UNIT- 4 IOT COMMUNICATION AND OPEN PLATFORMS

IoT Communication Models and APIs – IoT Communication Protocols – Bluetooth – WiFi – ZigBee– GPS – GSM modules – Open Platform (like Raspberry Pi) – Architecture – Programming – Interfacing – Accessing GPIO Pins – Sending and Receiving Signals Using GPIO Pins – Connecting to the Cloud.

Communication Models in IoT (Internet of Things)

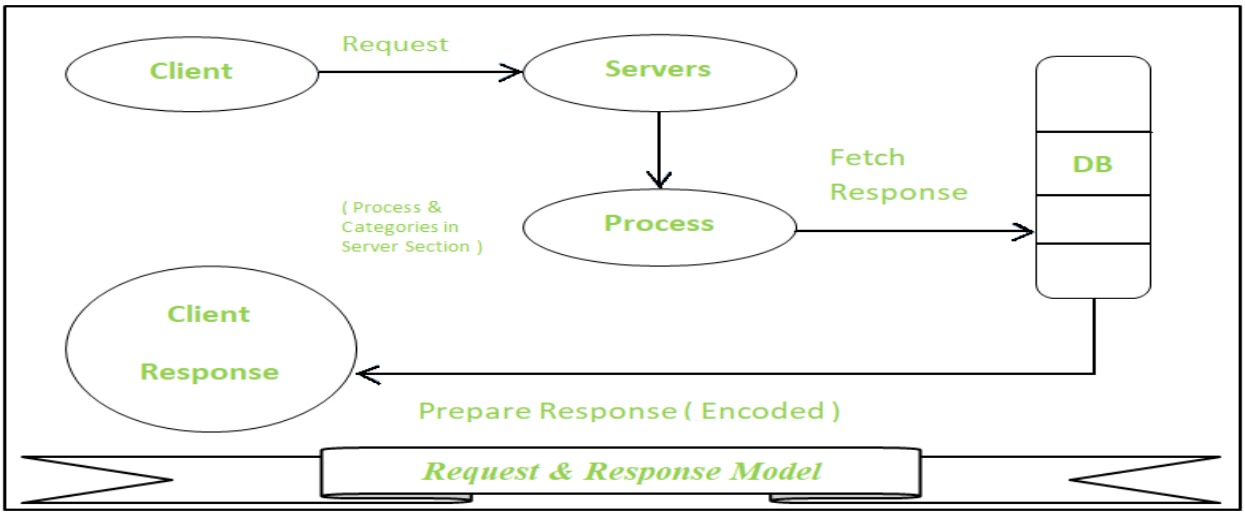
IoT devices are found everywhere and will enable circulatory intelligence in the future. For operational perception, it is important and useful to understand how various IoT devices communicate with each other. Communication models used in IoT have great value. The IoTs allow people and things to be connected any time, any space, with anything and anyone, using any network and any service.

Types of Communication Model :

1.Request & Response Model

This model follows a client-server architecture.

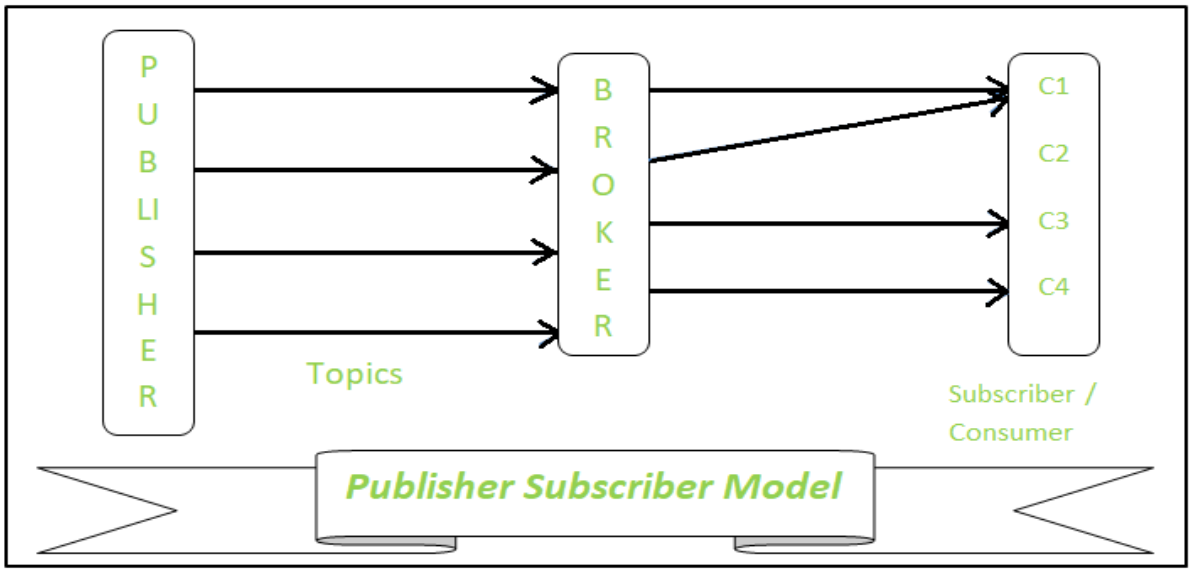
- The **client**, when required, requests the information from the server. This request is usually in the encoded format.
- This model is stateless since the data between the requests is not retained and each request is independently handled.
- The server Categories the request, and fetches the data from the database and its resource representation. This data is converted to response and is transferred in an encoded format to the client. The client, in turn, receives the response.
- On the other hand — In **Request-Response** communication model client sends a request to the server and the server responds to the request. When the server receives the request it decides how to respond, fetches the data retrieves resources, and prepares the response, and sends it to the client.



2. Publisher-Subscriber Model

This model comprises three entities: Publishers, Brokers, and Consumers.

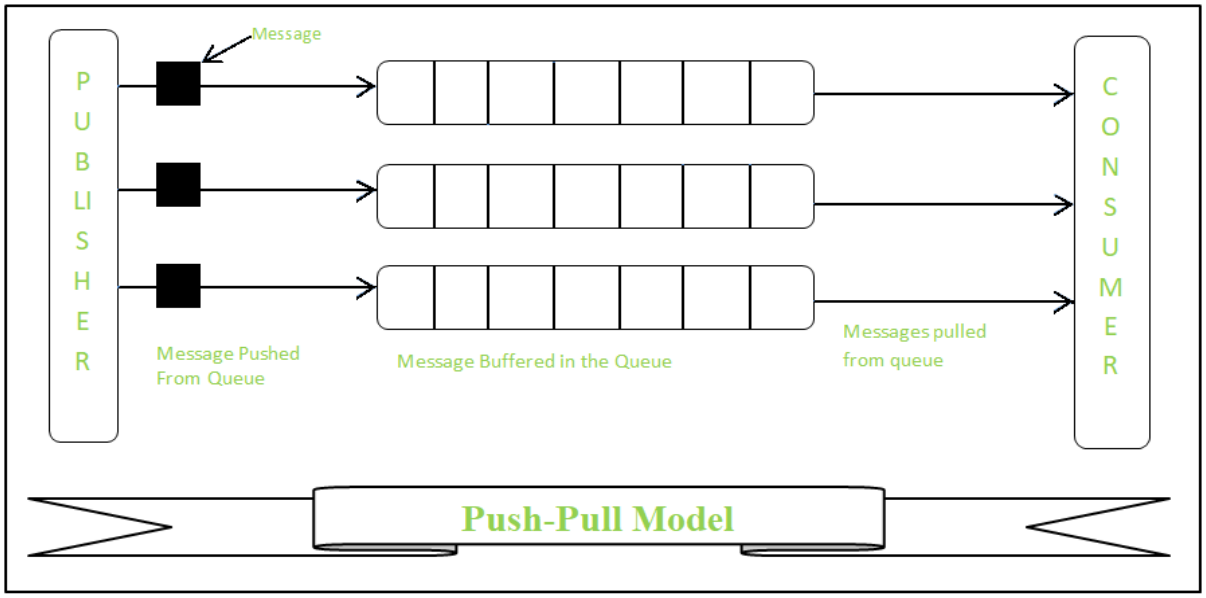
- **Publishers** are the source of data. It sends the data to the topic which are managed by the broker. They are not aware of consumers.
- **Consumers** subscribe to the topics which are managed by the broker.
- Hence, **Brokers** responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.



3. Push-Pull Model

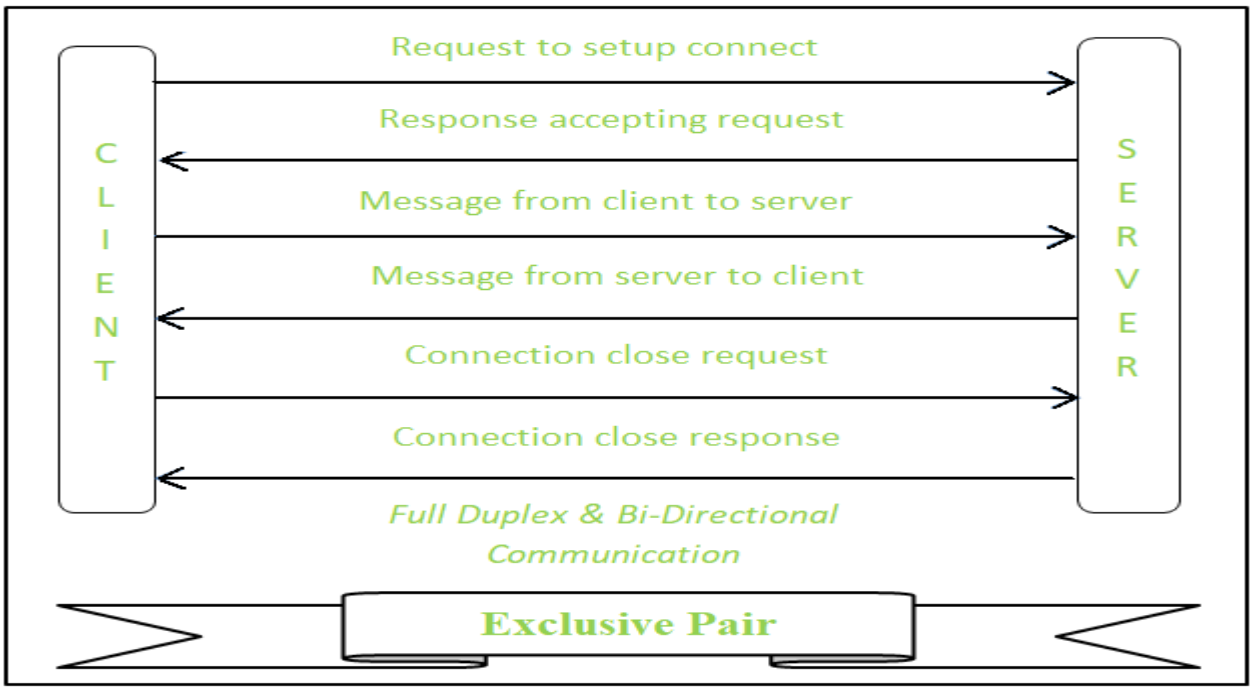
The push-pull model constitutes data publishers, data consumers, and data queues.

- **Publishers** and **Consumers** are not aware of each other.
- Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer.
- **Queues** help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.



4. Exclusive Pair

- **Exclusive Pair** is the bi-directional model, including full-duplex communication among client and server. The connection is constant and remains open till the client sends a request to close the connection.
- The **Server** has the record of all the connections which has been opened.
- This is a state-full connection model and the server is aware of all open connections.
- WebSocket based communication API is fully based on this model.



IoT Communication APIs

Generally we used Two APIs For IoT Communication. These IoT Communication APIs are:

- REST Based Communication APIs
- Web Socket Based Communication APIs

Web service can either be implemented using REST principles or using Web Socket Protocol –

1. REST Based Communication API :

REpresentational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred. REST APIs follow the request-response communication model. The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.

Advantages of REST API:

- Simplicity: REST APIs are relatively simple to design and implement, making them a popular choice for building APIs for web applications.

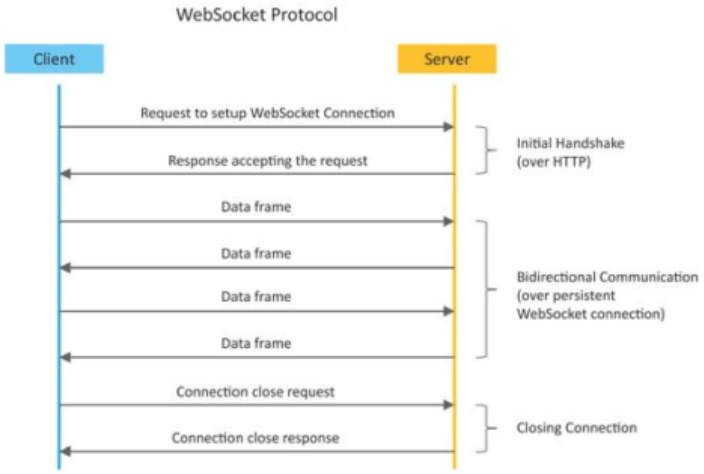
- Flexibility: REST APIs can be used to support a wide range of applications and services, from simple web applications to complex enterprise systems.
- Caching: REST APIs can leverage caching to improve performance and reduce server load.
- Stateless: REST APIs are stateless, meaning that each request is processed independently of any previous requests, making them easy to scale and distribute.

Disadvantages of REST API:

- Limited real-time support: REST APIs do not support real-time communication between the server and client, making them less suitable for applications that require real-time updates.
- Performance overhead: REST APIs require more overhead than WebSocket APIs, as each request and response must contain all the necessary information to complete the request.
- Complexity: REST APIs can be complex to design and implement for large, distributed systems.

2. Web Socket Based Communication APIs :

Web Socket APIs allow bi-directional, full-duplex communication between clients and servers. It follows the exclusive pair communication model. This Communication API does not require a new connection to be set up for each message to be sent between clients and servers. Once the connection is set up the messages can be sent and received continuously without any interruption. WebSocket APIs are suitable for IoT Applications with low latency or high throughput requirements.



Advantages of WebSocket API:

- Real-time communication: WebSocket APIs enable real-time communication between the server and client, making them ideal for applications that require real-time updates.
- Efficiency: WebSocket APIs are more efficient than REST APIs for real-time applications, as they use a persistent connection to enable bidirectional communication.
- Scalability: WebSocket APIs are highly scalable, as they can support thousands of connections per server.
- Reduced overhead: WebSocket APIs have lower overhead than REST APIs, as they use a single connection to transmit data.

Disadvantages of WebSocket API:

- **Complexity**: WebSocket APIs are more complex to design and implement than REST APIs, requiring additional programming skills and knowledge.
- **Security**: WebSocket APIs can be vulnerable to security threats if not properly secured.
- **Compatibility**: WebSocket APIs are not supported by all browsers, requiring fallback mechanisms for older browsers.

Similarities between REST API and WebSocket API:

- Both REST API and WebSocket API are used to build APIs for web applications.
- Both REST API and WebSocket API are standardized interfaces that enable communication between the server and client.
- Both REST API and WebSocket API can be customized to suit the specific needs of a particular application or system.
- Both REST API and WebSocket API can be secured using various authentication and encryption methods.

Difference between Rest API and Web Socket API :

S.NO.	REST API	WEB SOCKET API
1.	It is Stateless protocol. It will not store the data.	It is Stateful protocol. It will store the data.
2.	It is Uni-directional. Only either server or client will communicate.	It is Bi-directional. Messages can be received or sent by both server or client.
3.	It is Request-response model.	It is Full duplex model.
4.	HTTP request contains headers like head section, title section.	It is suitable for real-time applications. It does not have any overhead.
5.	New TCP connection will be set up for each HTTP request.	Only Single TCP connection.
6.	Both horizontal and vertical scaling (we can add many resources and number of users both horizontally and vertically).	Only vertical scaling (we can add resources only vertically).
7.	It depends upon the HTTP methods to retrieve the data..	It depends upon the IP address and port number to retrieve the data
8.	It is slower than web socket regarding the transmission of messages.	web socket transmits messages very fastly than REST API.
9.	It does not need memory or buffers to store the data.	It requires memory and buffers to store the data.

MQTT

Message Queuing Telemetry Transport (MQTT): The message query telemetry transport protocol is a communication-based protocol that is used for IoT devices. This protocol is based on the publish-subscribe methodology in which clients receive the information through a broker only to the subscribed topic. A broker is a mediator who categorizes messages into labels before being delivered.

Characteristics of the Protocol

- **Light-weight and reliable**: The MQTT message is compact, which can realize stable transmission on severely limited hardware equipment and network with low bandwidth and high delay.
- **Publish/subscribe mode**: Based on the publish/subscribe mode, the advantage of publishing and subscribing mode is that the publisher and subscriber are decoupled: Subscribers and publishers do not need to establish a direct connection or be online at the same time.
- **Created for the IoT**: It provides comprehensive IoT application features such as heartbeat mechanism, testament message, QoS quality level
- **Better ecosystem**: It covers all-language platform's clients and SDKs, and it has mature Broker server software, which can support massive Topic and ten-million-level device access and provide rich enterprise integration capabilities.

CoAP

Constrained Application Protocol (COAP): The constrained application protocol is a client server-based protocol. With this protocol, the COAP packet can be shared between different client nodes which are commanded by the COAP server. The server is responsible to share the information depending on its logic but has not acknowledged it. This is used with the applications which support the state transfer model.

Characteristics of the Protocol

CoAP refers to many design ideas of HTTP, and it also improves many design details and adds many practical functions according to the specific situation of limited resource-limited devices.

- It is based on message model

- Based on UDP Protocol, transport layer supports restricted devices
- It uses request/response model similar to HTTP request, and HTTP is text format, while CoAP is binary format, which is more compact than HTTP
- It supports two-way communication
- It has the characteristics of light-weight and low power consumption
- It supports reliable transmission, data re-transmission, and block transmission to ensure reliable arrival of data
- It supports IP multicast
- It supports observation mode
- It supports asynchronous communication

LoRaWAN

LoRaWAN refers to Long Rage Wide Area Network which is a wide area network protocol. It is an optimized low-power consumption protocol design to support large-scale public networks with millions of low-power devices. A single operator operates the LoRaWAN. The LoRaWAN network is a bi-directional communication for IoT application with low cost, mobility, and security..

An end device can connect to a network with LoRaWAN in two ways:

- Over-the-air Activation (OTAA): A device has to establish a network key and an application session key to connect with the network.
- Activation by Personalization (ABP): A device is hardcoded with keys needed to communicate with the network, making for a less secure but easier connection.

Properties of LoRaWAN protocol

- **Standard:** LoRaWAN
- **Frequency:** Various
- **Range:** 2-5km (urban environment), 15km (suburban environment)
- **Data Rates:** 0.3-50 kbps.

6LoWPAN

The 6LoWPAN protocol refers to IPv6 Low Power Personal Area Network which uses a lightweight IP-based communication to travel over low data rate networks. It has limited processing ability to transfer information wirelessly using an internet protocol. So, it is mainly used for home and building automation. The 6LoWPAN protocol operates only within the 2.4 GHz frequency range with 250 kbps transfer rate. It has a maximum length of 128-bit header packets.

6LowPAN Security Measure

Security is a major issue for 6LowPAN communication Protocol. There are several attacks issues at the security level of 6LoWPAN which aim is to direct destruction of the network. Since it is the combination of two systems, so, there is a possibility of attack from two sides that targets all the layer of the 6LoWPAN stack (Physical layer, Data link layer, Adaptation layer, Network layer, Transport layer, Application layer).

Basic Requirements of 6LoWPAN:

1. The device should be having sleep mode in order to support the battery saving.
2. Minimal memory requirement.
3. Routing overhead should be lowered.

Features of 6LoWPAN:

1. It is used with IEEE 802.15,.4 in the 2.4 GHz band.
2. Outdoor range: ~200 m (maximum)
3. Data rate: 200kbps (maximum)
4. Maximum number of nodes: ~100

Advantages of 6LoWPAN:

1. 6LoWPAN is a mesh network that is robust, scalable, and can heal on its own.
2. It delivers low-cost and secure communication in IoT devices.
3. It uses IPv6 protocol and so it can be directly routed to cloud platforms.
4. It offers one-to-many and many-to-one routing.

5. In the network, leaf nodes can be in sleep mode for a longer duration of time.

Disadvantages of 6LoWPAN:

1. It is comparatively less secure than Zigbee.
2. It has lesser immunity to interference than that Wi-Fi and Bluetooth.
3. Without the mesh topology, it supports a short range.

Applications of 6LoWPAN:

1. It is a wireless sensor network.
2. It is used in home-automation,
3. It is used in smart agricultural techniques, and industrial monitoring.
4. It is utilised to make IPv6 packet transmission on networks with constrained power and reliability resources possible.

Difference between COAP and MQTT protocols:

Basis of	COAP	MQTT
Abbreviation	Constrained Application Protocol	Message Queuing Telemetry Transport
Communication Type	It uses Request-Response model.	It uses Publish-Subscribe model
Messaging Mode	This uses both Asynchronous and Synchronous.	This uses only Asynchronous
Transport layer protocol	This mainly uses User Datagram protocol(UDP)	This mainly uses Transmission Control protocol(TCP)

Basis of	COAP	MQTT
Header size	It has 4 bytes sized header	It has 2 bytes sized header
RESTful based	Yes it uses REST principles	No it does not uses REST principles
Persistence support	It does not has such support	It supports and best used for live data communication
Message Labelling	It provides by adding labels to the messages.	It has no such feature.
Usability/Security	It is used in Utility area networks and has secured mechanism.	It is used in IoT applications and is secure
Effectiveness	Effectiveness in LNN is excellent.	Effectiveness in LNN is low.
Communication Model	Communication model is one-one.	Communication model is many-many.

Bluetooth

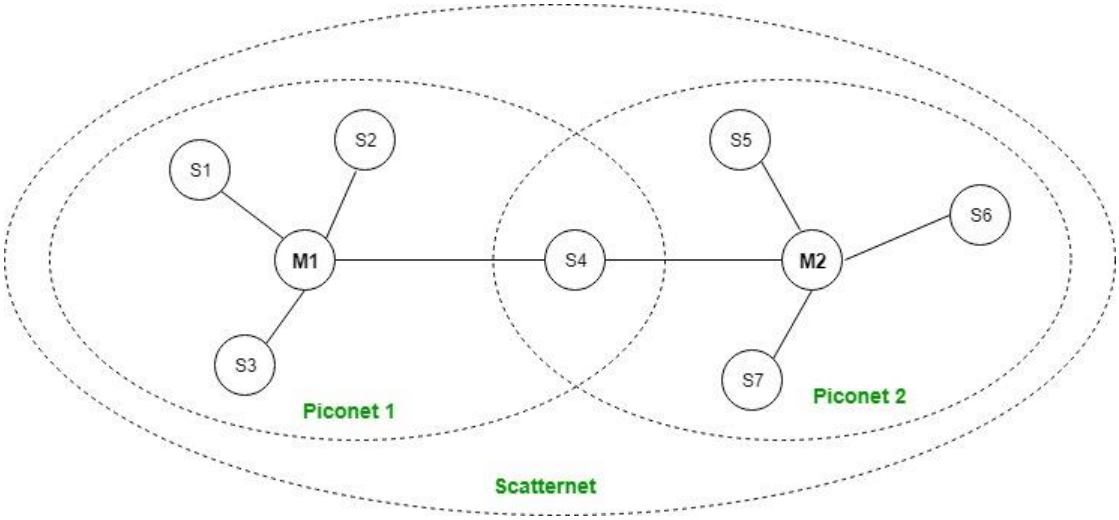
Bluetooth is universal for short-range wireless voice and data communication. It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific, and medical (ISM) band from 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges up to 10 meters. It provides data rates up to 1 Mbps or 3 Mbps depending upon the version. The

spreading technique that it uses is FHSS (Frequency-hopping spread spectrum). A Bluetooth network is called a **piconet** and a collection of interconnected piconets is called **scatternet**.

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1. Piconet
2. Scatternet



Piconet:

Piconet is a type of Bluetooth network that contains **one primary node** called the master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet:

It is formed by using **various piconets**. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message

from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Advantage:

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

- It can be used in laptops, and in wireless PCs, printers.
- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wirelessly to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical health care, sports and fitness, Military.

WIFI - Wireless Fidelity

Wifi is also known as **Wireless Fidelity.**

We are all familiar with Wi-Fi, which is available on our mobile phones, laptops, or wherever Wi-Fi is supported. Wi-Fi is **a wireless networking technology that permits to connect**

wirelessly to a network or to other computer or mobile device. A circular radio frequency range is used to transmit data in Wi-Fi.

Wireless Fidelity (Wi-Fi) is a generic term for the **wireless network in the communication norm**. Wifi operates like a local area network without the use of a wire or cables.

WLAN stands for **Wireless Local Area Network**. IEEE 802.11 is the rule for communication. WiFi uses the **Physical Data Link Layer (PDLL)** to operate.

Types or Kinds of Wifi

As mentioned earlier, Wi-Fi has numerous kinds or standards. Here, the names of the standards are defined.

- **Wi-Fi-1 (802.11b, launched in 1999**) - This version has link speed from 2Mb/s to 11 Mb/s over 2.4 GHz frequency band
- **Wi-Fi-2 (802.11a) launched in 1999**. After a month of releasing the previous version, 802.11a, was released, and it provides upto 54 Mb/s link speed over the 5 GHz band
- **Wi-Fi-3 (802.11g) was launched in 2003.** In this version, the speed was risen up to 54 to 108 Mb/s over 2.4 GHz
- **802.11i launched in 2004**. This is equivalentto**802.11g**, but only the security feature was enhanced in this version
- **802.11e launched in 2004**. This is also the same as **802.11g**; only Voice over Wireless LAN and multimedia streaming are included.
- **Wi-Fi-4 (802.11n) launched in 2009**. This version holds up both 2.4 GHz and 5 GHz radio frequencies, and it provides up to 72 to 600 Mb/s speed.
- **Wi-Fi-5 (802.11ac) launched in 2014**. It supports a speed of 1733 Mb/s in the 5 GHz band.

Advantages of WIFI

The advantages of Wi-Fi Tt include

- A **versatile network connection** and the absence of complicated wiring requirements for installation.
- Everywhere in the Wi-Fi range can access it.

- Independent users are not required to obtain regulatory approval.
- In addition, Wi-Fi Extenders make it possible to expand the network.
- It's easy and quick to set up.
- Only the SSID and password need to be configured.
- As part of its security measures, Wi-Fi networks encrypt radio signals using WPA encryption.
- It is also more affordable.
- Hotspots are another feature that it offers.
- Roaming is supported as well.

Wi-Fi Disadvantages

- Mobile phones, laptops, and other devices with batteries consume a lot of power when using Wi-Fi.
- Even when encryption is in place, security issues can still arise.
- Wi-Fi can be attacked and accessed in the same way that recognised devices become unidentified to the router.
- In comparison to a direct cable connection, the speed is slower.
- People can be harmed by it because it emits radiation like cell phones.
- Thunderstorms, for example, can interfere with Wi-Fi signals.
- Because it **lacks a firewall, unauthorised access** to Wi-Fi is possible.
- Since a router is required to access the internet via Wi-Fi, we can't access the internet if the power goes out.

Zigbee

What is Zigbee? – Zigbee is a **low power**, low data rate (250kbps) wireless protocol used primarily for Home automation and industrial control, building automation,sensor data collection etc

Zigbee devices have a range (1 hop) of 80 to 100m.

Devices can be split into:

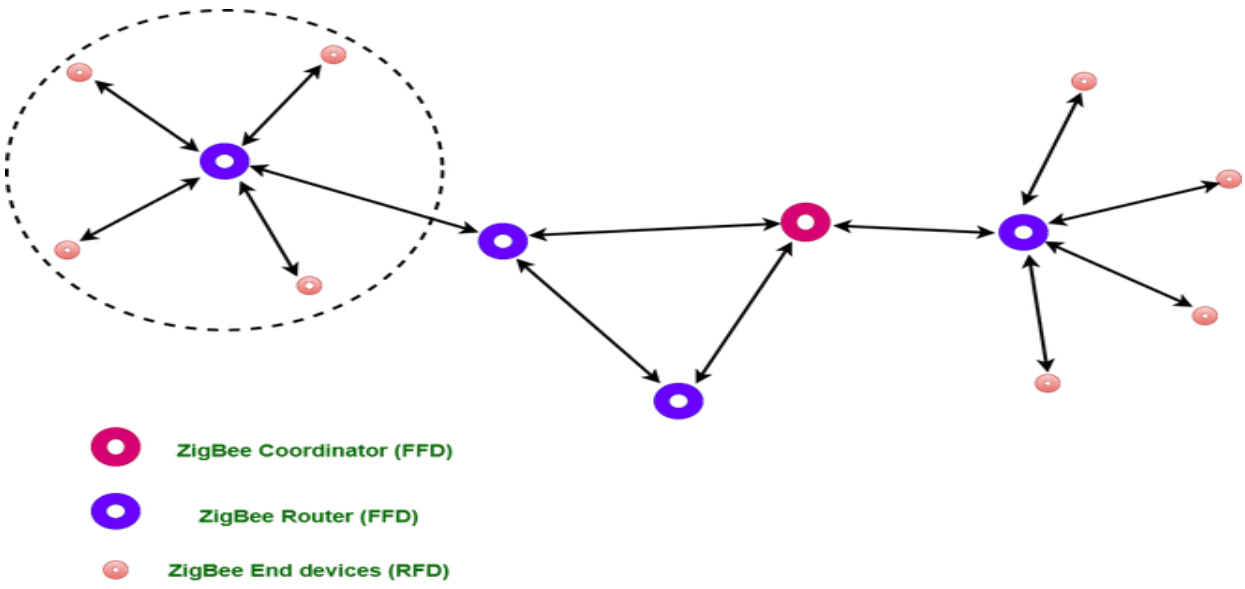
- **Full Function Device** (FFD)

Full Function Device (FFD)- Can communicates with all node types and can operate in one of three modes:

- **Zigbee Coordinator Device:** It communicates with routers. This device is used for connecting the devices.
- **Zigbee Router:** It is used for passing the data between devices.

Zigbee End Device: It is the device that is going to be controlled. There must be 1 coordinator on a Zigbee network.

Reduced Function Device (RFD): Can only talk to a single FFD. These are end nodes. Example a smart lock,switch ect



General Characteristics of Zigbee Standard:

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)
- Extremely low-duty cycle.
- 3 frequency bands with 27 channels.

Operating Frequency

1. **Channel 0**: 868 MHz (Europe)
2. **Channel 1-10**: 915 MHz (the US and Australia)
3. **Channel 11-26**: 2.4 GHz (Across the World)

Features of Zigbee:

1. Stochastic addressing: A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents node don't need to maintain assigned address table.

2. Link Management: Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.

3. Frequency Agility: Nodes experience interference report to channel manager, which then selects another channel

4. Asymmetric Link: Each node has different transmit power and sensitivity. Paths may be asymmetric.

5. Power Management: Routers and Coordinators use main power. End Devices use batteries.

Advantages of Zigbee:

1. Designed for low power consumption.
2. Provides network security and application support services operating on the top of IEEE.
3. Zigbee makes possible completely networks homes where all devices are able to communicate and be
4. Use in smart home
5. Easy implementation
6. Adequate security features.
7. **Low cost**: Zigbee chips and modules are relatively inexpensive, which makes it a cost-effective solution for IoT applications.
8. **Mesh networking:** Zigbee uses a mesh network topology, which allows for devices to communicate with each other without the need for a central hub or router. This makes it ideal for use in smart home applications where devices need to communicate with each other and with a central control hub.
9. **Reliability:** Zigbee protocol is designed to be highly reliable, with robust mechanisms in place to ensure that data is delivered reliably even in adverse conditions.

Disadvantages of Zigbee :

1. **Limited range:** Zigbee has a relatively short range compared to other wireless communications protocols, which can make it less suitable for certain types of applications or for use in large buildings.
2. **Limited data rate:** Zigbee is designed for low-data-rate applications, which can make it less suitable for applications that require high-speed data transfer.
3. **Interoperability:** Zigbee is not as widely adopted as other IoT protocols, which can make it difficult to find devices that are compatible with each other.
4. **Security:** Zigbee's security features are not as robust as other IoT protocols, making it more vulnerable to hacking and other security threats.

Zigbee Applications:

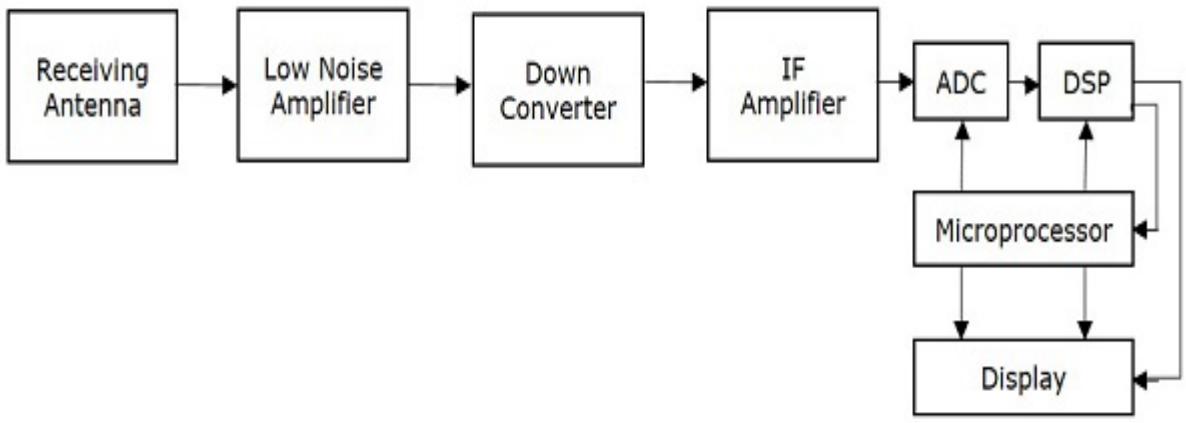
1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems
4. meter reading system
5. light control system
6. Commercial
7. Government Markets Worldwide
8. Home Networking

GPS

Global Positioning System **(GPS)** is a navigation system based on satellite. It has created the revolution in navigation and position location. It is mainly used in positioning, navigation, monitoring and surveying applications.

GPS receiver basically consists of three components:

- An Antenna (tuned to the frequencies transmitted by the satellites).
- Receiver processor.
- Highly Stable Clock (Commonly a Crystal oscillator).



- **Receiving Antenna** receives the satellite signals. It is mainly, a circularly polarized antenna.
- **Low Noise Amplifier** (LNA) amplifies the weak received signal
- **Down converter** converts the frequency of received signal to an Intermediate Frequency (IF) signal.
- **IF Amplifier** amplifies the Intermediate Frequency (IF) signal.
- **ADC** performs the conversion of analog signal, which is obtained from IF amplifier to digital. Assume, the sampling & quantization blocks are also present in ADC (Analog to Digital Converter).
- **DSP** (Digital Signal Processor) generates the C/A code.
- **Microprocessor** performs the calculation of position and provides the timing signals in order to control the operation of other digital blocks. It sends the useful information to Display unit in order to display it on the screen.

Usage of GPS:

There are five most uses of the GPS.

- **Location:-** with the help of GPS we can find the exact position of the object.
- **Navigation:**– we can navigate one location to another with the help of GPS.GPS technology is also useful for Transportation Management and breathing of Ship at docks.
- **Tracking**: -with the help of GPS we can Monitor object movement like speed, distance, position.
- **Mapping:**– GPS also helps in creating maps of the World.
- **Timing**:- GPS also provides the estimated time for reaching destination measurement its depend on speed and object movement.

GSM

GSM stands for **Global System for Mobile Communication.** GSM is an open and digital cellular technology used for mobile communication. It uses 4 different frequency bands of 850 MHz, 900 MHz, 1800 MHz and 1900 MHz . It uses the combination of FDMA and TDMA.

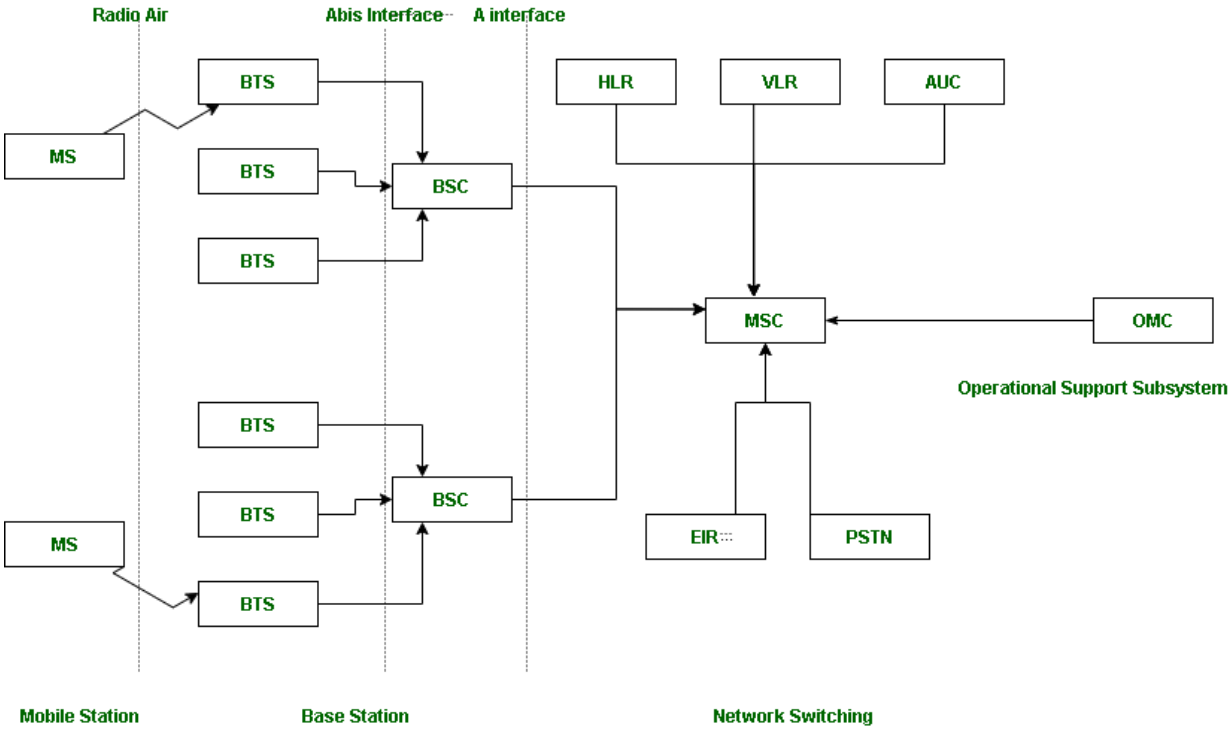
GSM is having 4 different sizes of cells are used in GSM :

1. Macro : In this size of cell, Base Station antenna is installed.
2. Micro : In this size of cell, antenna height is less than the average roof level.
3. Pico : Small cells' diameter of few meters.
4. Umbrella : It covers the shadowed (Fill the gaps between cells) regions.

Features of GSM are :

1. Supports international roaming
2. Clear voice clarity
3. Ability to support multiple handheld devices.
4. Spectral / frequency efficiency
5. Low powered handheld devices.
6. Ease of accessing network
7. International ISDN compatibility.
8. Low service cost.
9. New features and services.

1. **BSS :** BSS stands for Base Station Subsystem. BSS handles traffic and signaling between a mobile phone and the network switching subsystem. BSS having two components **BTS** and **BSC.**
2. **NSS :** NSS stands for Network and Switching Subsystem. NSS is the core network of GSM. That carried out call and mobility management functions for mobile phone present in network. NSS have different components like **VLR, HLR** and **EIR.**
3. **OSS :** OSS stands for Operating Subsystem. OSS is a functional entity which the network operator monitor and control the system. **OMC** is the part of OSS. Purpose of OSS is to offer the customer cost-effective support for all GSM related maintenance services.



Suppose there are 3 Mobile stations which are connected with the tower and that tower is connected to BTS through TRX, then further connected to BSC and MSC. Let's understand the functionality of different components.

1. MS : MS stands for Mobile System. MS comprises user equipment and software needed for communication with a mobile network. Mobile Station (MS) = Mobile Equipment(ME) + Subscriber Identity Module (SIM). Now, these mobile stations are connected to tower and that tower connected with BTS through TRX. TRX is a transceiver which comprises transmitter and receiver. Transceiver has two performance of sending and receiving.

2. BTS : BTS stands for Base Transceiver Station which facilitates wireless communication between user equipment and a network. Every tower has BTS.

3. BSC : BSC stands for Base Station Controller. BSC has multiple BTS. You can consider the BSC as a local exchange of your area which has multiple towers and multiple towers have BTS.

4. MSC : MSC stands for Mobile Switching Center. MSC is associated with communication switching functions such as call setup, call release and routing. Call tracing, call forwarding all functions are performed at the MSC level.

Services of GSM:

- Telephony services or teleservices
- Data services or bearer services
- Supplementary services

Advantages:

Compatibility: GSM is widely used around the world, so it is compatible with many different networks and devices.
Security: GSM offers enhanced security features such as authentication, encryption and confidentiality, which helps to protect the user's privacy and data.
Efficient use of bandwidth: GSM uses a time-division multiplexing (TDM) technique which enables many users to share the same frequency channel at different times, making it an efficient use of the available bandwidth.
Roaming: GSM allows users to roam internationally and use their mobile phones in other countries that use the same GSM standard.
Wide range of features: GSM supports a wide range of features, including call forwarding, call waiting, voicemail, conference calling, and more.

Disadvantages:

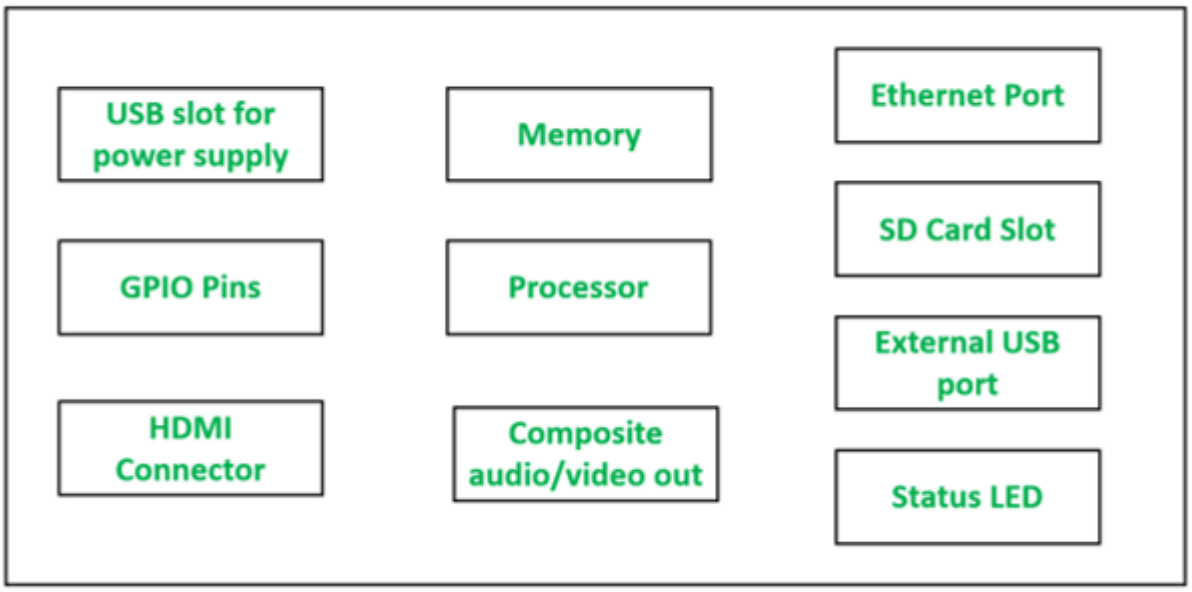
Limited coverage: GSM networks may have limited coverage in some remote areas, which can make it difficult for users to make calls or access the internet.
Network congestion: GSM networks may become congested during peak hours, which can lead to dropped calls or poor call quality.
Security vulnerabilities: Although GSM offers enhanced security features, it is still vulnerable to certain types of attacks, such as eavesdropping and spoofing.
Data transfer speed: GSM networks offer relatively slow data transfer speeds compared to newer technologies such as 3G and 4G.
Limited capacity: GSM networks have a limited capacity for handling large volumes of data, which can be a disadvantage for users who require high-speed internet access or other data-intensive applications.

Single Board Computers -Raspberry-Pi

Raspberry Pi is developed by Raspberry Pi Foundation in the United Kingdom. The Raspberry Pi is a series of powerful, small single-board computers.

Raspberry Pi is launched in 2012 and there have been several iterations and variations released since then.

Various versions of Raspberry Pi have been out till date. All versions consist of a Broadcom system on a chip (SoC) with an integrated ARM-compatible CPU and on-chip graphics processing unit (GPU).

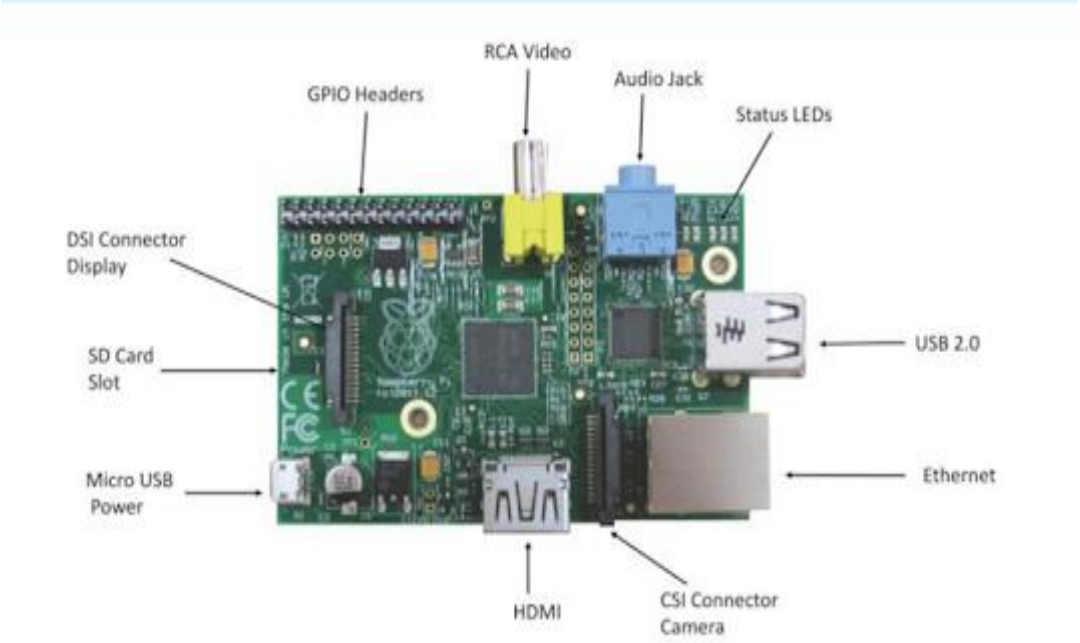


Block Diagram of Raspberry Pi

- A low-cost, **credit-card-sized** minicomputer**.**
- Plugs into a computer monitor or TV.
- Uses a standard keyboard and mouse.
- Use for explore computing as for programmings like Scratch and Python languages.
- Capable as a normal desktop computer to browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games."

- Allowing interface sensors and actuators through the general purpose IO pins
- Supports Python out of box

Structure of board



Raspberry Pi board uses various components and peripherals as follows:-

Processor and Ram

- Based on an ARM processor.
- The latest version of Raspberry Pi (model B, revision 2) comes with a 700 MHz low-power ARM 1176JZ-F processor And a 512 MB SD Ram.

USB ports

- Two USB 2.0 USB ports on Raspberry pi can provide a current of up to 100 mA.
- For connecting devices that draw a current of more than 100 mA, an external USB-powered hub is required.

Ethernet port

- Standard RJ45 Ethernet port.
- Connect an ethernet cable or USB Wi-Fi adaptor to provide internet connectivity.

HDMI outputs

- The HDMI port on Raspberry Pi provides both video and audio output.
- Connect the Raspberry Pi to a monitor by an HDMI cable.
- For monitors that have a DVI port but no HDMI port so use an HDMI to DVI adaptor or cable.

Composite video output with RCA jack

- Support both PAL and NTSC video output.
- RCA jack is used to connect old television that has an RCA input only.

Audio output

- 3.5 mm audio output jack is used for audio output to old television along with the RCA Jack for video.
- The audio quality is inferior to the HDMI output.

Display serial interface(DSI)

- Used to connect an LCD panel to Raspberry Pi.

Camera serial interface(CSI)

- Used to connect a camera module to Raspberry Pi.

Status LEDs

- Raspberry Pi has 5 status LED is which are:-
- ACT:- SD card access.
- PWR:- 3.3 V power is present.
- FDX:- Full duplex LAN connected.
- LNK:- link/ network activity.
- 100:- 100 Mbit LAN connected.

SD card slot

- Not have a built-in operating system and storage so plug in an SD card loaded with a Linux image to an SD card slot.

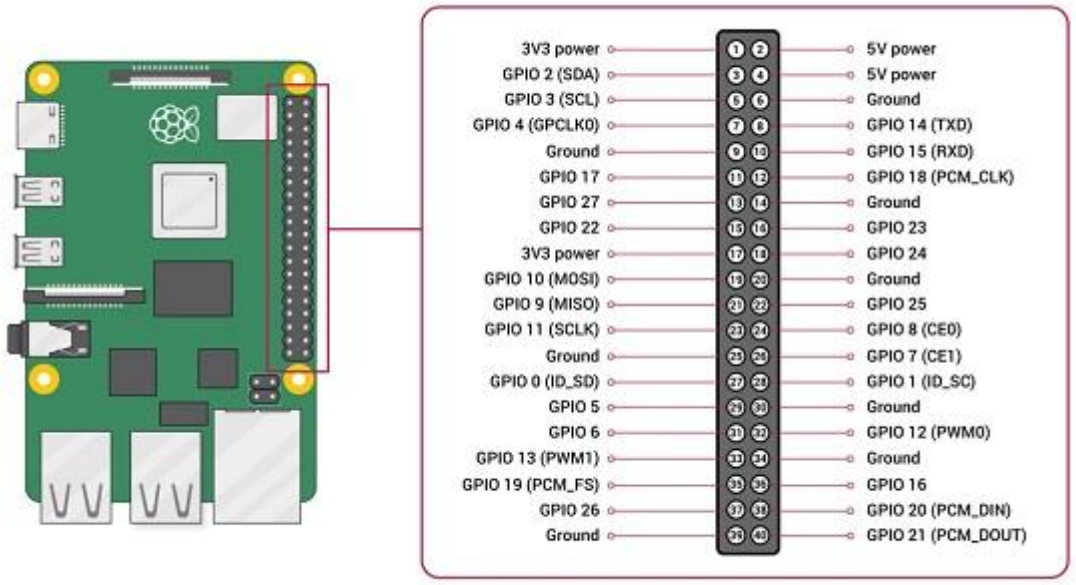
- Required at least an 8GB SD card for the setting up NOOBS software (new out-of-the-box software)

Power input

- A micro-USB connector for power input.

GPIO Pin

- A number of general-purpose Input / Output pins are used by Raspberry Pi.
- There are four types of pins on Raspberry Pi:- True GPIO pins, SPI interface pins, 12C interface pins, and Serial RX and TX pins.



Voltages

From the above diagram, we can see that there are two 5V pins and two 3V3 pins on the board. It also has several ground pins (0V). All these pins are unconfigurable.

Outputs

A GPIO pin can be designated as an output pin. The pin set as output pin can be set to 3V(high) or 0V(low).

Inputs

A GPIO pin can be designated as an input pin. The pin set as input pin can be read as 3V(high) or 0V(low). You can use internal pull-up or pull-down resistors.

above diagram, GPIO2 and GPIO3 pins have fixed pull-up resistors but for the other pins, you can configure it in software.

Alternative Functions

GPIO pins can be used with a variety of alternative functions. Among them, some are available on all pins and others on specific pins.

PWM: Pulse-width modulation

Software PWM are available on all the pins whereas Hardware PWM are available on GPIO12, GPIO13, GPIO18, and GPIO19.

SPI: Serial Peripheral Interface

The SPI are available on the following −

SPI0: MOSI (GPIO10); MISO (GPIO9); SCLK (GPIO11); CE0 (GPIO8), CE1 (GPIO7)
SPI1: MOSI (GPIO20); MISO (GPIO19); SCLK (GPIO21); CE0 (GPIO18); CE1 (GPIO17); CE2 (GPIO16)

I2C: Inter-integrated Circuit

The I2C are available on the following −

Data: (GPIO2); Clock (GPIO3)
EEPROM Data: (GPIO0); EEPROM Clock (GPIO1)

Serial

The serial function is available at the following −

TX(GPIO14)
RX(GPIO15)

Raspberry pi Connecting to the Cloud

Connecting a Raspberry Pi to the cloud allows you to access and manage your Raspberry Pi remotely, exchange data with cloud services, and perform various tasks such as data logging, remote control, and automation. Here's a general overview of how to connect a Raspberry Pi to the cloud:

1. **Select a Cloud Service Provider:** Choose a cloud service provider that fits your needs. Some popular options include AWS (Amazon Web Services), Microsoft Azure, Google Cloud Platform, and various IoT-focused platforms like AWS IoT, Azure IoT, or Google Cloud IoT. Each has its own set of features, pricing, and capabilities.
2. **Set Up Your Raspberry Pi:** Ensure your Raspberry Pi is set up correctly, connected to the internet, and running an appropriate operating system like Raspbian (now called Raspberry Pi OS).
3. **Install Necessary Software:** Depending on your chosen cloud platform, you may need to install specific libraries or SDKs on your Raspberry Pi. For example, if you're using AWS, you would install the AWS SDK for Python (Boto3). If you're using Azure, you might use the Azure IoT SDK or Azure Python SDK.
4. **Create Cloud Resources:** Create the necessary resources on your cloud platform. For example, if you're using AWS IoT, you'd create an IoT Thing, a policy, and certificates.
5. **Connect to the Cloud:** Write code on your Raspberry Pi to connect to your cloud platform of choice. This typically involves using the SDK you installed earlier and providing the necessary authentication credentials (e.g., API keys, certificates, or access tokens).
6. **Publish and Subscribe to Topics (MQTT):** Many IoT applications use the publish-subscribe model for communication. MQTT (Message Queuing Telemetry Transport) is a common protocol for this purpose. You can publish data from your Raspberry Pi to specific MQTT topics and subscribe to topics to receive commands or data from the cloud.
7. **Data Handling and Processing:** Once your Raspberry Pi is connected, you can send and receive data between the Raspberry Pi and the cloud. You may want to implement data processing, storage, or analytics depending on your project's requirements.
8. **Security Considerations:** Ensure proper security practices. Use secure connections (HTTPS, MQTT over TLS), secure your IoT devices and cloud resources, and regularly update your Raspberry Pi's software to patch any security vulnerabilities.

9. **Monitoring and Management:** Set up monitoring and management tools provided by your cloud platform to keep an eye on your Raspberry Pi's health and performance. This might include dashboards, alerts, and logging.
10. **Scale and Optimize:** As your project grows, you may need to scale your cloud resources and optimize your code and infrastructure for performance and cost-efficiency.

UNIT 5 - APPLICATIONS DEVELOPMENT

Complete Design of Embedded Systems – Development of IoT Applications – Home Automation –Smart Agriculture – Smart Cities – Smart Healthcare.

Embedded System

As its name suggests, Embedded means something that is attached to another thing. An embedded system can be thought of as a computer hardware system having software embedded in it. An embedded system can be an independent system or it can be a part of a large system. An embedded system is a microcontroller or microprocessor based system which is designed to perform a specific task. For example, a fire alarm is an embedded system; it will sense only smoke.

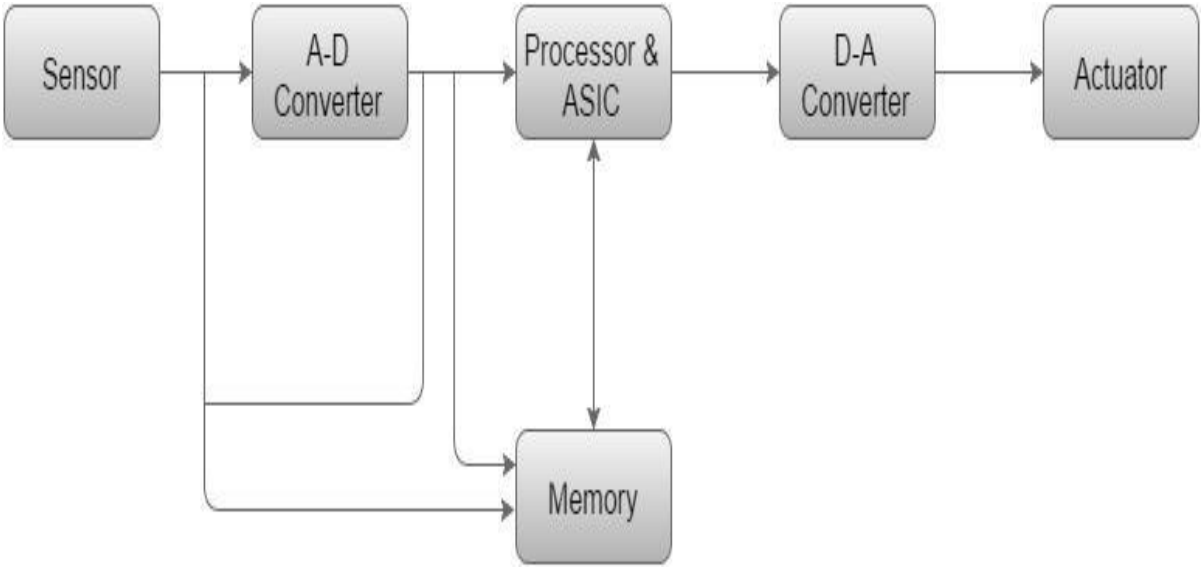
An embedded system has three components −

- It has hardware.
- It has application software.
- It has Real Time Operating system (RTOS) that supervises the application software and provide mechanism to let the processor run a process as per scheduling by following a plan to control the latencies. RTOS defines the way the system works. It sets the rules during the execution of application program. A small scale embedded system may not have RTOS.

So we can define an embedded system as a Microcontroller based, software driven, reliable, real-time control system.

Basic Structure of an Embedded System

The following illustration shows the basic structure of an embedded system −



- **Sensor** − It measures the physical quantity and converts it to an electrical signal which can be read by an observer or by any electronic instrument like an A2D converter. A sensor stores the measured quantity to the memory.
- **A-D Converter** − An analog-to-digital converter converts the analog signal sent by the sensor into a digital signal.
- **Processor & ASICs** − Processors process the data to measure the output and store it to the memory.
- **D-A Converter** − A digital-to-analog converter converts the digital data fed by the processor to analog data
- **Actuator** − An actuator compares the output given by the D-A Converter to the actual (expected) output stored in it and stores the approved output.

Advantages

- Easily Customizable
- Low power consumption
- Low cost
- Enhanced performance

Disadvantages

- High development effort
- Larger time to market

Home Automation

Home Automation is a system that allows users to control various appliances of varying kinds and also makes controlling of home appliances easier and saves energy. Nowadays, home automation is used more and more. On the other hand, it provides increased comfort especially when everyone is busy with their work. Home automation installed in houses does not only increase comfort but also allows centralized control of heating, ventilation, air-condition, and lighting. Hence, they contribute to an overall cost reduction and also useful in energy saving which is certainly the main problem today.

In present years, wireless systems like Wi-Fi, Bluetooth have become more and more common in home networking. Also in home automation, the use of wireless technologies gives several advantages that could not be achieved using a wired network only.

Home Automation Components: At the most initial level, home automation systems are made up of three elements-

1. A smart device.
2. A hub.
3. A connected application.

While some other home automation systems work with just two elements which include a single device that works with the help of an app on mobile or a tablet or a system that includes a hands-free hub that controls home automation system while most of the systems work using all the above three components.

1. Smart Devices: These are the real powerhouse of any home automation system. These are the main parts that actually implement the whole system commands. Examples of the smart devices which can be added to any home automation to complete the whole system are as follows:

- **Access Control**
- **Security Devices:** This includes security cameras, smart locks.
- **Home Appliances:** Smart refrigerators, washing machines, dishwashers, and ovens already exist.
- **Smaller Appliances:** As automatic coffee pots and electric kettle have been also around for a while too
- **Climate Controls:** Climate control system with energy management systems
- **Smart Thermostats.**

- **Entertainment Pieces:** Entertainment includes smart TVs, wireless speakers, and film projectors
- **Health Care Devices:** Smart humidifiers and smart scales are two common examples of health care devices.
- **Lighting Controls:** They include dimmers, light bulbs, light strips, and switches, etc.

A high-speed internet plays an important role in smooth connectivity and also plays an important reliable performance between Wi-Fi-enabled devices.

2. Smart Hubs: The hub is the controlling center of the home automation system. It is the piece that connects your individual devices and helps them talk to one another.

3. Mobile Apps: The mobile application provides an interface between the user and the system. It gives you the ability to control or monitor your smart devices remotely. They can be easily downloaded with the help of a provided application on mobile and provide access control of the system, power controls, timer access, and many more things.

How Home Automation Works?

Home automation works with the help of a network of devices that are connected to the Internet through different communication systems like Wi-Fi, Bluetooth, ZigBee, and others. Through these devices can be managed remotely through controllers through an app. Many of these IoT devices have sensors that monitor changes in motion, temperature, and light so the user can gain information about the device's surroundings.

Three steps are followed in Home automation as follows:

1. **Monitoring:** This means keeping the control of the system using an app on a device remotely.
2. **Control:** This means that the system can be controlled remotely from anywhere through the app by the user.
3. **Automation:** Automation means making almost all devices automatic for making it a better system.

Applications: Some of the most common applications of home automation are as follows-

- Heating, ventilation, and air conditioning.
- Lighting control system.

- Occupancy-aware control system.
- Leak detection.
- Smoke sensors.
- Indoor positioning systems.
- Home automation for the elderly and disabled.
- Air quality control.
- Smart Kitchen.
- Connected Cooking.
- Voice control devices like Amazon Alexa or Google Home used to control home appliances or systems etc.

Advantages of Home Automation:

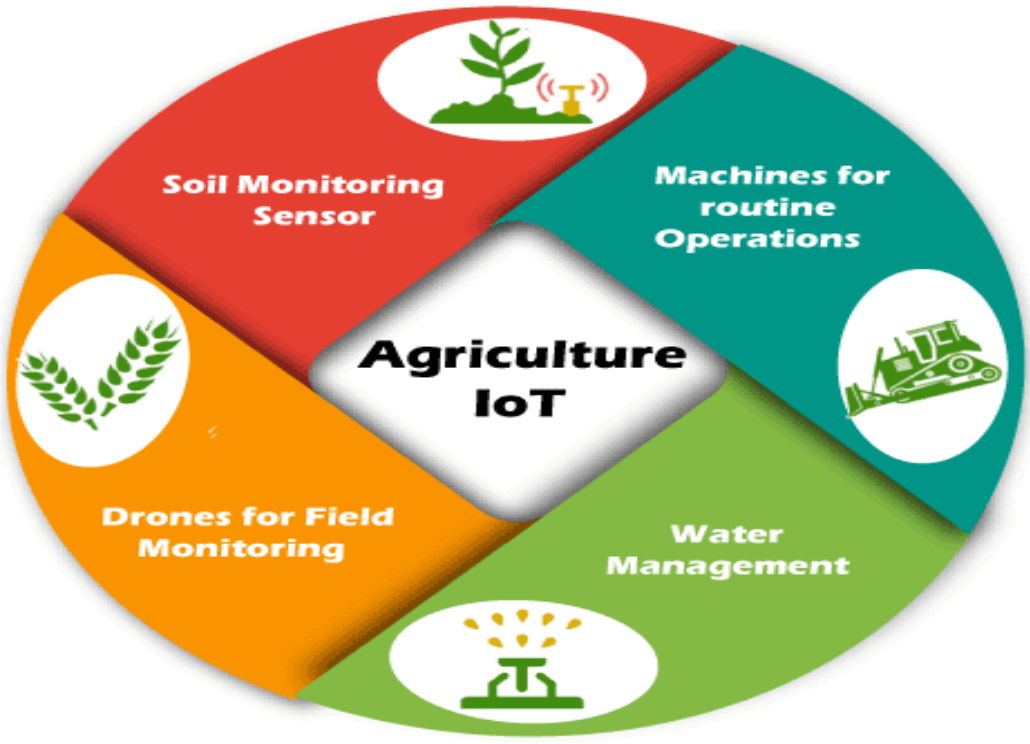
- **Energy Savings:** Self-automated light bulbs, fans, and switchboards save energy, cutting utility costs over time.
- **Home Safety:** Home automation provides the best technologies for home security. Consumers purchase these devices because they want to make their homes safer and more secure. Automatic lighting systems and motion sensors help people to enter doors and walk late at night.
- **User Convenient:** Because home automation performs role tasks automatically, end-users experience great convenience. For instance, you could use sensors indoors to turn on your smart lighting when you unlock the front door.
- **Better Control:** Consumers also choose smart home devices to better control functions within the home. With home automation technology, you can know easily what's happening inside your home at all times.
- **Comfortable Atmosphere:** All Connected devices around our home can also help to create a comfortable atmosphere—they provide intelligent and reliable lighting, sound, and temperature, which can all help to create a comfortable environment.
- **Provide Peace of Mind:** This system may help consumers to invest in home automation for peace of mind.
- **Remote Access:** Being able to control devices remotely means things like unlocking the door for a plant sitter without having to leave a key under the mat.

Disadvantages Of Home Automation:

- **Costs:** These are more expensive than their non-WiFi-connected counterparts.
- **Security Issues:** There are many security issues like the doorbell can be started ringing automatically etc.
- **New Technology:** Since IoT is a relatively new technology, you may run into some bugs, like devices having trouble connecting to the Internet or experiencing lag, depending on the device make and model.
- **Surveillance:** If privacy is a huge concern, then smart security is probably not for you, as users can live stream footage from the camera's respective app. Instead, you might want to opt for a local alarm system.

IOT in Agriculture

Agriculture is another important domain for IOT. IOT systems play an important role for crop and soil monitoring and give a proper solution accordingly. IOT leads to smart farming. Using IOT, farmers can minimize waste and increase productivity. The system allows the monitoring of fields with the help of sensors. Farmers can monitor the status of the area.



Challenges in the modern agriculture industry

The challenges faced by the farming industry and agriculture are listed as follows -

- Lack of workforce and manpower
- Environmental challenges and global warming
- Requirement of large manual intervention
- Lack of proper monitoring
- Challenges in analyzing the large scale unstructured data

There are various uses of IOT in agriculture that are discussed as follows -

IOT analytics in agriculture

The data from smart sensors can be further analyzed for automated decision-making and predictive analysis. Machine learning and predictive analysis will be helpful for farmers to cope up with the weather conditions such as drought, flood, etc.

Drone-based uses

Drones are also useful in smart farming. On one side, drones are useful to monitor the soil, air, moisture quality, and on another side, they can also be used for physical activities such as prevention of physical breakouts in farms, automated spraying of fertilizers, and many more. Although there are some limitations of using a drone, but it is useful to reduce the manual workforce.

Real-time crop monitoring

Motion detectors, light detectors, smart-motion sensing sensors, smart sensors are useful to provide real-time data to farmers of their farms. It will be helpful in the monitoring of the quality of their products.

Smart Irrigation system

It is one of the parts of smart agriculture using IOT. In it, IOT checks the water lanes created by the farmer or the moisture level in the environment.

Infrastructure requirements

There are some infrastructure requirements for adopting smart farming in IOT. Some of the requirements are listed as follows -

- Hardware maintenance cost
- Continuous connectivity to the internet
- Required high investments in drones, sensors
- The requirement to hire highly trained staff for management and to operate
- Requirement of power connectivity to operate and charge the robots and drones

IoT in Smart Cities

1. Water Level Checking

The water supply is one of the most significant perspectives for legislatures. With intelligent sensors, the water levels can be checked progressively.

These sensors can send triggers and alarms to key chiefs for low or high water levels. The spillages and water dispersion can be combined using IoT sensors and ICT frameworks.

All regions with a plentiful water supply can be set apart on the guide; correspondingly, the guides can feature regions with water spillage or deficiency.

A complete outline of the water supply with GPS directions can be given to water specialists with IoT frameworks.

2. Health Cards

Clinics and medical services frameworks are significant marks of administration. The smart city requires a state−of−the−art medical services framework that can follow quantifiable advancement concerning residents' well−being.

A shrewd card−based framework can be utilized by people that might be utilized in all administration and approved clinics.

This card will have the verifiable subtleties of the medicines and so on for people. The robust medical care framework will empower the public authority to look at the clinics and their administrations to residents.

The smart card empowers the framework to work with simple information assortment. The cloud−based framework can give essential knowledge to Medical services experts for a further progressive organization.

3. Waste & Garbage Management

The waste and trash the executive's exercises can be improved with intelligent sensors and IoT Frameworks.

The trash containers can utilize intelligent sensors to demonstrate when they should be discharged. This diminishes the times that vehicles are expected to gather the trash from the receptacles and evades what is going on of waste flood.

Metropolitan organizations can involve shrewd receptacles and IoT frameworks for trash assortment.

4. Transport Systems

The transportation framework for the residents can be improved with IoT−empowered frameworks. The armadas can be overseen and followed utilizing GPS beacons.

Legislatures can finish armadas' organization, planning, ongoing situating, support, and free time for executives with IoT frameworks.

The residents can likewise benefit from transportation administrations with a card−based framework for tickets and so on.

5. Smart Traffic Management

Traffic is one of the significant problem areas for residents. With IoT sensors, traffic can be controlled better.

The sensors are associated with traffic lights and send data to an incorporated server. The approaching vehicles are followed utilizing these sensors.

When the quantity of vehicles arrives at a limit, signals are shipped off to the drivers to redirect. These signs are shown with electronic showcase sheets.

Constant traffic cautions and GIS planning of the streets can further develop gridlocks and blockage during top hours.

6. Infrastructure Assets Management

The brilliant city requires advanced usage of framework resources. The plants, apparatus, and gear are labeled and observed with the brought−together resource of the executive's framework.

The continuous undertaking stock for different advancement works can be followed utilizing the brought−together framework.

The situation with framework resources, their usage, upkeep, and the complete lifecycle of the board should be possible with the brought−together IoT framework.

7. Surveillance Systems

IP cameras and reconnaissance frameworks can assist the public authority with controlling crime percentages in a city.

The IP cameras can be utilized for surveying and monitoring essential foundations. These cameras can be associated with unified frameworks with reinforcements for verifiable information.

A versatile reconnaissance framework can be set up with IoT video arrangements safeguarding individuals, spots, and resources.

8. Pollution Control With Sensors

Urbanization has prompted an uncommon expansion in contamination levels. The rising contamination levels are causing medical problems for residents.

With IoT−empowered sensors, contamination can be estimated progressively. The contamination sensors send data to an incorporated server.

The public authority can make a move given the contamination levels; e.g., they can establish trees in a specific area.

The plant life and contamination levels can likewise be portrayed online with google maps for executives.

9. Smart Energy Management

One of the critical difficulties for state−run administrations is to decrease energy utilization and introduce a proficient appropriation framework set up.

Brilliant framework arrangements, electronic meters, and intelligent lighting frameworks are a portion of the components that are utilized by legislatures to oversee energy effectively.

The power dispersion guides can show on going energy utilization levels, spillages, and upkeep plans. The IoT−empowered arrangements can improve the energy of the board for urban areas.

10. E-Services

This can be overseen through biometric confirmation or smart cards. Residents can benefit from all taxpayer−driven organizations through this card.

The public authority can collect data through these cards for proactive preparation and the executives.

All taxpayer−supported organizations can be incorporated through the e−administrations gateway.

The residents can benefit from these offices for paying their water and power bills, local charges, medical clinic check−ups, etc. Coordinated information additionally helps in strategy−making and organization.

Internet of Things (IoT) in Healthcare

IoT technology brings numerous applications in healthcare, from remote monitoring to smart sensors to medical device integration. It keeps the patients safe and healthy as well as improves the physician delivers care towards the patients.

Healthcare devices collect diverse data from a large set of real-world cases that increases the accuracy and the size of medical data.

Factor affecting IoT Healthcare Application

There are various factors that affect the IoT healthcare application. Some of them are mention below:

- **Continuous Research:** It requires continuous research in every field (smart devices, fast communication channel, etc.) of healthcare to provide a fast and better facility for patients.
- **Smart Devices:** Need to use the smart device in the healthcare system. IoT opens the potential of current technology and leads us toward new and better medical device solutions.
- **Better Care:** Using IoT technology, healthcare professionals get the enormous data of the patient, analysis the data and facilitate better care to the patient.
- **Medical Information Distribution:** IoT technology makes a transparency of information and distributes the accurate and current information to patients. This leads the fewer accidents from miscommunication, better preventive care, and improved patient satisfaction.

Simple Healthcare System Architecture

The application of the Internet of Things (IoT) in healthcare transforms it into more smart, fast and more accurate. There is different IoT architecture in healthcare that brings start health care system.

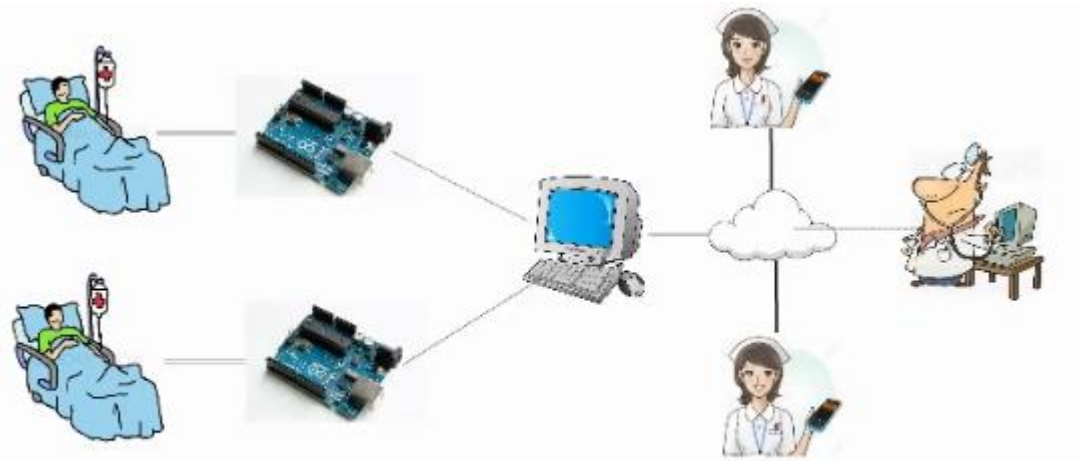
Product Infrastructure: IoT product infrastructure such as hardware/software component read the sensors signals and display them to a dedicated device.

Sensors: IoT in healthcare has different sensors devices such as pulse-oximeter, electrocardiogram, thermometer, fluid level sensor, sphygmomanometer (blood pressure) that read the current patient situation (data).

Connectivity: IoT system provides better connectivity (using Bluetooth, WiFi, etc.) of devices or sensors from microcontroller to server and vice-versa to read data.

Analytics: Healthcare system analyzes the data from sensors and correlates to get healthy parameters of the patient and on the basis of their analyze data they can upgrade the patient health.

Application Platform: IoT system access information to healthcare professionals on their monitor device for all patients with all details.



IoT in Healthcare – a concept

IoT challenges in Healthcare

- Data security & privacy
- Integration: multiple devices & protocols
- Data overload & accuracy
- Cost