Introduction To Internet Of Things

Course Outcomes:-

CO1 : Describe the evolution of IOT, IoT networki - ng components and addressing strategies in IOT

CO2 : Classify various sensing devices and actuat - ors types.

CO3 : Demonstrate the processing in IOT.

CO4 : Explain Associated IOT Technologies.

CO5 : Illustrate architecture of IoT applications.

Book :- "Introduction to IoT", Sudip Misra, Anandarup Mukherjee, Arijit Roy, Cambridge University press 2021.

MODULE - 1

Basics Of Networking - Introduction
Network Types
Layered N/w Models

Emergence of IoT - Introduction
Evolution of IoT
Enabling IoT & the complex interdependence of Technologies,
IoT Networking Components.

Basics of Networking :-

Today's world relies on data and networking which allows for the instant availability of information from anywhere on the earth at any moment.

Network :- Connection of computers and communication devices which interconnect through a N/w may be Internet or Intranet and are separated by unique device Identifiers (IP address, Internet protocol, Media access control, MAC address).

These computers or communication devices are also called hosts are connected by a single path or multiple paths for sending & receiving data.

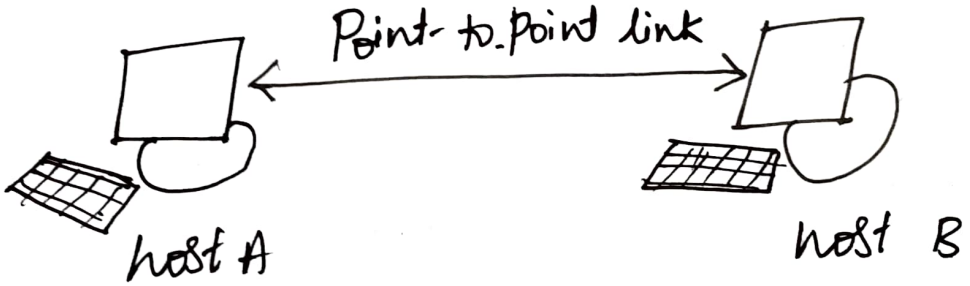
The data transferred between nodes may be text, images or videos which are typically in the form of binary bit streams.

Network Types :-

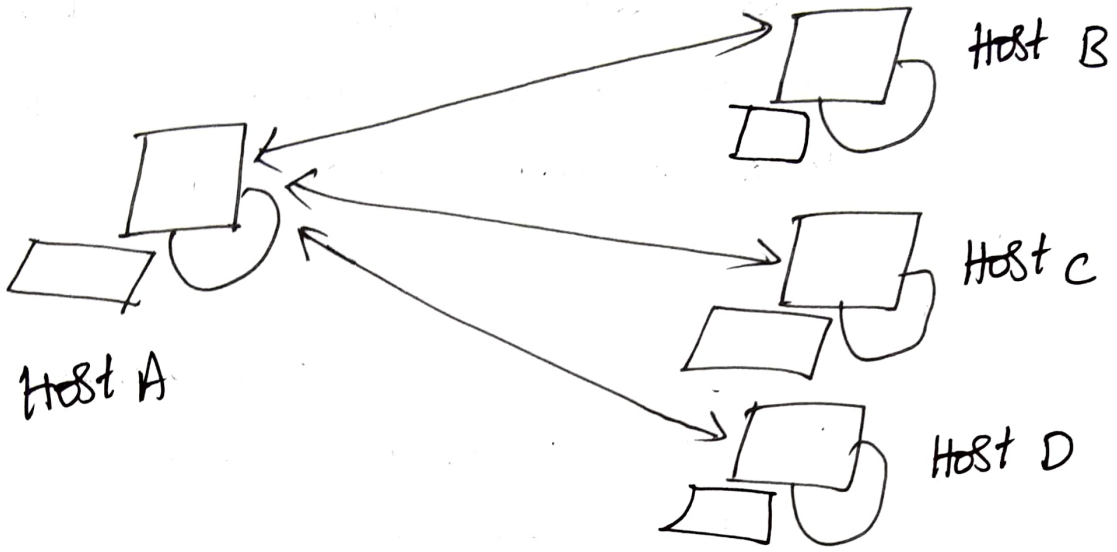
Computer networks are classified according to various parameters like Type of connection, Physical Topology and Reach of Network. These classifications helps in deciding requirements of a n/w setup and provide insights into appropriate selection of a n/w type for the setup.

Based on Connection Type n/ws are classified into point-to-point and point-to-multipoint types.

1) Point-to-Point :- These connections are used to establish direct connection b/w two hosts. These networks are designed to work over duplex links and are functional for both synchronous as well as asynchronous systems. These type of connections find usage for specific purpose such as optical networks.



Point-to-Multipoint : In this type of connection, more than two hosts share the same link. The channel is shared between the various hosts, either spatially or temporally. Common Scheme for spatial sharing is Frequency Division Multiple Access (FDMA) and temporal sharing is Time Division Multiple Access (TDMA). These type of connections find use in present-day networks like wireless networks and IP telephony.



Based On Physical Topology :- Deperding on the Physical manner in which communication paths blw hosts are connected Computer networks can have four brood topologies.

Star :- In star topology

→ every host has a point-point link to Central controller & hub

→ host can communicate only through hub

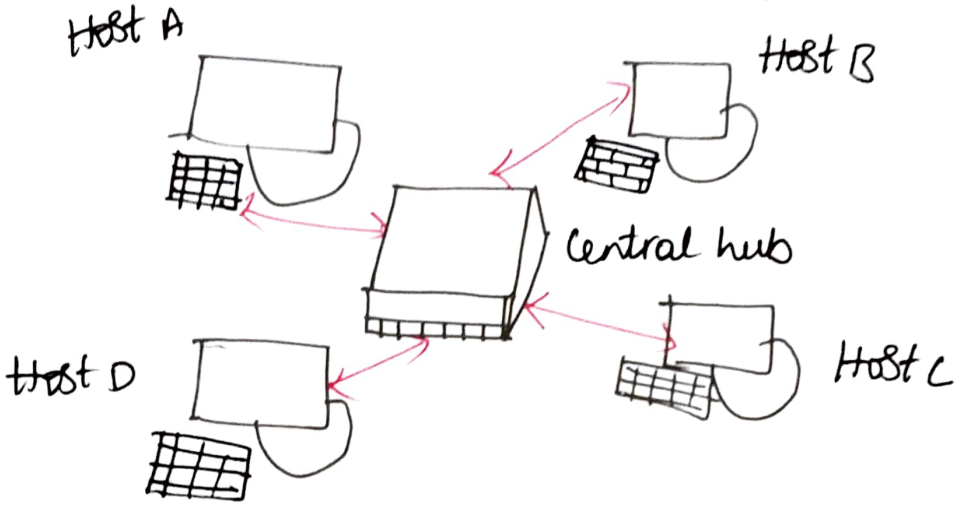
→ hub acts as N/w traffic exchange and essentially be powerful to handle all traffic through it for large scale systems.

→ As fewer links are present cost is less and easy to set up.

→ easy to identify fault in N/w

→ link failure b/w host and hub do not have big effect on N/w

→ Main disadvantage of this topology is the danger of a single point of failure, if the hub fails whole N/w fails.



Mesh :- In Mesh topology

→ Every host is connected to every other host using a dedicated link.

→ for n hosts in the N/w, $n(n-1)/2$ links between hosts are present.

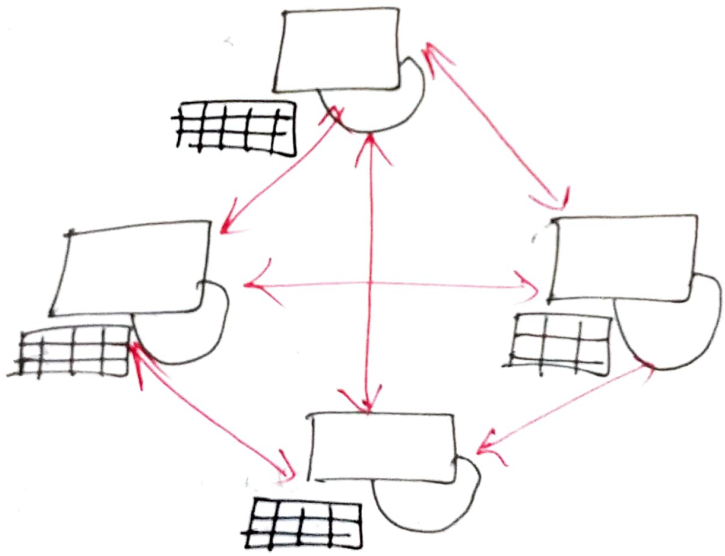
→ This makes the mesh topology expensive.

→ Even if a link is down or broken, the N/w is still fully functional as there remain other pathways for the traffic to flow hence N/w is robust & resilient.

→ The data is only seen by intended recipi - ents and not by all members of N/w hence N/w offers security & privacy.

→ load on each host is reduced as each host in N/w takes care of traffic

→ Owing to complexities in forming Physical connections and cost of establishing links Mesh networks are used selectively such as in backbone networks.



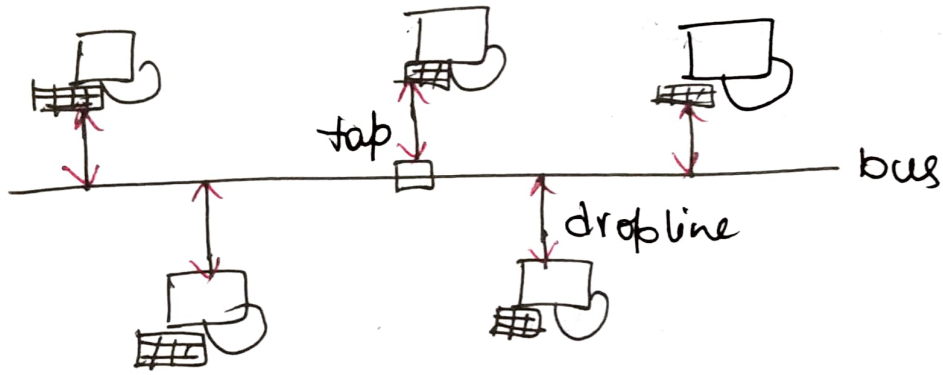
Bus:- In Bus topology

→ A backbone cable or bus serves as the primary traffic pathway b/w the hosts.

→ hosts are connected to bus employing drop lines or taps.

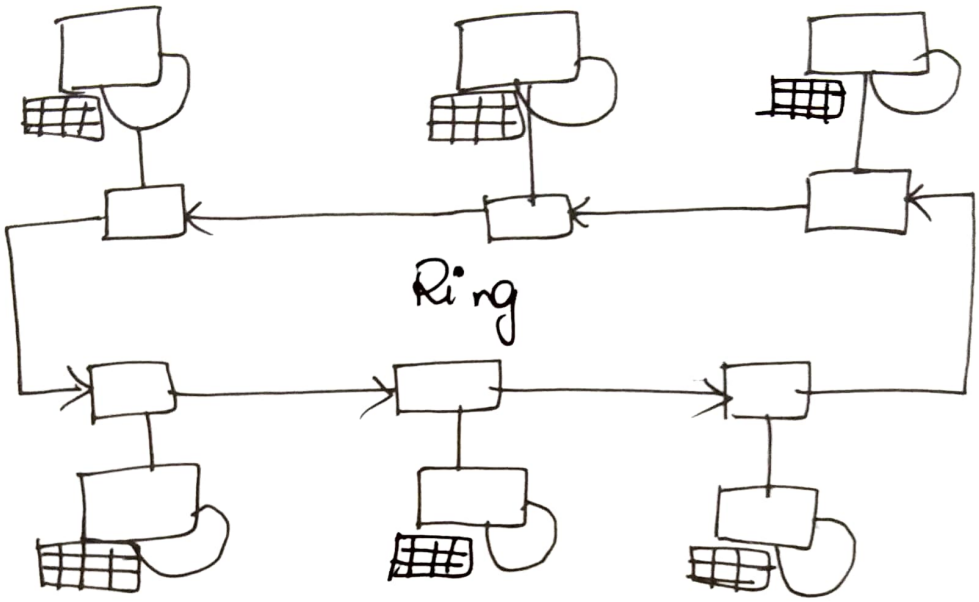
→ Installation is easy and cheap.

→ There is restriction on length of bus and number of hosts that can be connected due to signal
→ fault localization is difficult in the N/w.
→ It works with point to multipoint connection



Ring :- In Ring topology
→ Each host is configured to have Point-to-point connection with its 2 immediate neighboring hosts through repeaters at each host.
→ Repeaters at each host capture the bit stream, regenerates and passes it to next repeater.
→ Fault identification and set up of ring topology is simple & straight forward.
→ High probability of single point failure

→ Even if one repeater fails whole n/w goes down.



Comparision of n/w topology :-

Topology	Feature	Advantages	Disadvantages
Star	Point-to-Point	Cheap, ease of installation & fault identification	Single point failure, traffic visible to n/w entities
Mesh	point-to-point	Resilient against single point failure, Scalable, privacy & security ensured	costly complex connections
Bus	Point-to-Multipoint	Cheap, ease of installation	length of cable & no of hosts are limited, hard to locate faults

Ring	Point-to-Point	Cheap, ease of installation & fault Identification	Prone to single Point of failure

Based on N/w Reachability:-

Computer N/ws are divided into following 4 categories based on N/w reachability.

1) Personal Area N/w (PAN):-

Generally PANs are wireless N/ws which make use of low-range & low-power technologies such as Bluetooth to make a N/w. Reachability of PAN lies in the range of few centi meters to few meters.

Ex:- Connection of wireless speakers, Headphones, laptops, Smartphones, Keyboards, Printers for individual usage.

2) Local Area N/w (LAN):-

A LAN is a collection of hosts linked to a single N/w through wired or wireless connections. Commonly used N/w components

in a LAN are servers, hubs, routers, switches, terminals and computers. The Area Coverage of LANs are restricted to buildings, organizations or campuses.

3) Metropolitan Area N/W (MAN) :- Typically MANs connect various organizations or buildings with in a given geophic location or city. Networking devices in MAN are modems and cables. They have Moderate tolerance levels.

Ex :- Internet Service Provider (ISP) supplying Internet connectivity to various organizations in city.

4) Wide Area N/W (WAN) :- WANs connect diverse geographic locations. WANs connecting two LANs or MANs use Public Switched Telephone N/W (PSTN) or Satellite based links. Due to long transmission range WANs have more errors and noise during transmission and are very costly to maintain. Fault tolerance of WANs are generally low.

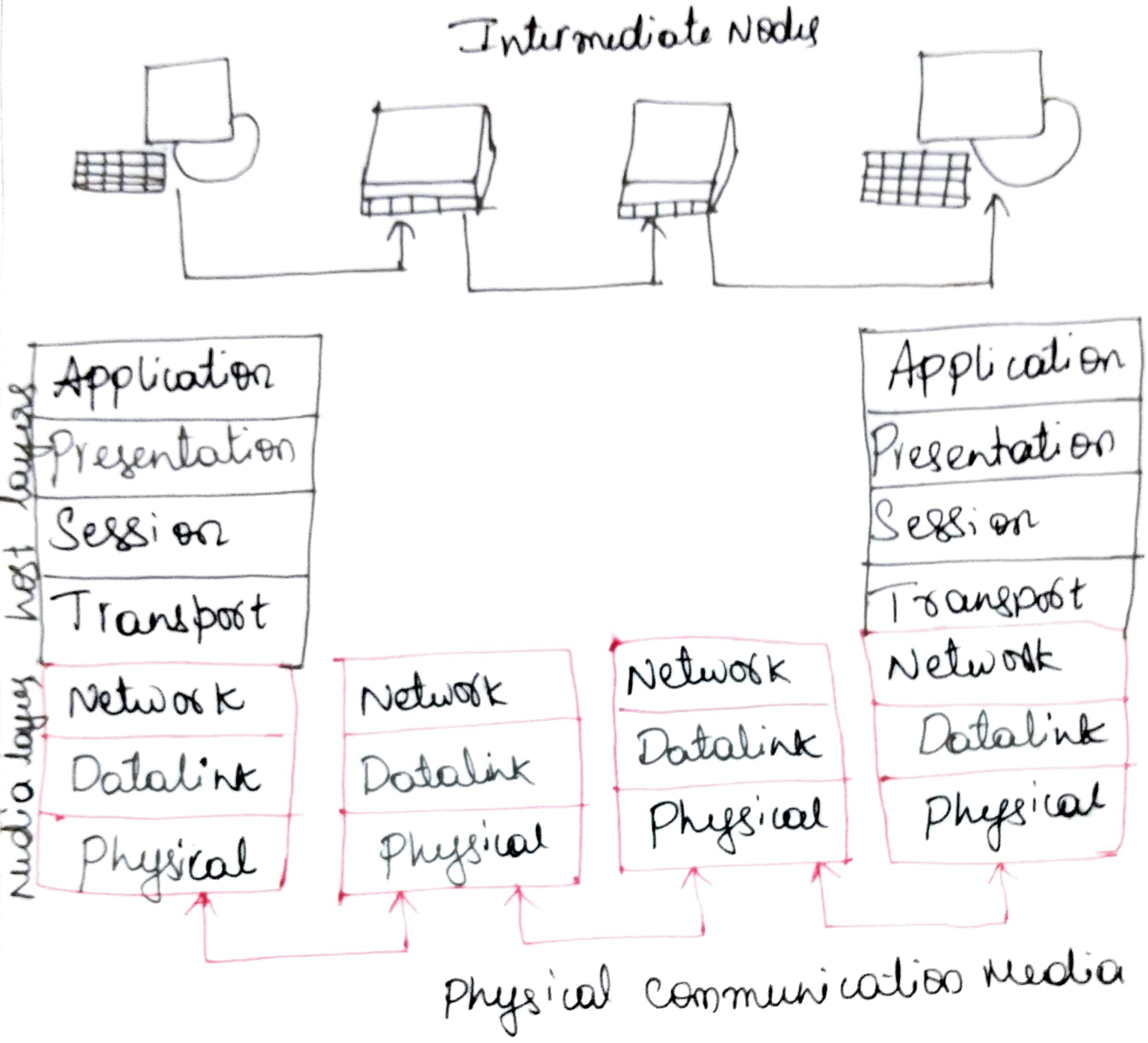
Layered Network Models :-

Intercommunication between hosts is built upon the promise of various task-specific layers. Two of most accepted and used traditional layered N/W models are Open System Interconnection (OSI) developed by ISO and Internet Protocol Suite.

OSI Model :-

The ISO-OSI is a conceptual framework that partitions any networked communication device into 7 layers of abstraction, each performing distinct tasks. These seven layers are Physical layers, Data link layer, Network layer, Transport layer, Session layer, Presentation layer and Application Layer.

A Networked Communication between two hosts following the OSI model is as shown. The Intermediate nodes like routers need to have media layers and host need to have have both media and host layers as shown.



Physical Layer - Layer 1 of OSI model

→ Responsible for taking care of electrical and mechanical operations of host at physical level

→ Electrical operations include signal generation, signal transfer, voltages, layout of cables, line impedance, signal loss, physical port layout, bit rate control operations.

→ This layer is also responsible for topological layout of N/W (Star, mesh, bus or ring) and communication mode (Simplex, half duplex, duplex)

→ Packed Data Unit (PDU) associated with this layer is Symbol.

2) Data link layer :-

→ Media layer & layer 2 of OSI model

→ Concerned with establishment & termination of connection b/w hosts and error detection and correction.

→ This layer is divided into 2 sublayers MAC (Media access control) and LLC (logical link control) sub layer.

→ MAC is responsible of access control of channel (Media)

→ LLC is tasked with error checking, flow control and frame synchronization.

→ PDU associated with this layer is frame.

3) Network Layer :-

→ Media layer and layer 3 of OSI Model

→ Provides means for routing of data packets to various hosts connected to different networks through logical paths called virtual circuits

→ These logical paths pass through other intermediate host before reaching actual destination host.

→ functions of this layer include addressing, sequencing of packets, congestion control, error handling and Internetworking

→ PDU associated with this layer is packet.

4) Transport Layer :-

→ host layer & 4th layer of OSI Model

→ This layer is tasked with end-to-end error recovery and flow control to achive transparent transfer of data between hosts.

→ Keeping track of acknowledgement during data transfer, resending data in case of erroneous transfer or if acknowledgement is not received are responsibilities of this layer.

→ PDU associated with layer is Segment or Datagram.

5) Session Layer :-

→ host layer and 5th layer of OSI model

→ This layer is responsible for establishing, controlling and terminating of communication b/w networked hosts.
→ PDU associated with this layer is Data.

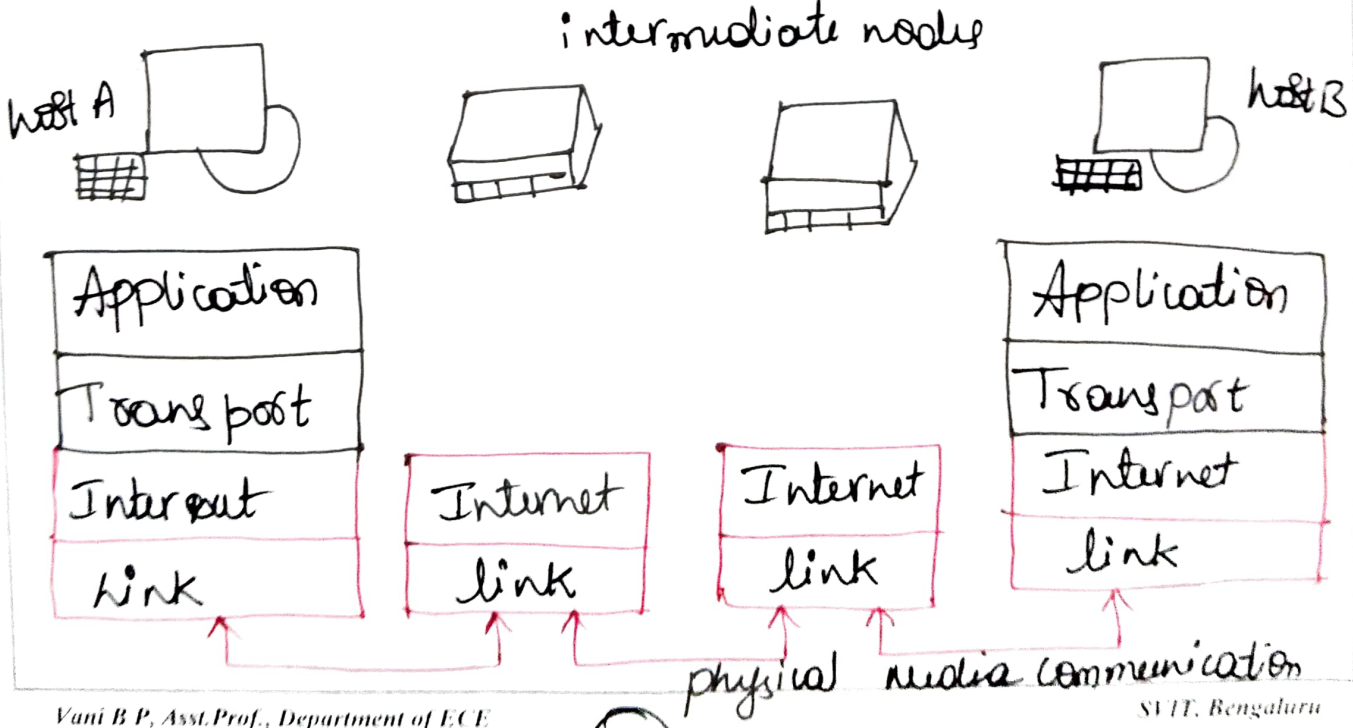
6) Presentation Layer :-
→ host layer & 6th layer of OSI model
→ Also reffered as Syntax layer which is responsible for data format conversions and encryption tasks such that syntatic compatibility of data is maintained across N/w.
→ PDU associated with this layer is Data.

7) Application Layer :-
→ host layer & 7th layer of OSI layer.
→ It is directly accessible by end user through S/W APIs
→ Applications such as file transfer, emails etc are initiated from this layer.
→ This layer deals with Authentication of user, Identification of hosts, Quality of Service (QOS) and Privacy.
→ PDU associated with this layer is Data.

Internet Protocol Suite :-

It is another conceptual framework that provides levels of abstraction for ease of understanding and development of communication and networked system on the Internet. As the foundation technologies of this suite are Transmission Control Protocol (TCP) and Internet protocol (IP) it is also called as TCP/IP suite. The layers of TCP/IP suite are Link layer, Internet layer, Transport layer and Application Layer.

A networked communication b/w two hosts following TCP/IP model is as shown.



Link Layer :-

→ First and base layer of TCP/IP protocol suite also known as N/w interface layer.

→ This layer synonymous with the collective physical and data link layer of OSI model.

→ It enables the transmission of TCP/IP packets over the physical medium.

→ According to its design principles the link layer is independent of medium in use, frame format, N/w access enabling it to be used with wide range of technologies such as Ethernet, wireless LAN, and Asynchro-nous transfer mode.

Internet Layer :-

→ Layer 2 of TCP/IP Protocol suite synonymous to Network layer of OSI model

→ Responsible for addressing, address translation, data packaging, data disassembly & assembly, routing and packet delivery tracking operations.

→ Protocols associated with this layer are ARP, ICMP, IGMP & IP etc.

3) Transport layer :-

→ Layer 3 of TCP/IP Suite functionally synonymous with transport layer of OSI model

→ This layer is tasked with functions of error control, flow control, congestion control, segmentation, addressing in an end-to-end manner.

→ It is independent of underlying N/w

→ TCP & UDP are 2 protocols in this layer which enables choice of providing connection oriented & connectionless services b/w 2 or more hosts.

4) Application layer :-

→ layer 4 of TCP/IP suite and functionally synonymous with collective functionalities of session, presentation & application layer.

→ This layer enables end user to access the services of underlying layers.

→ HTTP, SMTP, FTP, DNS, RIP, SNMP are the core protocols associated with this layer.

Emergance of IoT

Introduction :-

The miniaturization of electronics and the cheap affordability of resulting in surge of connected devices. The total number of connected devices globally is estimated to be around 25 billion. This number is to triple within a sharp span of 5 years by 2025. A huge variety of data is generated from massive number of connected devices. The data may be images, video, music, speech, text, numbers, binary codes, machine states, banking messages, data from sensors, health care data, home automation S/S status & control messages, data from vehicles, military comm and many more.

One of the best example of miniaturization & affordable electronics is evolution of "Smartphones". In 1990's cellular technology was expensive and could be afforded only

by few. Also these devices had only basic features of voice calling, text messaging and sharing low quality multimedia. with in next 10 years this technology has become common and easily affordable. with time features of this device is also evolved and many applications like messaging, Video calling, e-mails, games, music streaming, video streaming are added which works with packet based internet. The device is now called "Smart phone". Inline with this trend, other connected devices are also rapidly increasing, As all technologies and domains are moving toward Smart management systems, location independent access to control & monitor the systems their is further raise in number of Inter-connect -ed devices.

The original "Internet" intended for sending messages is now connected with all sorts of "Things". These things

can be legacy devices, modern-day computers, sensors, actuators, household appliances toys, clothes, shoes, vehicles, cameras etc.

Internet of Things (IOT) is an anytime, anywhere and anything Network of Interconnected physical devices or systems capable of sensing an environment and affecting sensed environment intelligently.

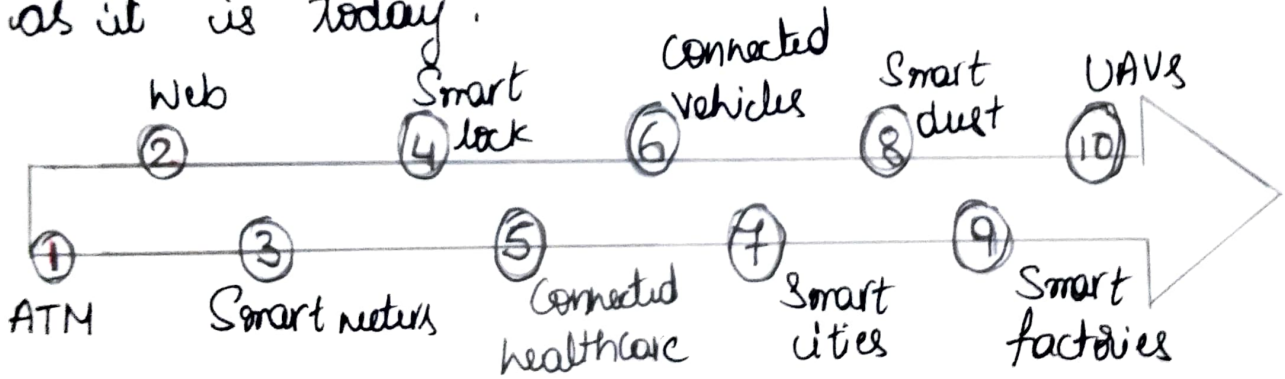
IOT consists of low-power, low form factor embedded processors on board the things connected to Internet either wirelessly or wired connection. Typically, IOT systems are characterized by following features

→ Associated architectures which are efficient & scalable
→ No ambiguity in addressing & naming.
→ Massive number of constrained devices, sleeping nodes, mobile devices & non-IP devices
→ Intermittent & unstable connectivity

Evolution Of IoT:-

The IoT as we see today is a result of a series of technological paradigm shifts over few decades. The technological foundations of connected systems which makes it easy integration to daily lives, popular public acceptance and massive benefits can be considered as founding solutions for the development of IoT.

The following figure shows sequence of technological advancements for shaping IoT as it is today.



ATMs:- Automated Teller Machines are cash distribution machines, which are linked to a user's bank Account.
The concept behind ATM was availability of financial services beyond regular work hours.

ATMs are ubiquitous (present everywhere) money dispensers, dispenses the cash upon verification of identity of user and their A/C through a specially coded card. (first started in 1974)

Web:- World Wide Web is a global information sharing and communication platform. Started first in 1991, Since then it has been massively responsible for many revolutions in the field of computing and communication.

Smart Meters:- Became operational in early 2000s for Power meters which are capable of communicating remotely with power grid and monitoring power usage by subscribers which made the billing process easy.

Digital locks:- Earliest attempts at connected home-automation systems. Present day digital locks are so robust that smart phones can be used to control them. Operations such as locking and unlocking doors, changing key codes, including new members in access lists can be performed remotely using smartphones.

Connected Healthcare :- Health care devices connect to hospitals, doctors and relatives to alert them in case of medical emergencies and take preventive measures. The devices are simple wearable devices which monitors heart rate and pulse of a wearer, as well as regular medical devices and monitors in hospitals. these connected devices make availability of medical records and test results much faster, cheaper and convenient for both patients as well as hospital authorities.

Connected vehicles :- Connected vehicles can communicate to the internet or with other vehicles or even with sensors and actuators contained with it. They self diagnose themselves and alert owners about system failure.

Smart cities :- This is a city wide implimentation of smart sensing, monitoring and actuation systems. city wide infrastructure communicating among themselves enables synchronized operations & information dissemination. Ex:- parking, transportation etc.

Smart Dust :- These are microscopic computers smaller than a grain of sand can be used in numerous ways where regular computer can not operate.

Ex:- measure chemicals in soil, diagnose problems in human body.

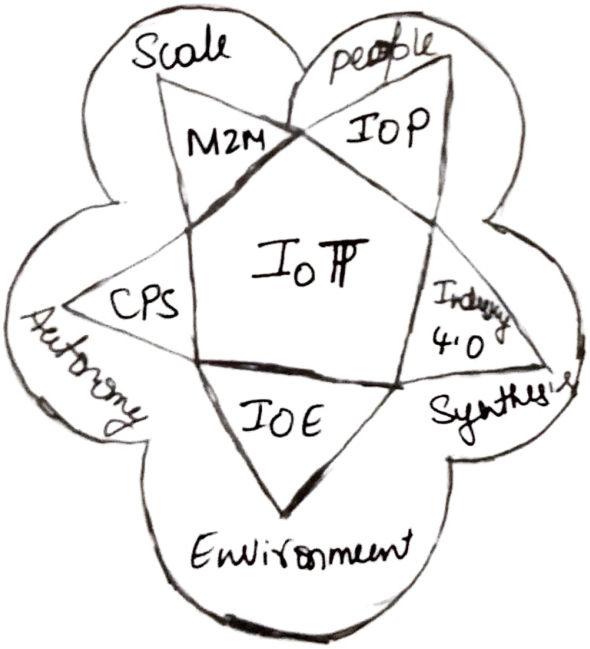
Smart factories :- These factories can monitor plant processes, assembly lines, distribution lines, manage floors on their own reducing human errors and unoptimized processes.

UAVs :- Unmanned Aerial Vehicles have emerged as robust public domain solutions tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintainance, assest management etc.

Present day IoT spans across various domains and applications. It has ability to function as cross domain technology enabler. Multiple domains can be supported and operated upon simultaneously ove IoT based platforms

The following figure shows various technological interdependencies of IoT with other domains and networking paradigms such as M2M, CPS, IoE, IoP and Industry 4.0.

Each of these networking paradigm is a massive domain on its own, but the omnipresent nature of IoT implies that these domains acts as subsets of IoT.



M2M :- Machine-to-Machine system is a system of connected machines and devices which can talk among themselves without human intervention. The communication between machines can be for updates on machine status, collab

-rative task completion, overall knowledge of systems and environment.

CPS :- Cyber Physical System is a closed control loop of sensing, processing, and actuation using feedback mechanism. These systems help in maintaining state of environment through feedback control loop, which ensures that until the desired state is attained the systems keeps on sensing and actuating. All ground level operations are automated and humans have only supervisory role in CPS based systems.

IoE :- This paradigm is concerned with minimizing and reversing ill effects of Internet based technologies on Environment. The major focus areas include smart & sustainable farming, energy efficient & sustainable habitats, any aspect of IoT that concerns and affects the environment falls under IoE.

IoP :- New technological movement on Internet which aims to decentralize online social

interactions, payments, transactions and other tasks while maintaining confidentiality and privacy of its user's data.

Ex:- bit coin.

Industry 4.0 :- fourth industrial Revoluti
- on pertaining to digitization in the manufact
- uring industry. The previous 3 revolutions are mechanization, mass production and indus trial revolution. This paradigm puts forward concept of smart factories, where machines can talk to each other without much invol -vement of humans based on a framework of CPS and IoT. This results in better resource and workspace management, optimizati - on of production time & resources and better upkeep and lifetimes of industrial systems.

IoT versus M2M :-

→ comm & interaction b/w machines & devices
→ Interaction are achived through cloud infra structure, server or local N/W hub.
→ Machine interactions via one or more comm N/W.

→ Operational & functional scope of IoT is vaster than M2M where interactions b/w things, people, devices and applications.
→ Internet connectivity is central to IoT theme but is not necessarily focus on the use of telecom N/w of M2M.

IoT Versus CPS :-

→ CPS encompasses sensing, control, actuation & feedback as complete package.
→ Digital twin is attached to CPS based S/S.
→ Digital twin is virtual model of S/S which is used in parallel to physical S/S which allows comparision of physical S/S O/P, performance & health.
→ In contrast IoT does not use feedback control.

IoT Versus WOT :-

→ WOT paradigm enable access & control over IoT resources & applications.
→ REST & RESTful APIs enable both developers & deployers to benefit from recognition, acceptance, & maturity of existing web technologies.
→ It can be thought of as an application layer based ~~not~~ over N/w layer.
→ IoT ~~is~~ include non-IP based S/S that are not accessible through web

Enabling IoT and the Complex Interdependence of Technologies

IoT is a paradigm built upon complex interdependencies of technologies both legacy and modern which occur at various planes of this paradigm.

IoT paradigm can be devided into 4 planes as shown Service, local connectivity, global connectivity and processing.

Service plane is composed of 2 parts, Things or devics and low power connectivi-ty, the service offered fall under the control and purviews of Service providers. Services offered in this layer are combination of things and low power connectivity. Any IoT application require basic setup of sensing, processing and low power low range N/w built on IEEE 802.15.4 protocol. Example for things - wearables, computers

Smartphones, household appliances, smart glasses, machines, vehicles, UAV's, robots. low power connectivity which is responsible for connecting things such as Wi-Fi, Ethernet or cellular N/w OR modern wireless progra -mable technologies like Zigbee, bluetooth, 6LOWPAN, LORA, Instion, DASH etc. The range of connectivity is severely restricted and responsible for connectivity b/w IOT things and nearest hub or gateways to access Inter -net.

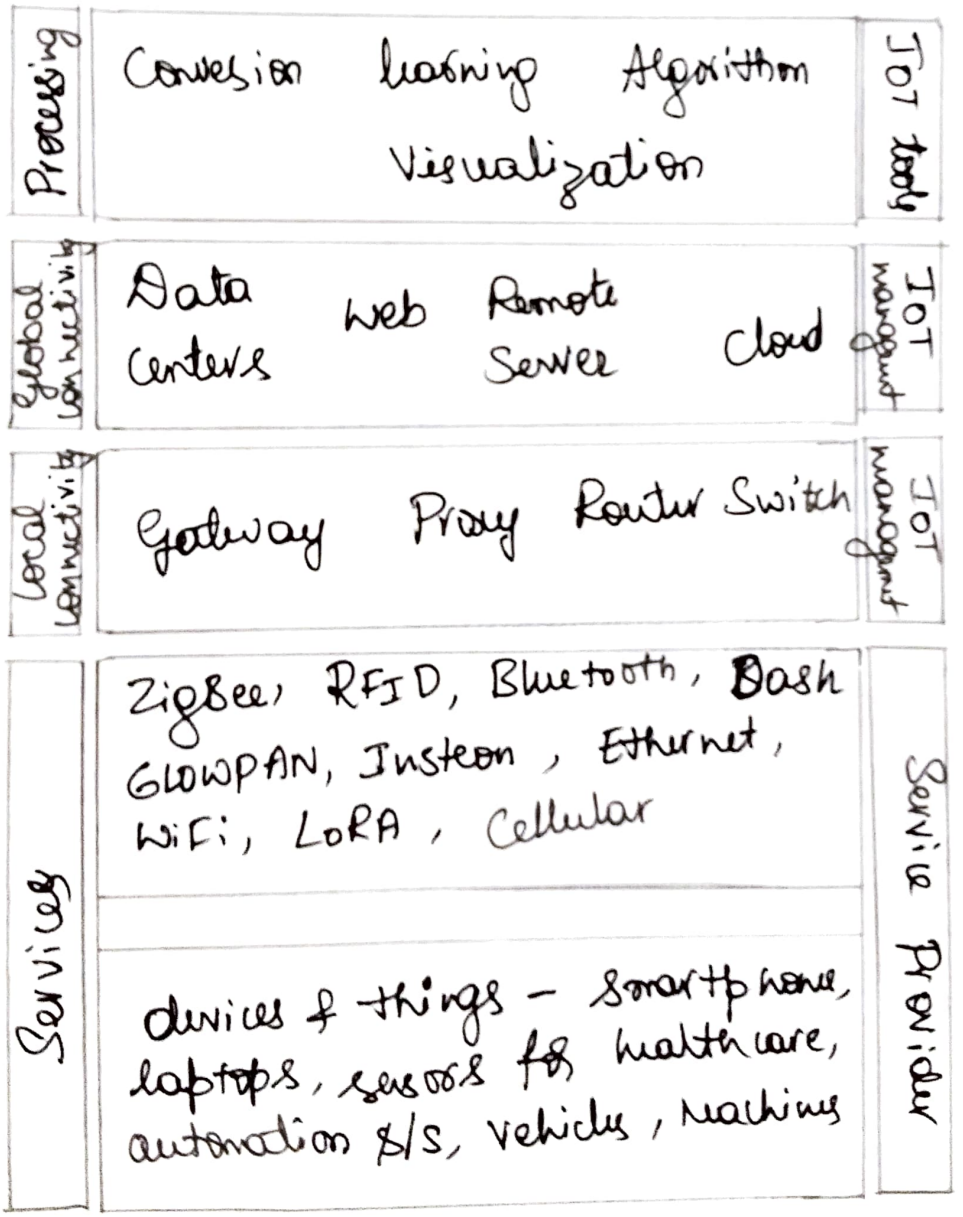
Local connectivity is responsible for distribu -ting Internet access to multiple local IOT deployments. Distribution of internet is based on physical placement of things, application domains or service providers. Gateways, Routers, Switches or proxies help in distribution. These gateways devices forwarding traffic from multiple things to internet through single gateways or routers, this helps in conserva -tion of already limited global IP address. This plane takes cares of management of

things. "Edge computing" is deployed b/w sensie and local connectivity layers

Global connectivity plays a significant role in enabling IoT in real sense by allowing for world wide implimentations and connectivity between things, users, controllers and applications. This plane also falls under the purview of IoT management as it decides how and when to store data, when to process it, when to forward it and in which form to forward it. "Fog computing" lies b/w planes of local connectivity & global connectivity. The web, data centers, remote servers, cloud and others make up this plane.

The final plane is Processing plane and consists of tools to wiring out useful and human readable information from all the raw data that flows from IoT devices and deployments. The various sub domains of this plane include intelligence, conversion

— data & format conversion & data cleaning, learning, cognition, algorithms (control & monitoring), visualization and Analysis. Computing Paradigms such as "Bigdata" "machine learning" and others fall with in scope of this domain



IoT Networking Components:-

IoT Networking components can be categorized into 6 broad components as shown below.

IoT node:- These are the networking devices within an IoT LAN. Each of these node consists of sensors, processors and a radio which communicates with the N/w. These nodes connect to other nodes inside LAN directly or by means of gateways. Connection outside LAN are through gateways & proxies.

IoT Router:- Router is a networking equipment that is primarily tasked with routing of packets b/w different entities of IoT N/w & keeps traffic flow correctly within N/w.

IoT LAN:- LAN enable local connectivity with in purview of single gateways. They consists of short range connectivity techno

- logies. IOT LAN may or may not be connect
- ed to Internet.

IOT WAN :- Wide Area Network connects various N/w LANs which are geographically wide. IOT WANs connect to Internet and enable Internet access to segments they are connecting.

IOT gateway :- It is a router connecting IOT LAN to WAN or internet. This gateway connect several LANs & WANs & forward packets b/w them.

IOT proxy :- proxies lie on application layer & perform application layer function b/w IOT nodes & other entities. They provide security to N/w entities & helps to extend addressing range of N/w.