Unit-1:- Wireless Sensor Networks (WSN)

Basic components of a sensor Node, Types of sensors, constraint in the sensor nodes, characteristics of WSN, Nature of data in Sensor Networks, Manual VS Randomized node deployment, Event aware topology management in WSN, Data dissemination, Aggregation, Virtual Sensor Network, Operating systems for WSN, issues and challenges of WSN, Some applications of WSN.

Unit - I

Basic components of a Sensor Node:- There are typically four main components in a sensor node:

(a) Sensing Unit
(b) Processing Unit
(c) Communication Unit
(d) Power Supply.

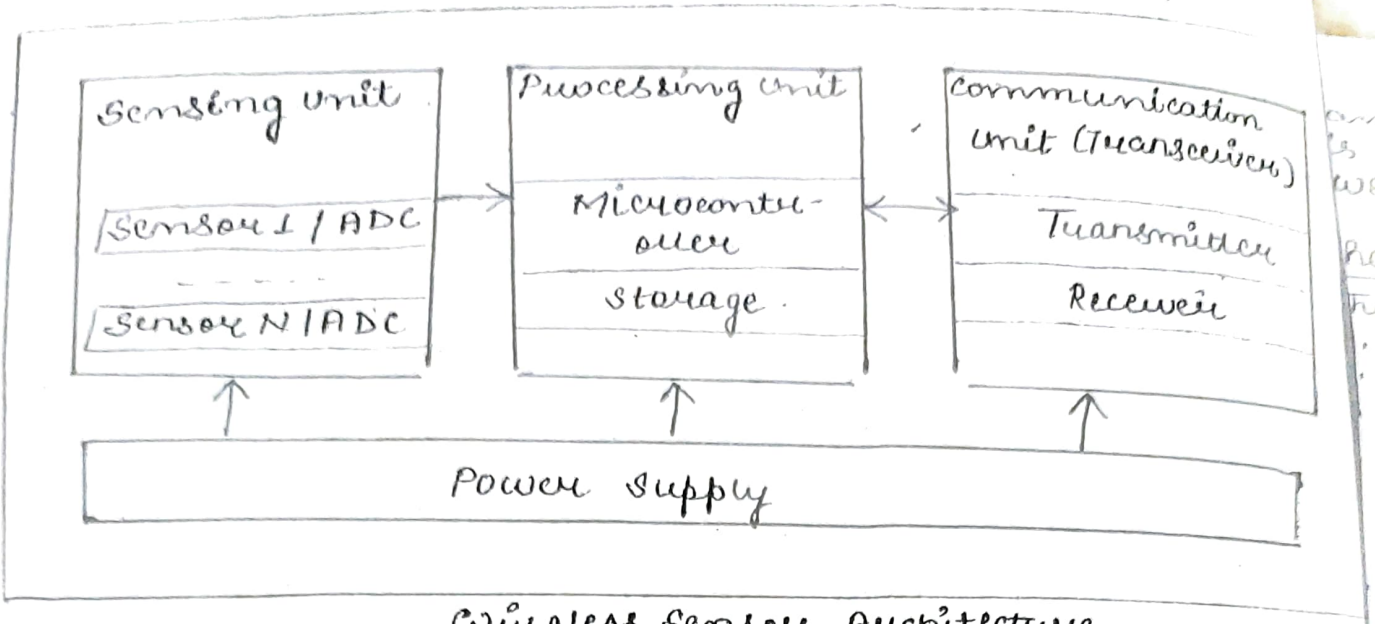
1. Sensing Unit:- Sensors are hardware devices that measure some physical data of the monitored systems such as temperature, humidity, pressure or speed. The analog signals produced by the sensors are digitalized by ADCs and sent to processing unit for further processing.

2. Processing Unit:- Within the processing unit, there is a microcontroller associated with a small storage unit including on-chip memory and flash memory. A processing unit is responsible for performing tasks, processing data and controlling functionality of other components of sensor node.

3. Communication Unit:- A wireless sensor connects with other nodes via the communication unit, where a transceiver encompasses the functionality of both transmitter and receiver. The wireless transmission media may be radio frequency, optical (laser), or infrared.

4. Power Supply:- At present, the main type of power supply for wireless sensor node are batteries, either rechargeable or non-rechargeable. Energy is consumed for sensing, data processing, and communication.

For small wireless sensor nodes, data communication will expend the majority of energy, while sensing and data processing are much less energy consuming.



Wireless Sensor Architecture.

Types of Sensors:-

Sensor:- It is a device that converts signals from one energy domain to electrical domain.

The following is a list of different types of sensors that are commonly used in various applications. All these sensors are used for measuring one of the physical properties like Temperature, Resistance, Capacitance, conduction, Heat Transfer etc.

1. Temperature Sensor
2. Proximity Sensor
3. Accelerometer
4. IR Sensor (Infrared Sensor)
5. Pressure Sensor
6. Light Sensor
7. Ultrasonic Sensor
8. Smoke, Gas and Alcohol Sensor
9. Touch Sensor
10. Color Sensor
11. Humidity Sensor
12. Position Sensor
13. Magnetic Sensor (Hall effect Sensor)
14. Microphone (Sound Sensor)
15. Tilt Sensor
16. Flow and level Sensor
17. PIR Sensor
18. Touch Sensor
19. Strain and weight Sensor

Temperature Sensor:- One of the most common and most popular sensors is the temp. sensor. A temp. sensor senses the temp. i.e. it measures the change in temp.

There are different types of temperature sensors like Temperature Sensor ICs (like LM35, DS18B20), Thermistors, Thermocouples, RTD (Resistive Temperature Devices) etc.

Applications:- computers, mobile phones, automobiles, air conditioning systems, industries, etc.

Proximity Sensors:- A proximity sensor is a non-contact type sensor that detects the presence of an object. Proximity sensors can be implemented using different techniques like optical, sound, Magnetic, capacitive etc.

Applications:- Mobile Phones, Cars (parking sensors), industries (object alignment), Ground Proximity in Aircrafts etc.

Constraints on the Sensor Nodes:-

The individual nodes in a WSN are inherently resource constrained:-

(a) Limited power or energy.
(b) Limited processing speed
(c) Limited storage capacity
(d) Limited communication bandwidth
(e) Limited size node.

Energy:- In WSN energy is the biggest constraint. Energy consumption in sensor nodes can be divided into three parts:-

(i) Energy for the transducer.
(ii) Energy for communication among sensor nodes
(iii) Energy for microprocessor computation.

Power Consumption:- The wireless sensor node are micro-electronic device that can be equipped with very limited power source (<0.5Ah, 1.2V). In some applications, replenishment of power resources might be impossible.

Memory:- Memory of sensor nodes usually consists of flash memory and RAM. Flash memory is used to store downloaded application and RAM is used for storing application programs. There is limited space to run complicated algorithms and application code.

Transmission Range:- Range of communication in sensor nodes is very limited for both technically and by need to conserve energy. The actual range achieved from given transmission signal strength is dependent on various environmental factors such as weather, vibration, humidity, pressure etc.

Higher Latency in communication:- Network congestion, multi hop routing and processing in the intermediate nodes of WSN may give rise to higher latency in packet transmission. So, it is very difficult to achieve synchronization.

Unattended operation of Networks:- Generally, the nodes in WSN

and are left unattended. Detection of physical tampering is virtually impossible due to remote management of a WSN.

Characteristics for WSN:-

The important characteristics of WSN includes-

1. Power consumption limitations for sensor nodes.
2. Ability to cope with failure of nodes.
3. Mobility of nodes
4. Heterogeneity of nodes
5. Homogeneity of nodes.
6. Ability to deploy on a large scale.
7. Capability to survive harsh environmental conditions.
8. Helps to Use easily.

nsor nodes have been defined into two characteristics:-

(a) Static characteristics:- In fact such as smart buildings, physical infrastructure are some applications, where network s stable i.e. static over space. The fixed parts would be connected to continuous power supply, so that wireless parts an use low power to transfer data to them and also nodes can go in standby mode from time to time.

aracteristics:- low cost, small size, low power consumption, flexibility and often privacy and security.

b) Dynamic characteristics:- An active care approach i.e. dynamic works as an 'on-the-fly' based initiating technique that creates a fresh topology where existing one is no longer ideal.

Characteristics:- low power consumption, low levels of physical security and broadcast physical medium

(i) Ad-hoc network like MANET:- MANET means Mobile Ad-hoc Network. It is also known as wireless ad hoc network or temporary wireless network. It usually has a searching path network interacting environment on top of IR layer. They consists of set by mobiles nodes connected wirelessly in a self-configured, network.

llowing are the some common characteristics that need to be considered while using WSN for developing different pplications.

4. Power Efficiency:- The consumption of power limits for nodes with batteries. Many of challenges of Sensor network revolves around limited power resources. The size of nodes limits the size of battery.

5. Low powers- The key to accomplish a longer lifespan for WSN is to design with minimal power consumption of wireless sensor nodes, hence titled "less power".

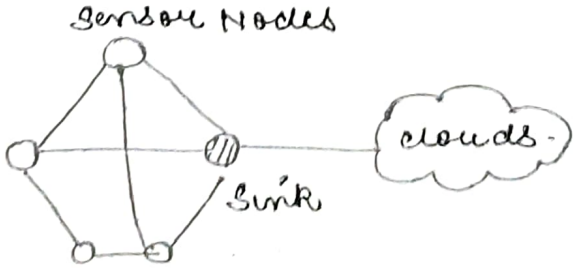
6. Responsiveness:- The Sensor nodes need to become independent to work even in bad situations and portrait responsiveness. WSN works more efficiently if sensor nodes develop characteristics of responsiveness.

7. Reliability:- WSNs involve a no. of sensor nodes with limited processing, storage and battery capabilities. The overall reliability of a WSN is enhanced by reliability of components of node.

8. Data compression:- while designing WSN, it is necessary to reduce amount of energy used for radio transmission, but nodes can use additional energy for computation.

9. Scalability:- A good routing protocol has to be scalable and easily adaptive to changes in network topology.

10. Mobility:- Mobility in wireless Sensor Networks is an element which directly influences the network performance.



WSN.

Nature of data in Sensor Networks:

Manual vs Randomized Node Deployment:-

Node Deployment

- Manual
  - (i) Easy to reach area
  - (ii) Nodes are fixed manually.
- Randomized
  - (i) Hard to reach area.
  - (ii) Nodes are deployed through Helicopter.

Node deployment in WSNs is application-dependent and can be whichever manual or randomized.

In manual placement, the sensors are manually allocated and data is routed across predetermined paths. Though, in random node placement, the sensor nodes are dispersed randomly, crafting an ad hoc routing infrastructure. If the resultant allocation of nodes is not uniform, optimal clustering becomes vital to permit connectivity and enable energy-efficient web procedure.

Event Aware Topology Management in WSN:- (EATM)

(a) It includes monitoring the event.
(b) It means managing/organizing the physical arrangement of nodes.
(c) It is done to conserve energy while maintaining n/w connectivity.
(d) Topology can be organized as per the even.
(e) WSN Topologies: BUS, TREE, STAR, MESH, Circular, RING, Grid

Event aware topology management in WSNs include monitoring the event. Topology Management is managing/organizing the physical arrangement of the mobile nodes in a network. This includes degree of connectivity of the network, transmission power, state, or role of the nodes, etc.

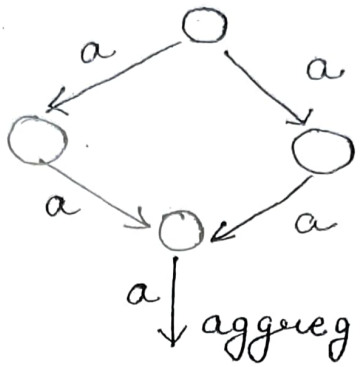
EATM, regularly builds the network topology on the basis the current event state, and the status of the nodes of the network.

ATM splits the network into clusters and uses principles associated with the Facility location Theory concepts n a distributed way to reduce the energy dissipation of event monitoring nodes by reducing their verage transmission distance.

ta Dissemination :-
t is performed from sensor node to the same for data gathering.
t is the process for by which data or queries for data are requested in WSN.
WSNS, it is often necessary to update the software running on sensors, which requires reliable ssemination of large data objects to each sensor ith energy efficiency. During data dissemination, due o sleep scheduling designed for energy efficiency, some sensors may not receive some packets at some ime slots.
the meantime, due to the unreliability of wireless communication, a sensor may not successfully receive packet even when it is in the active node. Thus, etransmission of such packets to those sensors is necessary, which consumes more energy and ncreases the delay of data dissemination cycle.

ata Aggregation :-
SNS consists of large no. of small sized sensor nodes, whose main task is to sense the desired phenomena n a particular region of interest. These networks have rge no. of applications such as habitat monitoring, disaster management, security and military etc. sor nodes are very small in size and have limited processing capability as these nodes have very low attery power WSNS are also prone to the failure, due to low battery power constraint. Data aggregation is in fficient energy technique in WSNS due to high node

by many nodes, which results in redundancy. This redundancy can be eliminated by using data aggregation approach while routing packets from source nodes to base station.



Operating System for WSN:-

OS	Memory Management	Simulation Support	Programming Language
Tiny OS	Static Memory Management	TOSSIM	Nesc.
contiKi	Dynamic	COOJA	C.
MANTIS	Dynamic	through AVRORA	C
Nano-RK	static (support for real-time application)	Not available	C.
Li	Dynamic Memory Management	through AVRORA	Lite C

Applications of WSN:-

1. Military Applications:- WSN is an essential fragment of military intelligence, facility, control, communications computing, frontline surveillance, investigation and targeting systems.

2. Applications in Area Monitoring:- In the aspect, the sensor nodes are positioned over an area where some display is to be observed, the occurrence is conveyed to one of the base stations, which then takes action appropriately.

3. Transport Applications:- Instantaneous traffic statistics is being composed by WSNs to later forage

of possible congestion and traffic difficulties.

4. Industrial Applications:- WSNs have been advanced for "Technological condition-based maintenance (TCBM)" since they could offer momentous cost reductions / investments and allow innovative functionalities.

5. Agricultural Applications:- The employment of WSNs has been reported for assist farmers in various aspects such as the maintenance of wiring in a problematic environment, irrigation mechanisation which aids more resourceful water use and reduction of wastes.

6. Environmental applications:- The term "environmental Sensor Networks. (ESNs)" has developed to cover several benefits of WSNs to environmental and earth science study. This comprises of sensing oceans, seas, glaciers, atmosphere, volcanoes, forest etc.

7. Medical / Health Applications:- Some of the medical / health benefits of WSNs are in the area of diagnostics, investigative, and drug administration as well as management, integrated patient monitoring and monitoring medical practitioners.

8. Structural applications:- WSNs can be employed for monitoring and the development of diverse structural projects. Like flyovers, bridges, roads, tunnels etc, allowing engineering practices to monitor possessions without necessarily visiting the sites.

Issues and challenges with WSN:-

Issues Related to WSN:-

1. Design Issues:-

(a) Fault-tolerant communication:- Due to deployment of sensor nodes in an uncontrolled or harsh environment. it is not common for sensory node to become faulty and unreliable.

(b) Low latency:- The events which the framework deals with are urgent which should be recognized immediately by operator.

(c) Scalability:- A system, whose performance improves after adding hardware, proportionally to the capacity added, is said to be scalable system.

(d) Transmission Media:- In a multi-hop sensor network, communicating nodes are connected by wireless medium.

(e) Coverage problems:- One fundamental problem in WSN is coverage problem, which reflects the quality of service that can be provided by particular sensor network.

2. Topology Issues:-

(a) Geographic Routing:- Geographic routing is a routing principle that relies on geographic position information.

(b). Sensor Holes:- The task of identifying holes is especially challenging since typical WSN consists of light weight, low capability nodes that are unaware of geographic location

(c) Coverage Topology:- Coverage problem reflects how well an area is monitored or tracked by sensors.

3. Other Issues:-

(a) Hardware and OS for WSN (b) Medium Access schemes (c) Deployment (d) Localization (e) Calibration (f) Synchronization (g) Network layer (h) Transport layer (i) Architecture (j) Middleware

Challenges Related to WSN

Challenges in Real-time:-
WSN deal with real world environments, In many cases, sensor data must be delivered within time constraints so that appropriate observations can be made. actions taken. Most protocols either ignore real-time or simply attempt to process as fast as possible.

Challenges in power management:-
Low-cost deployment is one acclaimed advantage of sensor networks. Limited processor bandwidth and small memory are two arguable constraints in sensor networks, which will disappear with development of fabrication techniques.

Management at a Distance:-
Sensor nodes will be deployed at our door field such as a subway station. It is difficult for managers and operator to manage the network directly.

Virtual Sensor Network (VSN)

VSN is an emerging form of collaborative wireless sensor network In contrast, to early wireless sensor networks that were dedicated to a specific application, VSNs enable multi-purpose, collaborative and resource efficient WSNs. The key diff. of VSNs is the collaboration and resource sharing.

VSN can be formed by providing logical connectivity among collaborative sensors. VSNs are expected to provide the protocols to support form formation, usage, adaptation and maintenance. subset of sensor collaborating on a specific task(s). Thus VSNs make use of intermediate nodes, networks, or other VSNs to efficiently deliver messages across members of a VSN.

Applications:-
Geographically overlapped applications:- Eg: monitoring rock slides and animal crossing within a mountainous terrain.
Advantage:- saving in hardware cost.
while logically separating multi-purpose networks:- Eg:- smart neighbourhood

3. In certain dedicated but dynamic applications:-

Eg:- To enhance efficiency of a system that track dynamic phenomena such as subsurface chemical plumes that migrate, split, or merge.

Advantage:- ability to connect right set of nodes at right time.

Unit-2.

Internet of Things: (IOT):- Physical Design of IOT, logical Design of IOT, IOT enabling Technologies, M-2-M communication, Difference B/w IOT and M2M, Software Defined Networking, SDN for IOT, Network function Virtualization, Interoperability in IOT, Issues and challenges with IOT, some applications of IOT.

Machine to Machine communication:

M2M is a broad level that can be used to describe any technology that enables networked devices to exchange information and perform actions without manual assistance of humans.

5 Helps the devices to connect

IoT needs end to end but end to end does not need IoT

Helps in data sharing and data analytics.

M2M use point to point communication b/w machines, sensors over cellular or wired networks while IoT system rely on IoT based networks.

M2M are often isolated and standalone network equipment

IoT system take M2M to the next level bring together into one large connected ecosystem.

7 The main purpose of M2M is to tap into sensor data and transmit it to a network.

Applications:- Remote Monitoring, billing, robotics, security, automotive, traffic control, telemedicine, utilities, industrial and manufacturing.

8

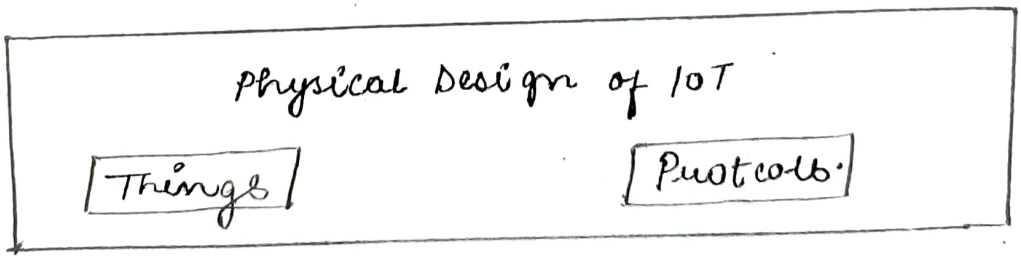
Difference b/w IoT and M2M:-

	IoT	M2M
Abbreviation:-	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making.	Some degree of intelligence is observed in this.
Connection Type Used	The connection is via Network and using various communication types.	The connection is a point to point.
communication protocol used	Internet protocols are used such as HTTP, FTP and Telnet.	Traditional protocols and communication technologies are used.

Data Sharing	Data is shared b/w other applications that are used to improve the end-user experience	Data is shared with only the communication parties.
Internet	Internet connection is required for communication	Devices are not dependent on the internet limited scope for devices.
Scope	A large no. of devices yet scope is large.	
Business Type used	B2B and B2C	B2B.
Open API support	Support open API Integrations.	There is no support for open APIs.
Examples	Smart wearables, Big Data and Cloud, etc.	Sensors, Data and Information etc

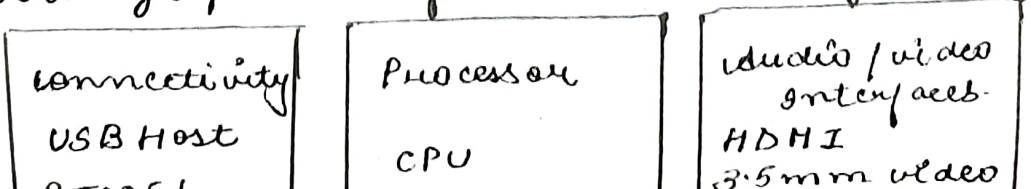
Physical Design of IOT

The physical design of an IOT system is referred to the things/devices and protocols that used to build an IOT system. All these things/devices are called Node Devices and protocols are used to establish communication b/w the node devices and server over the internet.



Things/devices

Things/devices are used to build a connection, process data, provides interfaces, provide storage, and provide graphic interfaces in an IOT system.



Memory Interfaces	Graphics	Storage Interfaces	I/O Interfaces.
NAND/NOR	GPU	SD	UART
SRI/DDR2/ DDR3		MMC	SPI
		SDIO	I2C
			CAN

Connectivity:-
Devices like USB Host and Ethernet are used for connectivity b/w the devices and server.

Processor:-
A processor like CPU and other units are used to process the data.

Audio/Video Interfaces:-
An interface like HDMI and RCA devices is used to record audio and videos in a system.

Input/output Interface:-
To input and output signal to sensors, and actuators we use things like UART, SPI, CAN, etc.

Storage Interfaces:-
Things like SD, MMC, SDIO are used to store the data generated from an IOT device.

IOT Protocols:-
These protocols are used to establish communication b/w a node devi and server over the internet. It helps to send commands to an IOT device and receive data from IOT device over the internet.

Application layer			
HTTP	CoAP	WebSockets	
MQTT	XMPP	DDS	AMQP
Transport layer			
TCP		UDP	
Network layer			
IPv4	IPv6	6LoWPAN	
Link layer			
802.3 - Ethernet		802.16 - WiMax	
802.11 - WiFi		2G/3G/LTE - Cellular	

Application layer protocols:-
In this layer, protocol defines how data should be sent over the network with the lower layer protocols using application interface.

(a) HTTP:- Hypertext transfer protocol is a protocol that presents in an application layer for transferring media documents.

(b) Websocket:- This protocol enables two way communication on b/w a client and a host that can be run on a untrusted code in a controlled environment.

(c) MQTT:- It is a M2M connectivity protocol that was designed as a public messaging transport.

Transport layer:-
This layer is used to control the flow of data segments and error control handling.

(a) TCP:- TCP is a protocol that defines how to establish and maintain a network that can exchange data in proper manner.

(b) UDP:- a user datagram protocol is a part of internet protocol called connectionless protocol.

Network layer:-
This layer is used to send datagrams from source network to destination network.

(a) IPv4:- This is a protocol address that is unique and numerical label assigned to each device connected with network.

(b) IPv6:- It is a successor of IPv4 that uses 128 bits for an IP address.

Link layer:-
Link layer protocols are used to send data over network's physical layer.

(a) Ethernet:- It is a set of technologies and protocols are used primarily in LANs.

(b) WiFi:- It is a set of LAN protocols and specifies the set of media access control and physical layer protocols.

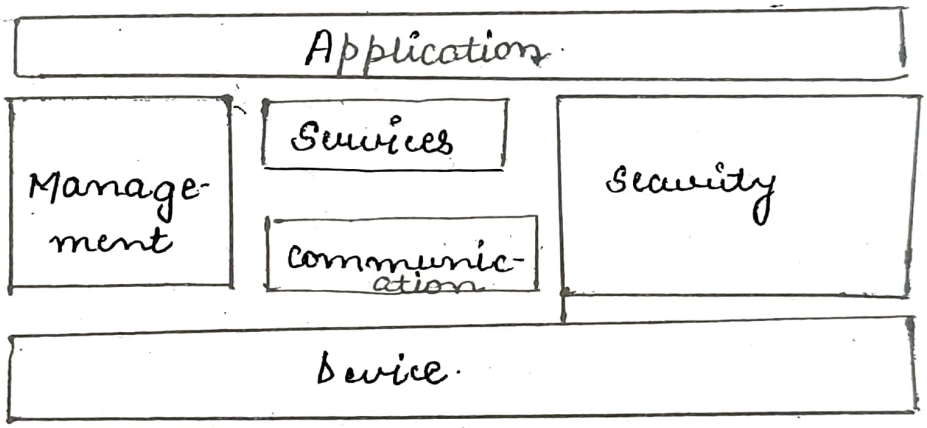
Logical Design of IOT.

The logical design of an IOT system refers to an abstract representation of entities and processes without going into the low-level specifics of implementation. It uses functional BLOCKS, communication Models, and communication APIs to implement a system.

Logical design of IOT

→ IOT functional BLOCKS
→ IOT communication Models
→ IOT Communication APIs.

1. IOT functional BLOCKS:-
An IOT system consists no. of funational blocks like devices, services, security, and application that provides capability for sensing, communication and management.



(a) Application:- It is an interface that provides a control system that is used by users to view status and analyze system.

(b) Management:- This functional block provides various functions that are used to manage an IOT system.

(c) Services:- This functional block provides some services like monitoring and controlling a device.

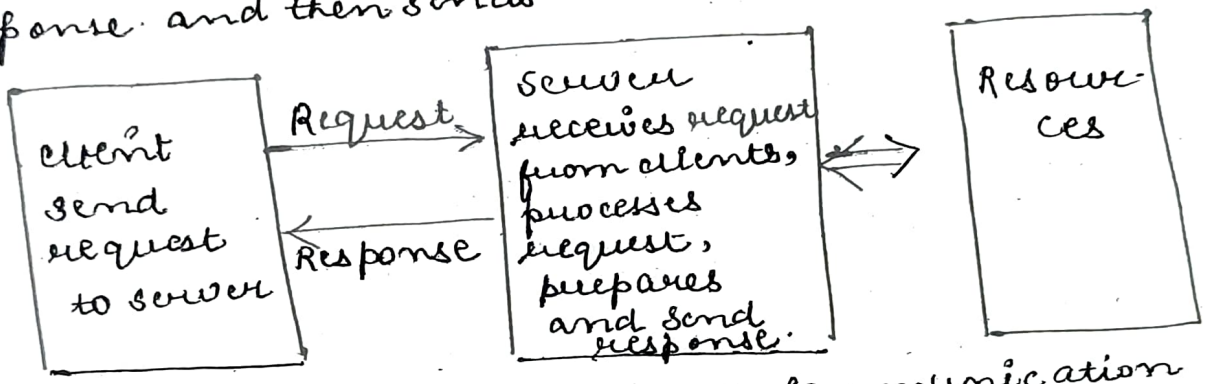
(d) Communication:- This block handles the communication b/w the client and cloud-based server.

(e) Security:- This block is used to secure an IOT system using authorization, data security.

(f) Devices:- These devices are used to provide sensing and monitoring control functions.

2. IOT communication models:-
There are several diff. types of models available in an IOT system that used to communicate b/w the system and server.

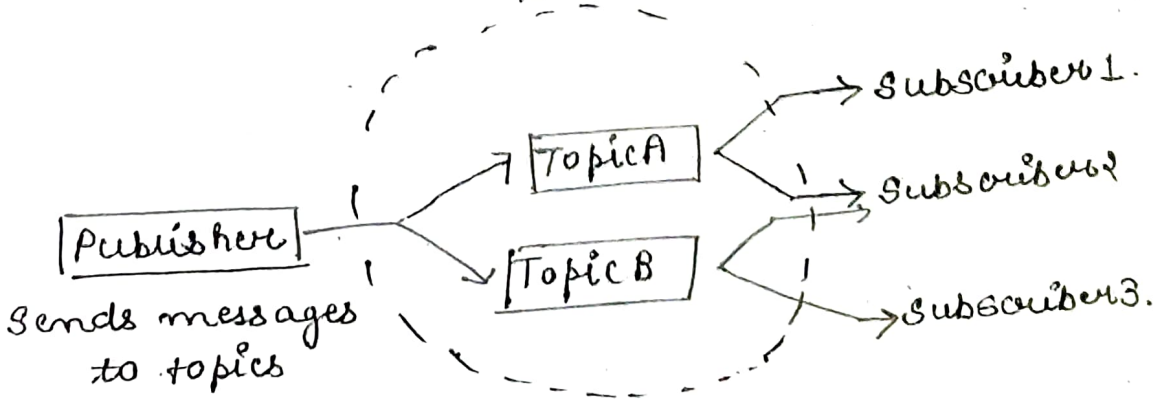
(a) Request - Response communication Model.
This model is a communication model in which client sends the request for data to the server and the server responds according to the request. when a server receives a request, it fetches the data and retrieves its resources and prepares the response and then sends data back to client.



Request - Response communication Model

In this model, HTTP works as request-response protocol b/w client and server.

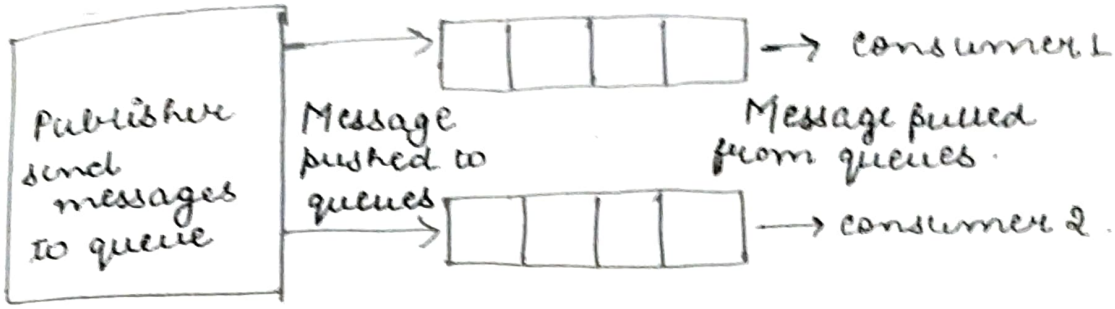
(b) Publish - Subscribe communication Model
In this model, we have a broker b/w publisher and consumer. Here, the publishers are source of data but they are not aware of consumers. They send the data managed by brokers. and when consumers subscribe to a topic that managed by the broker and when they broker receives data from publisher, it sends data to all subscribed consumers.



Publish - Subscribe communication Model.

Push-pull communication Model

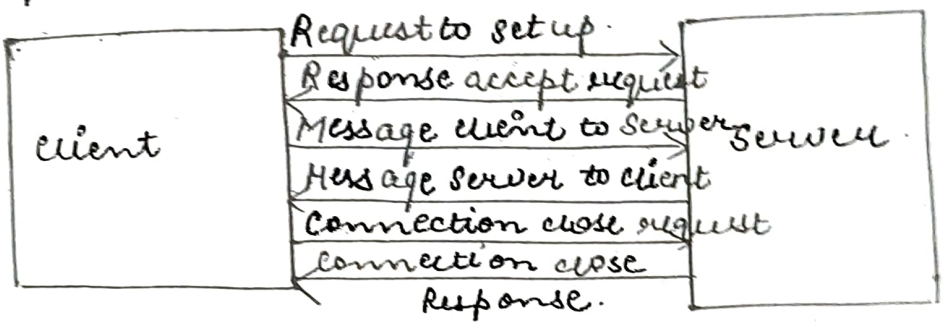
It is a communication model in which the data push by the producers in a queue and the consumers pull the data from the queues. Here also producers are not aware of the consumers.



Push Pull Model

Exclusive Pair communication Model.

It is a bidirectional fully duplex communication model that uses a persistent connection b/w the client and server.



Exclusive Pair communication Model

3. IoT based communication APIs

These APIs like REST and WebSocket are used to communicate b/w the server and system in IoT.

① REST-based communication APIs:-

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

(a) client-server

(b) Stateless

(c) Cacheable

WebSocket based communication APIs - This type of API allows bi-directional full duplex communication b/w server and client using exclusive pair communication model. This type of API reduces the traffic and latency of data.

Software Defined Networking (SDN)

SDN is an emerging architecture that is dynamic, manageable, cost-effective and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The openflow protocol is a foundational element for building SDN solutions.

The SDN architecture is:-

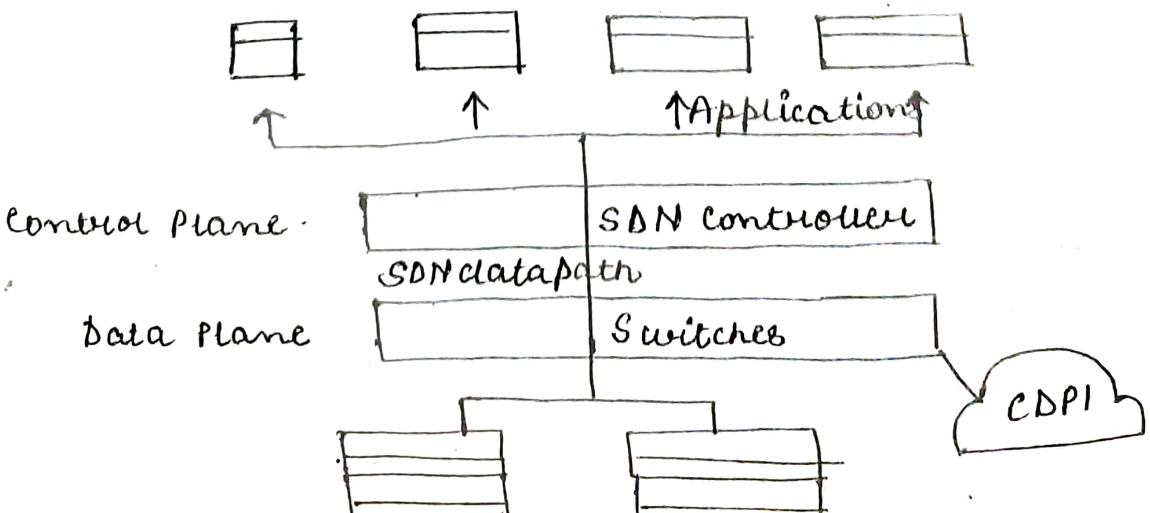
(i) Directly Programmable:- Network control is directly programmable because it is decoupled from forwarding functions.

(ii) Agile:- Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.

(iii) Centrally-managed:- Network intelligence is centralized in software based SDN controllers that maintain a global view of the network.

(iv) Programmatically configured:- SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs.

(v). Open Standards-based and Vendor-Neutral:- When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers.



Interoperability in IOT.

IOT is an ever-growing network of physical devices embedded with sensors, actuators and wire-less connectivity to communicate and share their information among themselves. The application of IOT is in diverse areas such as agriculture, poultry and farming, smart city, and health care, where a sensor node must support heterogeneous sensors/actuators, and varying types of wireless connectivity.

Interoperability is the ability of two or more objects/devices, systems, platforms or networks to work in conjunction.

Interoperability enables communication b/w heterogeneous devices or system in order to achieve a common goal. However, the current devices and systems are fragmented with respect to the communication technologies, protocols, and data formats. The utility of IOT network is limited by the lack of interoperability.

We work towards achieving and implementing interoperability in IOT based systems and environment. We propose solutions to enable seamless integration of peripheral with IOT device towards building a global IOT network of heterogeneous sensors and actuators.