world data collection, network analysis, data correlation & fusion of data from other sensor with its own data.

- A sensor node in WSN not only communicate with other sensor nodes but also with a base station using wireless communication.

<u>Base station</u>:- A base station acts as a processing unit in WSN.

A base station also acts as a gateway to other networks through the Internet.

The BS sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other.

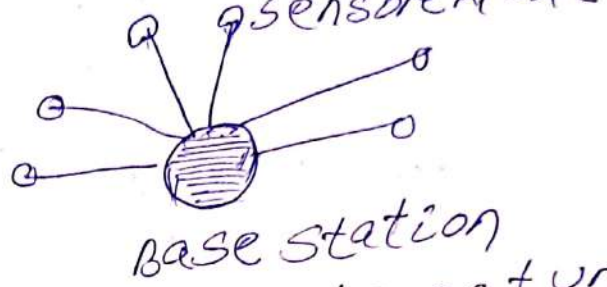
After collecting the necessary data, the sensor nodes send the data back to the base station.

After receiving the data from the sensor nodes, a BS performs simple data processing & sends the updated information to the user using Internet.

There are different ways of communication in WSNs, designed based on the energy conservation of the sensors.

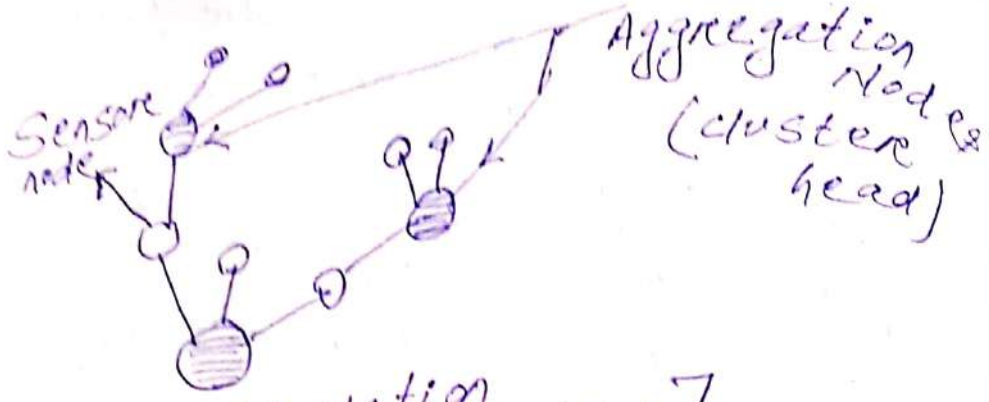
① single hop network Architecture:-

- All sensores send information collected directly to the Base station.
- The easy way of establishing single hop WSN makes them the most commonly used & widely known type.



② Multi hop network Architecture:-

- For long distance Transmission, multihop network architecture is used.
- Here the energy consumption for communication will be significantly higher than data collection & computation.
- Base station (BS) is located at higher distance from the nodes.
- Here the data of sensor node is transmitted through one (or) more intermediate node.
- sensores send the data to a aggregation node & then those nodes collect the information & finally send them to the Base station.



[Multihop communication]

Multihop Architecture

- Flat Network Architecture
- Hierarchial Network Architecture

Flat network architecture of WSNs :-

- The BS sends commands to all the sensor nodes but the sensor with matching query will respond using its peer nodes via a multi-hop path.

Hierarchial network architecture of WSNs :-

- A group of sensor nodes are formed as a cluster & the sensor nodes transmit data to the corresponding cluster heads & the cluster heads can then relay the data to the BS.

- WSN is sometimes referred to as a subset of IOT.

IOT = WSN + Internet + cloud storage + mobile/web application

- WSNs are not necessarily connected to the Internet & only sensors are information gathering devices. while, in IOT things are always connected to the Internet & things may be sensors, humans, cameras, PCs & phones that upload their data to the Internet so other users may use them.

Advantages of WSNs :-

① It avoids lot of wiring.
② It can accomodate new devices at any time.
③ It is flexible to go through physical partitions.
④ It can be accessed through a centralized monitor.

Disadvantages :-

① Lower speed as compared to wired network.
② Less secure, hackers can easily hack the network.
③ More complex to configure than wired network.
④ Gets distracted by various wireless elements like Bluetooth.

Applications of Wireless sensore network :- (WSN)

① Military surveillance & Target tracking :-

WSNs can be rapidly deployed for surveillance & used to provide battle field intelligence regarding the locations, numbers, movement, & identity of troops & vehicles, & for detection of chemical, biological & nuclear weapons.

② Environmental Monitoring :-

Environmental monitoring can be used for animal Tracking, forest surveillance, flood detection & Weather forecasting. Some of the major areas where WSNs are used are as follows :-

(i) Forest fire detection.
(ii) Air pollution monitoring.
(iii) Land slide detection.
(iv) Water quality Monitoring.
(v) Natural disastere prevention.

③ Health Monitoring :- WSNs can be embedded in to a hospital building to track & monitor patients & all medical resources.

There are various kinds of sensors which can measure blood pressure, body Temperature & ECG.

BSN (Body sensor network) is a special kind of sensor network formed when the sensors are implemented for health care purposes. It helps continuous & ambulatory heath monitoring with real time update of medical records via the Internet.

④ Traffic control :-

WSNs can be used for vehicle traffic monitoring & control. WSNs will completely change the Landscape of traffic monitoring & control by installing cheap sensor nodes in the car, at the parking lots, along the roadside streetline is a company which uses sensor network topology to help drivers find unoccupied parking places & avoid traffic.

⑤ Industrial Monitoring :-

WSNs make it economically feasible to monitor the health of machines & to ensure safe operation by embedding sensor nodes in to machines.

Monitoring corrosion using manual processes is extremely costly, time consuming & unreliable. A network of wireless corrosion sensors can be economically

deployed to reliably identify issues before they become catastrophic failures.

— x — x —

Difference between Zigbee, 6LoWPAN, WiFi & Bluetooth :-

	Zigbee	6LoWPAN	WiFi	Bluetooth
① IEEE specification :-	802.15.4	802.15.4	802.11a/b/g	802.15.1
② Maximum signal rate :-	250 Kb/s	200 Kb/s	54 Mb/s	1 Mb/s
③ Range :-	10-100 mtr (~500)	~200 m	50-100 mtr	1 to 10 mtr
④ Networking Topology :-	Adhoc, peer To peer, star or mesh	star, mesh, P2P	star, Tree, point to hub P2P	Adhoc, star very small Network
⑤ security :-	128 AES plus application layer security (middle)	128 bits AES.	RC4 stream & AES block cipher. (Low)	64 & 128 bit encryption (High)
⑥ operating frequency :-	868 MHZ, 915 MHZ, 2.4 GHZ	2.4 GHZ	2.4 GHZ & 5 GHZ	AES block cipher 2.4 GHZ
⑦ power consumption :-	very Low	Low	High	medium
⑧ Maximum Nodes per Network :-	65,536	~100	30	8

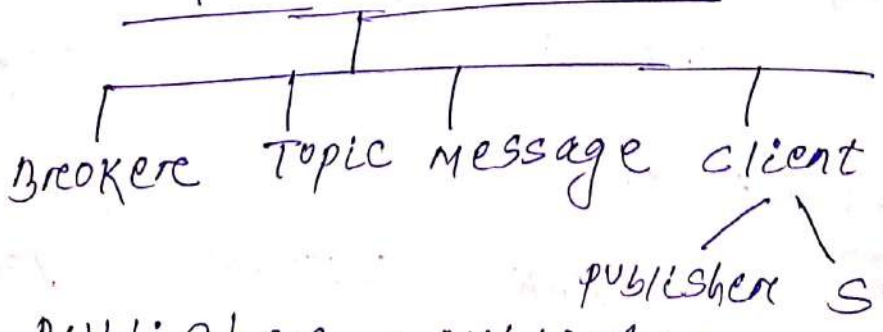
(9) Data protection :-	16 bit CRC	16 bit CRC	32 bit CRC	16 bit CRC
(10) Key characteristics :-	stability, Low power consumption, Low cost	same as ZigBee	very High speed, Large network	Low price, easy use, High data rate.
(11) Application :-	Industrial control & monitoring, sensor networks, Building Automation	same as ZigBee	Broadband Internet access, Wireless LAN connectivity	cable replacement & Wireless connectivity between devices such as phone, PDA, Laptops.
(12) Main applications :-	Monitoring & control	such as ZigBee	Data Transmission	Data & voice Transmission.
(13) Access protocol :-	CSMA/CA	CSMA/CA	CSMA/CA	OFDMA MC-CDMA
(14) packet Length :-	127 bytes	127 bytes	up to 1048575 bytes	10 to 265 bytes
(15) power consumption :-	< 10 mW	< 10mW	> 100 mW	< 10mW

— Y —

MQTT :-

- It stands for Message Queuing Telemetry Transport.
- It is a machine to machine (M2M) or IOT connectivity protocol.
- It is a publish subscribe based messaging protocol that transport messages between devices.
- It usually runs over TCP/IP protocol.
- It is very light weight and thus suited for M2M (Mobile To Mobile) WSN (wireless sensor N/ws) and IOT scenarios where sender nodes communicate with applications through the MQTT message broker.
- MQTT was initially developed by IBM & Eurotech.
- It is designed for limited devices & networks with high latency & low bandwidth.

MQTT components



Publisher – publishes messages.
Subscriber – Receives messages that are intended for it.

publish – It is the process a device does to send its message to the broker.

subscribe – It is the process where a device does to retrieve a message from the broker.

MQTT Broker :-

- It is a central point of communication.
- It is responsible for dispatching all messages between the clients.
- It receives subscriptions from clients on topics.
- It receives messages from clients & forward these messages based on client's subscriptions to interested clients.

MQTT client :-

- MQTT client is any device (Example :- a computer, or a mobile phone) that connects to the broker.
- A client that sends messages is a publisher.
- A client that receives messages is a subscriber.
- To receive a message, the client must subscribe to the topic of that message.

Topics :- - A Topic is an identifier used by MQTT broker to identify rightful clients for delivering messages.

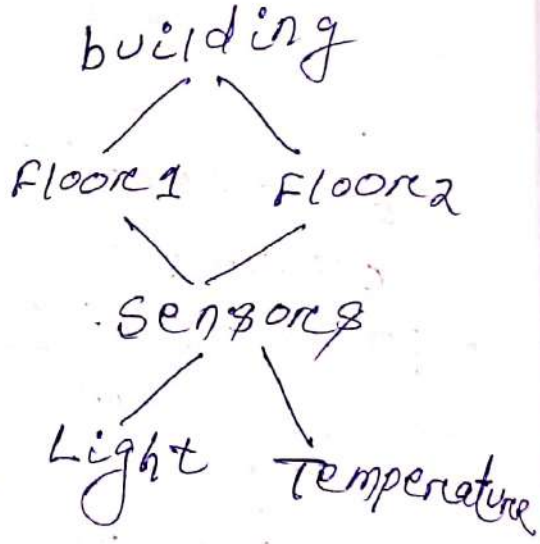
- Each client that wants to send messages publishes them on a certain topics.
- Each client that wants to receive messages subscribes to a certain topic.
- Topics are case sensitive.

A Topic is a string & can consist of one (or) more topic levels and each level is separated by a forward slash (/).

Example :-

building/Floor1/sensors/Temperature

building/Floor2/sensors/Temperature



building/+/sensors

building/Floor-1/# → matches all nodes under building/Floor2

+ → single level wildcard

→ multi level wildcard

topic

house/+/temperature — subscriber will receive msgs.
- house/Livingroom/Temperature
- house/bedroom/Temperature

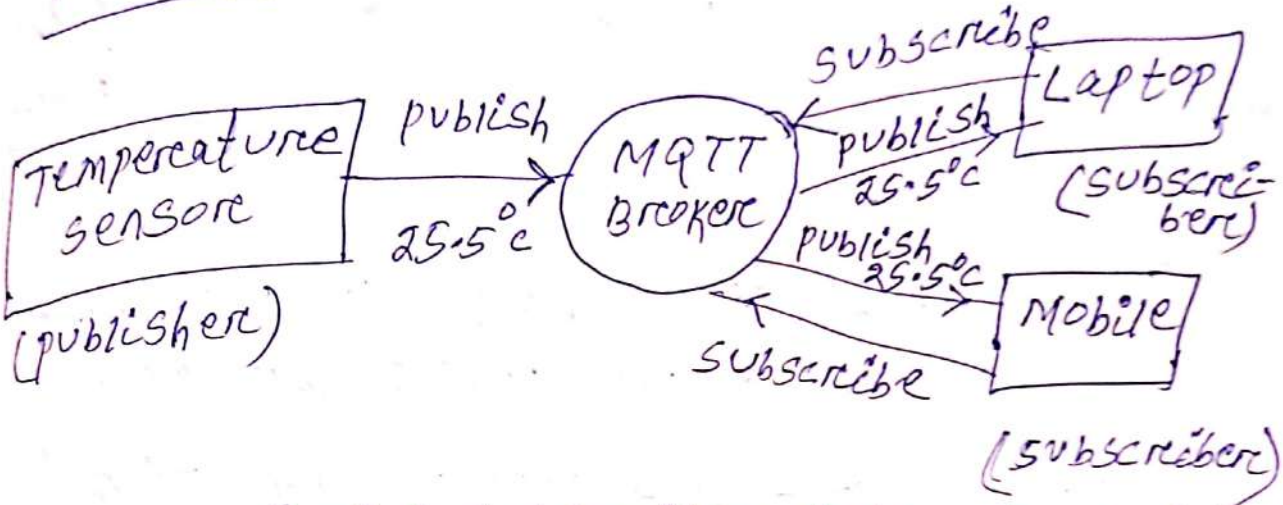
house/# → subscriber is subscribing to all topics begins with house.

Applications :-

① Home Automation ② Factory Automation

③ Medical & Healthcare.

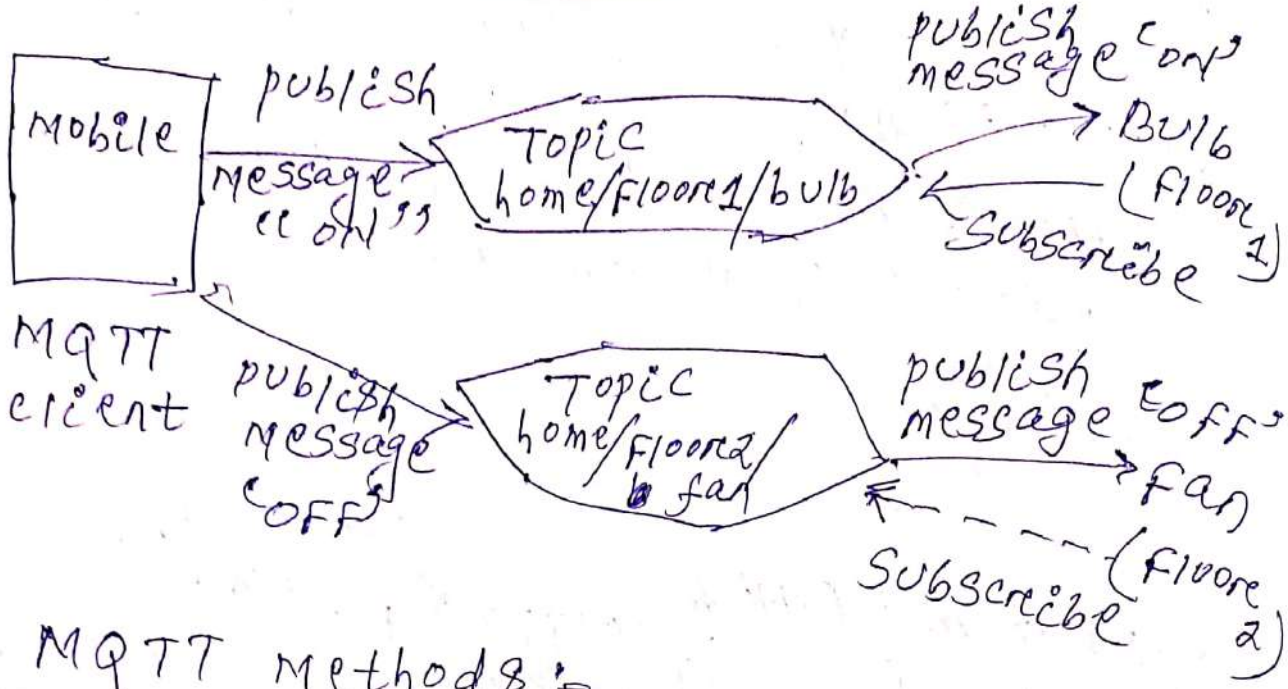
Working :-



① First of all a subscriber subscribes to one (or) more Topics. In above figure the Laptop & the Mobile device are the subscribers.

② The Temperature sensor is the publisher. Then one or more publishers publish message to ~~several~~ a server (MQTT Broker) (Local or remote) The Temperature sensor publishes it temperature value to the broker.

③ Then the server publishes the message to the subscribers which have subscribed to the topic specified by the publisher in above figure, broker publishes the Temperature value to the Laptop & mobile device.



MQTT Methods :-

① connect - client request a connection with the MQTT broker.

② disconnect - disconnect connection/notifications

③ subscribe :- subscribe to topics

④ unsubscribe :- unsubscribe from topics.

⑤ publish :- publish message.

Advantages of MQTT :-

① Its small size, low power usage, minimized data packet and easy of implementation make the protocol ideal of M2M (or) IOT world.

② It is a lightweight protocol. So it is easy to implement in software and fast in data transmission.

(3) Low network usage because of minimized data packet.
(4) Low power usage saves the connected device's battery.

Applications:- (1) Home Automation (2) Factory Automation (3) Medical & Healthcare (4) Transport & Logistics.

—x—x—

SMQTT [Secure Message Queue Telemetry Transport] :-

- SMQTT is proposed only to enhance MQTT security feature.
- It is extension to simple message queue Telemetry Transport protocol.
- It uses encryption based on Lightweight attribute based encryption.
- The main advantage of attribute based encryption is, it uses the broadcast encryption function. In this function, the message is encrypted and transmitted to several nodes that are quite common in IOT applications.
- The process of message Transfer & receiving consists of 4 major stages:-

(1) Setup :- In this phase, the publishers & subscribers registers themselves to the broker and get a secret master key.

② Encryption :- When the data is published to broker, it is encrypted by broker.

③ publish :- The broker publishes the encrypted message to the subscribers.

④ Decryption :- Finally the received message is decrypted by subscribers with the same master key.

key generation and encryption algorithms depends on developers (are not standardized)

—— x —— x ——

COAP [constrained Application protocol] :-

- It is an IOT protocol.
- It is designed to allow single and small devices to join the IOT through low bandwidth restricted network.
- The protocol is designed for M2M & IOT applications such as smart energy and building automation.
- It is an application layer protocol follows the request response pattern/model.
- COAP runs over UDP protocol.

- It also uses Restful Architecture.
- It uses less resources than HTTP.
- In CoAP client can use GET, PUT, DELETE methods during request.

CoAP Layers :-

Mostly it is divided in to 2 Layers.

Application
Request/ Response
Messages
UDP

① upper Layer (Request & Response) - It concerns communication method & deal with request/response method.

② Lower Layer (Message) - It has been designed to deal with UDP and asynchronous messages.

Message Types :-

CoAP supports 4 different message types.

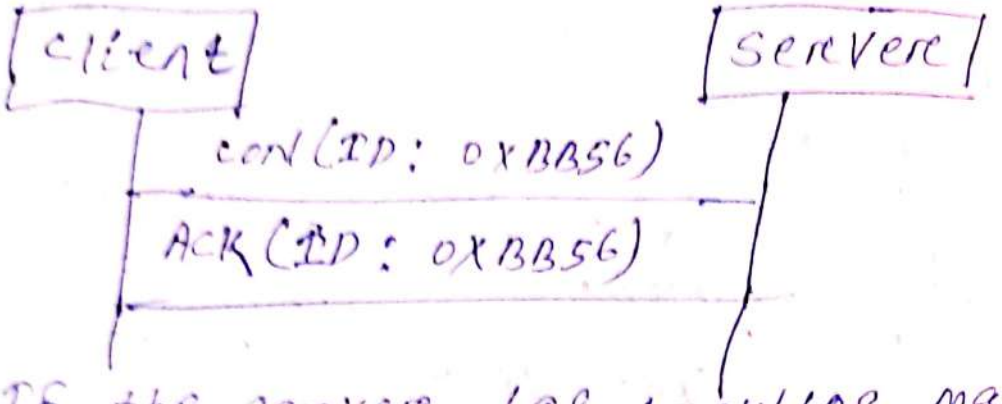
① confiremable ② Non confiremable
③ Acknowledgement ④ Reset.

① Con/confiremable message (Reliable message) :-

A confiremable message requires a response, either a positive acknowledgement (or) a negative acknowledgement.

Incase acknowledgement is not received retransmission are made until all attempts are exhausted.

The Acknowledgement message contain the same ID of the confirmable message (con).

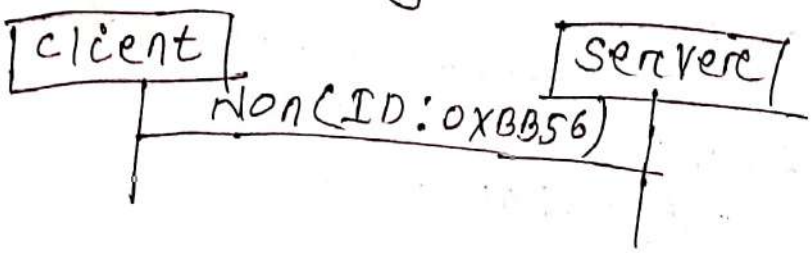


- If the server has troubles managing the incoming request, it can send back a Reset message (RST) instead of Acknowledge message (ACK)

② Non confirmable message (NON) :-

A Non confirmable request is used for unreliable transmission. These are messages that don't require an acknowledgement by the server. messages do not contain critical information that must be delivered to the server. Like a request for a server measurement made in periodic basis. Even if one value is missed, there is not too much impact.

Even if these messages are unreliable, they have a unique ID.



③ ACK/Acknowledgement :- It is sent to acknowledge a confirmable (con) message.

④ RST/Reset :- It represents a negative acknowledgement and means 'reset'. It generally indicates some kind of failure (like unable to parse received data.)

Domain Specific IOTs

① Home Automation

Smart Lighting :- Smart Lighting for homes helps in saving energy by adapting the lighting to the ambient conditions and switching on/OFF or dimming the lights when needed.

- smart lighting solutions for home achieve energy savings by sensing the human movements and their environments and controlling the lights accordingly.

Smart Appliances :- Smart Appliances make the management easier and also provide status information to the users remotely.

Example :- ① Smart washer/dryer can be controlled remotely and notify when the washing/drying is complete.

② Smart Refrigerators can keep track of the items store and send updates to the users when an item is low on stock.

Intrusion Detection :-

- Home intrusion detection systems use security cameras and sensors to detect intrusion and raise alerts.
- Alerts can be in the form of an SMS (or) an email sent to the user.
- Advanced systems can even send detailed alerts such as an image grab (or) short video clip.

Smoke/Gas detectors :-

- These are installed in home and buildings to detect smoke that is typically an early sign of fire.
- It uses optical detection, ionization (or) air sampling techniques to detect smoke.
- Gas detector can detect the presence of harmful gases such as CO, LPG etc.
- It can raise alerts in human voice describing where the problem is.

(2) CITIES :-

Smart parking :- It makes the search for parking space easier and convenient for drivers.

- These are powered by IOT systems that detect the no. of empty parking slots and send the information over the Internet to smart parking application ~~the~~ back ends.

Smart Lighting :- It allows lighting to be dynamically controlled remotely to configure lighting schedules and lighting intensity.

- custom lighting configurations can be set of fore different situations such as a foggy day, a festival etc.

- Smart lights are equipped with sensor that can communicate with other lights and exchange information on the sensed ambient conditions to adapt the lighting.

Smart Roads :- It can provide information on driving conditions, travel time estimates and alerts in case of poor driving conditions, traffic congestions and accidents.

- Such information can help in making the roads safere and help in reducing traffic Jams.

Structural Health Monitoring :-

- This system uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.
- The data collected from these sensors is analyzed to access the health of the structures (detecting cracks and mechanical breakdowns), remaining life of the structure.

Surveillance :-

- Surveillance of infrastructure, public Transport and events in cities is required to ensure safety and security.
- City wide surveillance infrastructure comprising of large no. of distributed and internet connected video surveillance cameras can be created.

Emergency response :-

- IOT systems can be used for monitoring the critical infrastructure in cities such as buildings, gas and water pipelines, public Transport and power stations.
- Fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructure.

- such systems can reduce the latency of emergency services for vehicles such as ambulences and police cars while minimizing disruption of regular traffic.

(3) Environment

Weather Monitoring :- This system can collect data from a no. of sensor attached (such as Temperature, humidity, pressure etc) and send the data to cloud based applications and storage back ends.

- The data collected in the cloud can then be analyzed and visualized by cloud based applications.
- Weather alerts can be sent to the subscribed users from such applications.

Air pollution Monitoring :- IOT based air pollution monitoring systems can monitor emission of harmful gases by factories and automobiles using gaseous and meterological sensors.

- The collected data can be analyzed to make informed decisions on pollution control approaches.

Noise pollution Monitoring :- This system uses a no. of noise monitoring stations that are deployed at different places in a city.

- The data on noise levels from the stations is collected on servers (ore) in the cloud.
- The collected data is then aggregated to generate noise maps.
- Noise maps can help the policy makers in urban planning and making policies to control noise levels near residential areas, schools & parks.

Forest Fire detection :-

- Early detection of forest fires can help in minimizing the damage caused by forest fires.
- IOT based forest fire detection systems use a no. of monitoring nodes deployed at different locations in a forest.
- Each monitoring node collects measurements on ambient conditions including temperature, humidity, light levels etc.

River Floods Detection :-

- It can cause extensive damage to the natural and human resources and human life.
- IOT based river flood monitoring system use a no. of sensore nodes that monitore the water level and flow rate.
- Monitoring applications raise alerts when rapid increase in water level & flow rate is detected.

(4) Industry :-

Machine Diagnosis and prognosis :-

Machine prognosis :- predicting the performance of a machine by analyzing the data on the current operating conditions.

Machine Diagnosis :- Determining the cause of a machine fault.

- sensors in machines can monitore the operating conditions such as Temperature and vibration levels.

Indoore Air quality Monitoring :-

- monitoring indoore air quality in factories is important for health and safety of the workers.
- IOT based gas monitoring systems can help in monitoring the indoore air quality using various gas sensors.
- Wireless sensor networks based IOT devices can identify the hazardous zones, so that corrective measures can be taken to ensure propere ventilation.