UNIT III

IoT Design Methodology:

* Steps:-

Purpose and requirements
Define purpose and requirements of IoT
↓
Process model specification
Define the use cases
↓
Domain model Specification
Define physical entities, virtual entities, devices, resource & services in the IoT system
↓
Information Model Specification
Define the structure (e.g. relations, attributes) of all the information in the IoT system
↓
Service specifications
Map Process and Information Model to services and define service specifications
↓
IoT level Specification
Define the IoT level for the system
↓
Functional View Specification
Map IoT level to functional groups
↓
Operational view Specification
Define commn options, service hosting options, storage options, device option.
↓
Device & component Integration
Integrate devices, develop and integrate the components
↓
Application Development
Develop Applications.

Steps:

1) Purpose & Requirements Specification:-

- First step is to define the purpose and requirements of the system. In this step, the system purpose, behavior and requirements are captured.
  Requirements can be:
  - Data collection requirements.
  - Data analysis requirements.
  - System management requirements.
  - User interface requirements.

2) Process Specification:-

- The use cases of the IoT system are formally described based on or derived from the purpose and requirements specifications.

3) Domain Model Specification:-

- The domain model describes the main concepts, entiti and objects in the domain of the IoT system to be designed.
- Domain model defines the attributes of the objects and relationships between objects.
- Using domain model, system designers can get an understanding of the IoT domain for which the system is to be designed.

4) Information Model Specification:

- Information model defines the structure of all the information in the IoT system.
- Does not describe how the information is stored and represented.
- To define the information model, we first list the virtual entities.
- Later more details like attributes and relationships are added.

5) Service Specifications:

The service specifications defines the following:
- Services in the system
- Service types
- Service Inputs/output
- Service endpoints
- Service schedules
- Service preconditions
- Service effects.

- For each state and attribute in the process specification and information model, we define a service.

6) IoT level Specification:

- Based on the requirements we will choose the IoT application deployment level.

7) Functional View Specification:

- The Functional view defines the functions of the IoT systems grouped into various functional groups.
- Each Functional group provides functionalities for interacting with concepts in the domain model and information related to the concepts.
- The functional groups in a functional view include: Device, Communication, Service, Security, Management, Application.

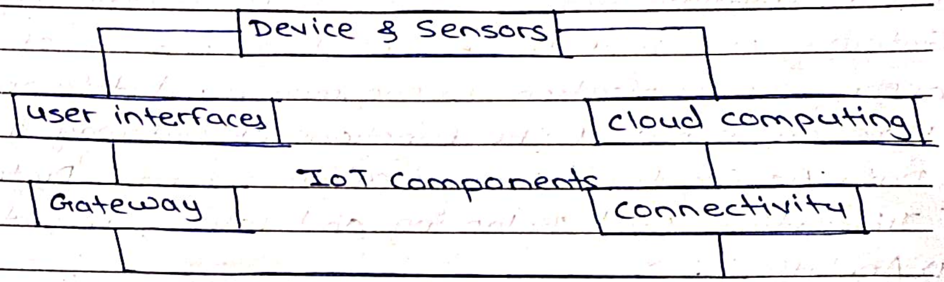
8) Operational View Specification
- In this step, various options related to the IoT syste deployment and operation are defined, such as:
- Service hosting options
- Storage options
- Device options
- Application hosting options.

9) Device and Component Integration:
- In this step the devices like sensors, computing devices and other components are integrated togethe

10) Application Development:
- Using all information from previous steps, we will develop the application (code) for the IoT system.

* Basics of IoT Networking:
- Several network protocols are commonly used for IoT devices. These includes Wi-Fi, Bluetooth, Zigbee LoRaWAN
- Each protocol has its own advantages and disadvantages
- After setting up the network infrastructure, it is necessary to configure the devices.

* Networking Components:-
1) Device & Sensors
2) Cloud Computing
3) User interface
4) Networking connection.
5) Gateway.



1. Device & Sensors:-
- Connectivity layer components are devices & sensors
- These smart sensors continuously collect data from the environment and transmit it to the next layer.
- The latest techniques in semiconductor technology permit intelligent micro-sensors to be formed for different applications.
- Some common sensors are as follows:
- RFID tags
- Temperature & thermostats sensors
- Humidity / Moisture level
- Pressure sensors
- Light Intensity detectors
- Proximity detection

2. Cloud computing:
- Cloud in IoT refers to the service that provides the management, storage, and processing of the data that is generated by IoT devices Here are some key aspects of cloud in IoT:
Data storage, Data collection, Security, Connectivity, Integration and cost efficiency.

3) Gateway:

- Gateway is also a device component that basically acts as an intermediate between the sensors and the central cloud. Gateway is one of the essential components of IoT that offers communication, management, and data processing. Here are some of the functions of Gateway in IoT: Data Aggregation, communication, security, Protocol Translation, Load Balancing and latency Reduction.

4) Analytics:-

- This is the crucial component of the IoT that basically harness the potential of IoT.
  In analytics, meaningful insights are analyzed that are generated by IoT devices and sensors.
  There are some functions included in analytics, such as data processing, machine learning, statistical analysis.

5) User Interface:-

- User interface, also known as UI in the IoT and provide an interface by which the users can interact with the applications and systems.
  Here are some of the key points in the user interface of the IoT: Data visualization, user-friendly design, Personalization, remote management, integration, authentication and security.

* Internet Structure:-

- IoT Internet structure covers following points:-
  - Messages travel from source to destination by hopping through networks.
  - It uses Ad hoc interconnection of network.

* Connectivity Technologies:

- Network connectivity is one of the main principal units of an IoT association, alongside information preparing, UI and sensors / gadget.

Mostly, connectivity technologies can be categorized into - wired and wireless.

1. Wired Connectivity: features
- More Expensive
- More cost of damage repairs
- low power consumption
- Higher security
- higher bandwidth
- less affected by the ambient conditions.

e.g. Ethernet, USB cables, HDMI technology.

2. Wireless Connectivity:
- Higher reliability & longevity
- higher power consumption
- higher range
- higher bandwidth.

A) Wi-Fi:-
- Wireless Fidelity is a convenient connectivity option that allows devices to transmit data over the internet without physical cables.
- Advantages of Wi-Fi:-
  - High speed data transfer.
  - Ease of use and setup
  - Strong compatibility
  - Relatively low cost.
  - Widespread availability in homes, offices or public spaces.

Disadvantages of Wi-Fi:-
- Higher power consumption
- Limited range, up to around 35 m
- Network congestion and Wi-Fi source dependency.

2> Bluetooth:

Adv:-
- Low power consumption
- cost-effective implementation
- Ease of use and setup

Disadvantages:-
- low bandwidth
- Slower data transfer. compared to Wi-Fi
- short range
- higher latency.

3> Cellular Networks:-
- Cellular networks (2G, 3G, 4G, 5G, LTE-M & NB-IoT) constitute around 20% of all IoT connections.
- Advantages:-
  - High reliability
  - Scalability
  - Robust security features.
  - high speed and bandwidth
  - Widespread coverage
- Disadvantages:
  - usually high cost
  - high power consumption
  - latency, through 5G reduces delays significantly.

4> Zigbee:-
- Zigbee, an IoT connectivity technology is known for its low-power mesh networking.

Advantages:-
- low power consumption.
- Scalability
- Reliability
- Resistance to other wireless device's interference.

Disadvantages of Zigbee:
- Limited Range, from 10 to 100 meters
- Potential compatibility issues.
- Low bandwidth
- Relatively complex to set up for a regular user.

5> LoRaWAN:-
- Long Range Wide Area Network
- Advantages:-
  - Remarkable range, up to 15 km
  - low power consumption
  - low cost

Disadvantages:-
- low bandwidth
- high latency.

6> Ethernet:-
- The core wired connectivity technology is Ethernet

Adv. of Ethernet:-
- Reliability,
- high speed data transmission
- Noise resistance
- unmatch security

Disadv:
- Cable dependence, range limited to wire length.
- Installation complexity
- Relatively costly.

* Comparision between:-

1) Bluetooth & Wi-Fi

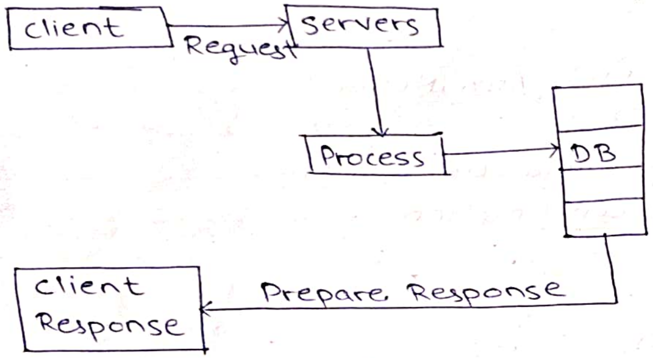
2) Zigbee, Bluetooth, WiFi

* IoT communication Models:-

- Types of communication models:-

A) Request - Response communication model:

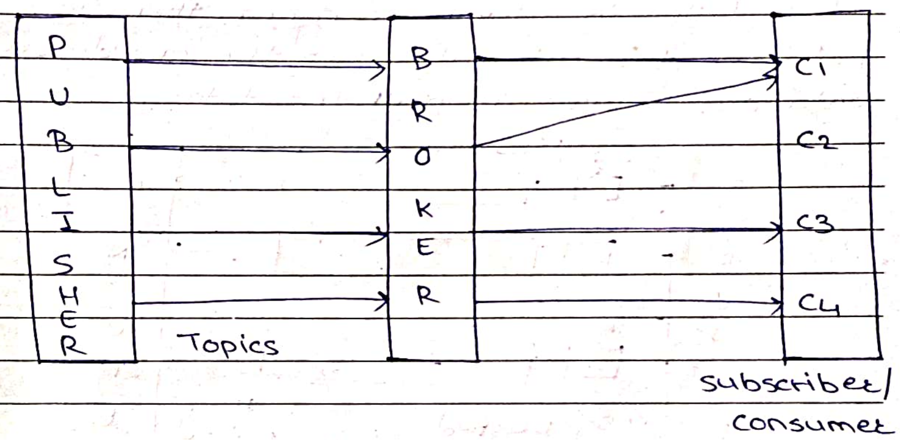
- This model follows a client - server architecture.



- 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.
- 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 retrives resources, and prepares the response, and sends it to the client.

B) Publisher - Subscriber Model:

- This model comprises three entities:
  Publishers, Brokers, 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.

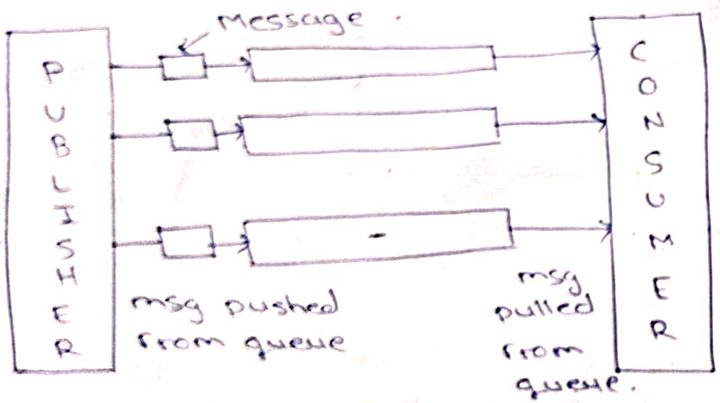


- Consumers subscribe to the topics which are managed by the broker.
- Hence, Brokers responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.

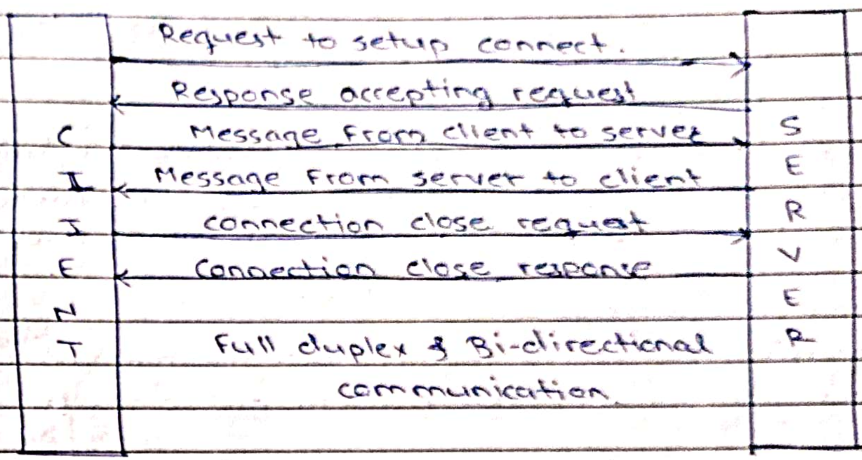
C) Push - Pull Model:-

- 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 procedurers push the data and consumers pull the data.



4) Exclusive Pair :-
- Exclusive Pair is the bi-directional, model including full-duplex communication among client & 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 :- used to communicate bet" server & system in IoT
- There are two IoT communication APIs
1. REST based communication API
2. Web Socket based Communication API

1. REST based communication API :-
- Representational state Transfer (REST) API uses a set of architectural principles that used to design web services.
- These APIs focus on the system's resources that how resource states are transferred using the request-response communication model.
- This API uses some architectural constraints :-

a) Client - Server :-
- The principle behind the client-server constraints is the separation of ~~each~~ concerns.

b) Stateless :-
- Each request from client to server must contain all the information necessary to understand the request.

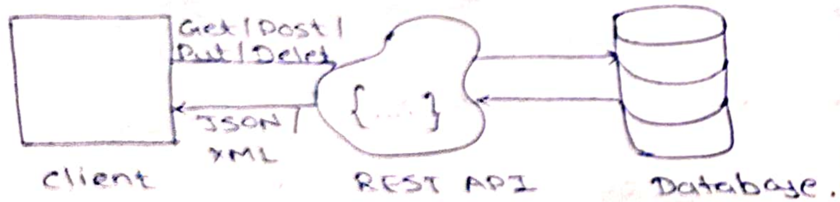
- The session state is kept entirely on the client.

c) Cache-able :-
- Cache constraints require that the data within a response to a request be implicity or explicity labled as cacheable or non-cache-able.

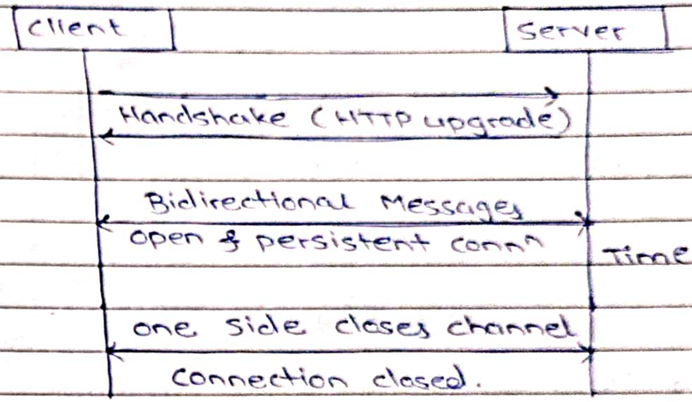
d) Layered System :-
- Layered system constraints, constraints the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting

e) Uniform Interface :-
- Interface constraints require that the method of communication between a client and a server must be uniform.

f) Code on Demand :-
- Servers can provide executable code or scripts for clients to execute in their context.



2) WebSocket-based Communication APIs :-
- WebSocket APIs allow bi-directional, full duplex communication between clients and servers.
- It follows the exclusive pair communication model.
- WebSocket APIs reduce the network traffic and latency as there is no overhead for connection setup and termination requests for each message.



* Four Pillars of IoT :-

* Horizontal Applications of an IoT :-
- Provides solution to common problems
- These are not business specific
- It can be used monitored and controlled by multiple companies.
- Allows multiple providers to work together on a single platform.

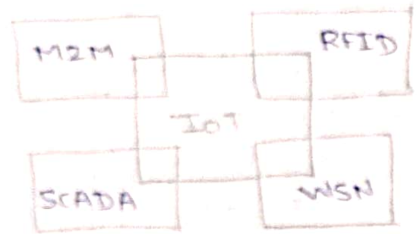
Advantages :-
- Robust
- Developed fast & less costly.

* Vertical Applications of an IoT :-
- These are business specific
- Can be used monitored and controlled by only single company
- Does not allow multiple providers to work together on a single platform

Advantages :-
- No compatibility issue as no other companies are involved.

- Disadvantages:
- Depended entirely on a single vendor for modifications or upgrades

* Four Pillars of IoT:



I) M2M - Machine to Machine
- It is a subset of an IoT.
- Enables flow of data between machines which monitor data by means of sensors and at other end extracts the information on gathered data and processes it.
- It uses WAN, GPRS, Cellular and fixed N/w's.

M2M Architecture:
- Components of M2M architecture are:
1) M2M Devices
2) M2M Area Network i.e. Device Domain
3) M2M Gateway
4) M2M communication N/w's : Network Domain
5) M2M Applications i.e. Application Domain

1) M2M Devices:
- Device that are capable of replying to request for data contained within those devices or capable of transmitting data autonomously are M2M Devices.
- Sensors and communication devices are the endpoints of M2M applications.

2) M2M Area Network:
- It provide connectivity between M2M Devices and M2M Gateways.
- e.g. Personal Area Network (PAN)

3) M2M Network Domain:
- It provides communication between M2M Gateways and M2M applications.
- e.g. WiMax, WLAN, LTE

4) M2M Application Domain:
- It contains the middleware layer where data goes through various application services and is used by the specific business - processing engines

II RFID:
- Radio Frequency Identification:
- It uses radio frequency to read and capture information stored on a tag attached to an object.
- A tag can be read from up to several feet away and does not need to be within direct line of sight of the reader to be tracked.
- It uses NFC (Next field Communication Protocol).
- IC (Integrated circuit) cards, Radio waves

RFID System

- RFID Reader
- RFID tag
  - Active tag
  - Passive tag
  - Semi Passive tag

* RFID Tags

RFID Passive tags:-

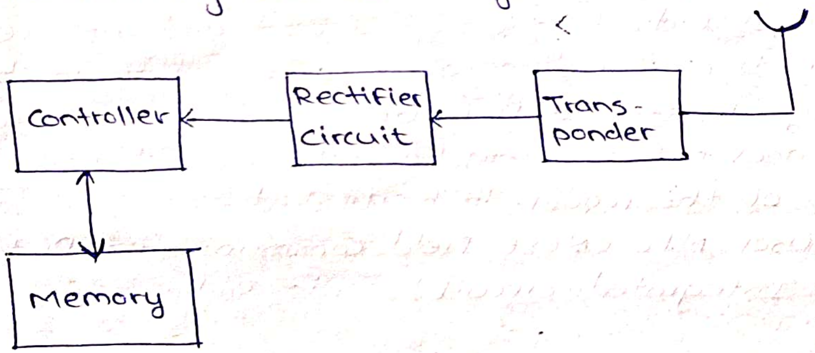
- Passive tags are cheaper
- Passive tags do not use any power source hence they are compact.

RFID Semi Passive tags:

- Semi Passive Tag have their own power supply, but for transmitting back they rely on signals coming from RFID Reader.

RFID Active tags:

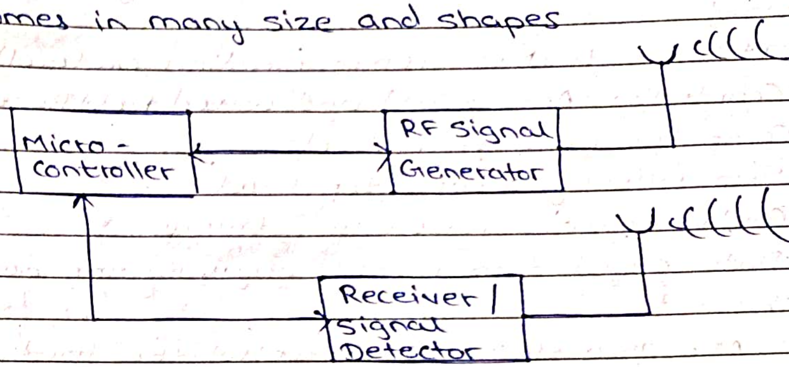
- Active Tag uses their own power supply for both transmitting and receiving.



- Transponder receives signals from reader and sends back feedback to the reader.
- The passive tags use the rectifier circuit to store the energy coming from the radio waves.
- This energy is used as the supply for the controller and the memory element.

* RFID Reader:

- It comes in many size and shapes



- RF Signal Generator generates radio waves which are transmitted through the antenna.
- Receiver or signal detector receives the signals coming from the object.
- And to process these signals microcontroller is used

RFID Frequency operation

LF	HF	UHF
low freq	High freq	ultra high freq
125 kHz to 134 kHz	13.56 MHz	860-960 MHz
Range upto 10cm	Range upto 1m	Range 10 to 15m
used for person identification	clothes at shopping mall	vehicle identification at Toll Plazza.

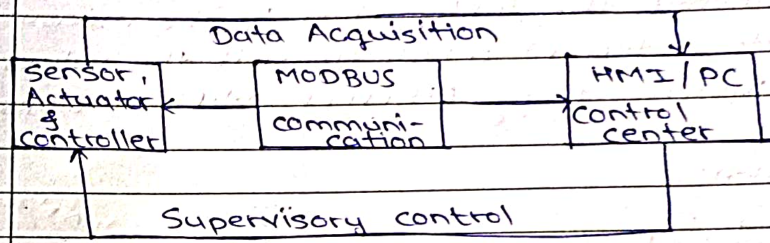
III) SCADA :-

- Supervisory Control & Data Acquisition
- These connect, monitor and control equipment's using short range n/w inside a building or an industrial plant.
- It uses BacNet (communication protocol), CanBus (Controller Area N/w) and wired FieldBuses (Industrial Computer Network Protocols)
- Supervisory means top level
- Control means controlling things.
- Data acquisition means acquiring the data / reading the data.
- SCADA is a s/w used to control the hardware i.e. PLC, drives, servers, sensors and also acquire the data which is stored on the personal computer or Human Machine Interface (HMI)

*SCADA architecture:

- SCADA architecture has a control centre connected to the main hub (i.e. the ethernet port)
- The PLC (Relay Reader is connected to the ethernet board which is overall connected to the CPU.
- PLC on other hand is connected to various Field instruments which can be the temp. sensors or actuators that can be analog or digital
- The PC has a SCADA s/w which can interact with the Field instruments.
- PC is also connected to various other PLC's units I, units II
- There is an Human Machine Interface (HMI) which is individually connected to the PLC.
- The HMI individually monitors and controls the PLC
- To read information from all the units we need a SCADA system.

- PLC (Programmable Logic Unit) monitor and control the data.
- RTU (Remote Terminal Units) receive data from sensors and convert this data to digital data and send to SCADA System.



SCADA Applications:-

- Food processing industry
- chemical industry
- Water Treatment Plant

IV WSN: (Wireless Sensor Network)

- It senses and gathers data using sensors which are spatially distributed.
- It collects this data into a centralized location with the help of wired / wireless connection.
- It is a deployment of several devices equipped with sensors that perform a collaborative measurement process.
- WSN consists of three basic things
  - Sensors to send values
  - Communication model using any protocol
  - API to display data.

* WSN Elements :-

1) Node : Autonomous sensor - equipped device.

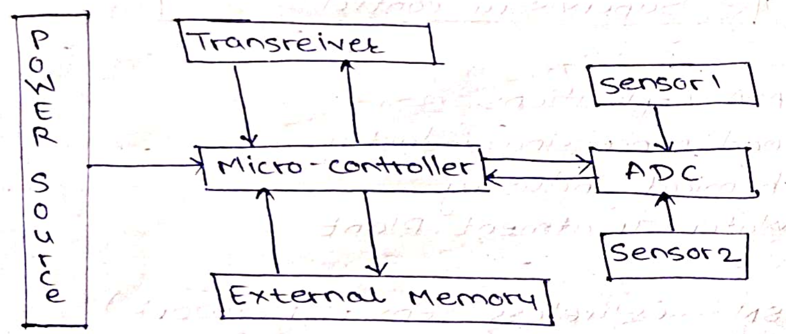
2) Data gatherer - Data capture and gateway to extern systems.

3) External systems - Data storing and managing centres.

* Working of WSN :

- ~~In the above diagram we can~~
- The sensors (nodes) are sensing the device values
- These transmit the information to the measuring device (data gatherer) which transmit the values to external systems using Ethernet, WiFi or GPRS.

Parts of WSN :



* DCM :-

Device - connect - Manage

1) Devices :

Sensors, Actuators

2) Connect :

- The communications layer is the foundational infrastructure of IoT
- There are two major communication technologies
  - wireless
    - → Short Ranged Networks like RFID, NFC, WiMax, WPAN, LAN, MAN etc.
    - → Long Ranged : GSM, CDMA, Cellular, WLAN, Satellitie
  - Wired communication
    - Wired
      - → Short Ranged FieldBus Networks for SCADA
      - → IP based Network for some M2M & SCADA

3) Manage :

- The business value of IoT comes from knowing how, when and where to use the data in value - adding ways.