

Introduction to IoT

Module 1:

I. Basics of Networking: Today's world relies heavily on data and networking, which allows for the instant availability of information from anywhere on the earth at any moment. Networking refers to the linking of computers and communication network devices (also referred to as hosts), which interconnect through a network (Internet or Intranet) and are separated by unique device identifiers (Internet protocol, IP addresses and media access control, MAC addresses). These hosts may be connected by a single path or through multiple paths for sending and receiving data. The data transferred between the hosts 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:

- 1) Type of connection
- 2) physical topology, and
- 3) reach of the network.

These classifications are helpful in deciding the requirements of a network setup and provide insights into the appropriate selection of a network type for the setup.

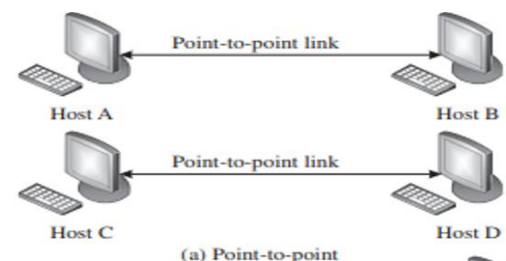
1. Connection type (Type of connection):

Depending on the way a host communicates with other hosts, computer networks are of two type:

- Point-to-point
- Point-to-multipoint.

1.1 Point-to-point:

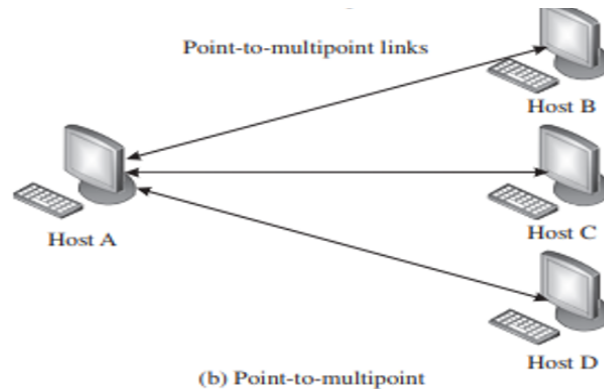
Point-to-point connections are used to establish direct connections between two hosts. Day-to-day systems such as a remote control for an air conditioner or television is a point to point connection, where the connection has the whole channel dedicated to it only. These networks were designed to work over duplex links and are functional for both



synchronous as well as asynchronous systems. In computer networks, point to point connections find usage for specific purposes such as in optical networks.

1.2 Point-to-multipoint

In a point-to-multipoint connection, more than two hosts share the same link. This type of configuration is similar to the one-to-many connection type. Point-to-multipoint connections find popular use in wireless networks and IP telephony.



The channel is shared between the various hosts, either spatially or temporally. One common scheme of spatial sharing of the channel is frequency division multiple access (FDMA). Temporal sharing of channels includes approaches such as time division multiple access (TDMA). Each of the spectral and temporal sharing approaches has various schemes and protocols for channel sharing in point-to-multipoint networks. Point-to-multipoint connections find popular use in present-day networks, especially while enabling communication between a massive number of connected devices.

2. Physical topology

Depending on the physical manner in which communication paths between the hosts are connected, computer networks can have the following four broad topologies like

- Star
- Mesh
- Bus
- Ring

2.1 Star connection: In a star topology, every host has a point-to-point link to a central controller or hub. The hosts cannot communicate with one another directly; they can only do so through the central hub. The hub acts as the network traffic exchange. For large-scale systems, the hub, essentially, has to be a powerful server to handle all the simultaneous traffic flowing through it. However, as there are fewer links (only one link per host), this topology is cheaper and easier to set up. The main advantages of the star topology are easy installation and the ease of fault identification within the network. If the central hub remains uncompromised, link failures between a host and the hub do not have a big effect on the network, except for the host that is affected. However, the main disadvantage of this topology is the danger of a single point of failure. If the hub fails, the whole network fails.

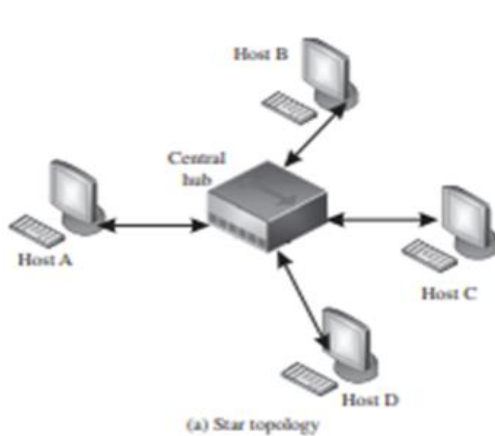


Fig1 Star connection

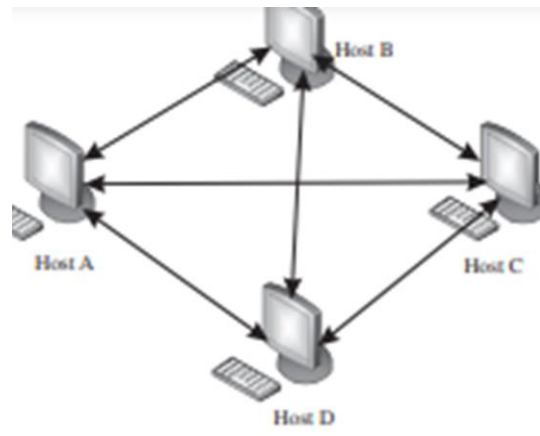


Fig2.Mesh Topology

2.2 Mesh Topology: In a mesh topology, every host is connected to every other host using a dedicated link (in a point-to-point manner). This implies that for n hosts in a mesh, there are a total of $n(n-1)/2$ dedicated full duplex links between the hosts. This massive number of links makes the mesh topology expensive. However, it offers certain specific advantages over other topologies. The first significant advantage is the robustness and resilience of the system. Even if a link is down or broken, the network is still fully functional as there remain other pathways for the traffic to flow through. The second advantage is the security and privacy of the traffic as the data is only seen by the intended recipients and not by all members of the network. The third advantage is the reduced data load on a network. The reduced data load on a single host, as every host in this network takes care of its traffic load.

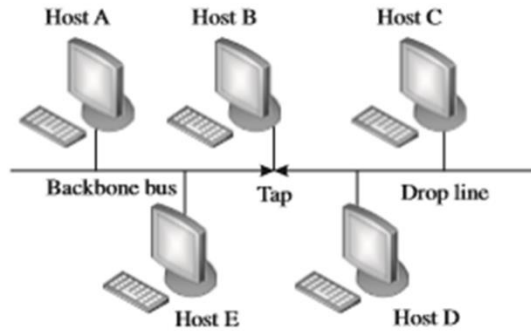


Fig3 Bus connection

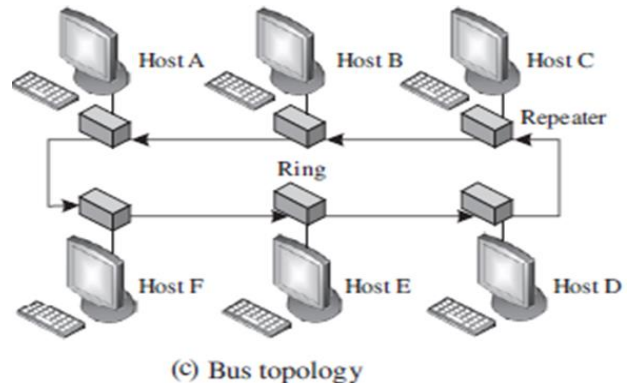


Fig4. Ring Topology

2.3 Bus: A bus topology follows the point-to-multipoint connection. A backbone cable or bus serves as the primary traffic pathway between the hosts. The hosts are connected to the main bus employing drop lines or taps. The main advantage of this topology is the ease of installation. However, there is a restriction on the length of the bus and the number of hosts that can be simultaneously connected to the bus due to signal loss over the extended bus. The bus topology has a simple cabling procedure in which a single bus (backbone cable) can be used for an organization. Multiple drop lines and taps can be used to connect various hosts to the bus, making installation very easy and cheap. However, the main drawback of this topology is the difficulty in fault localization within the network.

2.4 Ring: A ring topology works on the principle of a point-to-point connection. Here, each host is configured to have a dedicated point-to-point connection with its two immediate neighbouring hosts on either side of it through repeaters at each host. The repetition of this system forms a ring. The repeaters at each host capture the incoming signal intended for other hosts, regenerates the bit stream, and passes it onto the next repeater. Fault identification and set up of the ring topology is quite simple and straightforward. However, the main disadvantage of this system is the high probability of a single point of failure. If even one repeater fails, the whole network goes down.

Comparison of the various network topologies

Table 1.1 Network topology comparison

Topology	Feature	Advantage	Disadvantage
Star	Point-to-point	Cheap; ease of installation; ease of fault identification	Single point of failure; traffic visible to network entities
Mesh	Point-to-point	Resilient against single point of failures; scalable; traffic privacy and security ensured	Costly; complex connections
Bus	Point-to-multipoint	Ease of installation; cheap	Length of backbone cable limited; number of hosts limited; hard to localize faults
Ring	Point-to-point	Ease of installation; cheap; ease of fault identification	Prone to single point of failure

3. Network reachability

Computer networks are divided into four broad categories based on network reachability: personal area networks, local area networks, wide area networks, and metropolitan area networks.

3.1 Personal Area Networks (PAN): PANs, as the name suggests, are mostly restricted to individual usage. A good example of PANs may be connected wireless headphones, wireless speakers, laptops, smartphones, wireless keyboards, wireless mouse, and printers within a house. Generally, PANs are wireless networks, which make use of low-range and low-power technologies such as Bluetooth. The reachability of PANs lies in the range of a few centimetres to a few meters.

3.2 Local Area Networks (LAN): A LAN is a collection of hosts linked to a single network through wired or wireless connections. However, LANs are restricted to buildings, organizations, or campuses. Typically, a few leased lines connected to the Internet provide web access to the whole organization or a campus; the lines are further redistributed to multiple hosts within the LAN enabling hosts. The hosts are much more in number than the actual direct lines to the Internet to access the web from within the organization. This also allows the organization to define various access control policies for web access within its hierarchy. Typically, the present-day data access rates within the LANs range

from 100Mbps to 1000 Mbps, with very high fault-tolerance levels. Commonly used network components in a LAN are servers, hubs, routers, switches, terminals, and computers.

3.3 Metropolitan Area Networks (MAN): The reachability of a MAN lies between that of a LAN and a WAN. Typically, MANs connect various organizations or buildings within a given geographic location or city. An excellent example of a MAN is an Internet service provider (ISP) supplying Internet connectivity to various organizations within a city. As MANs are costly, they may not be owned by individuals or even single organizations. Typical networking devices/components in MANs are modems and cables. MANs tend to have moderate fault tolerance levels.

3.4 Wide Area Networks (WAN): WANs typically connect diverse geographic locations. However, they are restricted within the boundaries of a state or country. The data rate of WANs is in the order of a fraction of LAN's data rate. Typically, WANs connecting two LANs or MANs may use public switched telephone networks (PSTNs) or satellite-based links. Due to the long transmission ranges, WANs tend to have more errors and noise during transmission and are very costly to maintain. The fault tolerance of WANs are also generally low.

4. Layered Network Models

The intercommunication between hosts in any computer network, be it a large-scale or a small-scale one, is built upon the premise of various task-specific layers. Two of the most commonly accepted and used traditional layered network models are:

4.1 The **open systems interconnection** developed by the International Organization of Standardization (**ISO-OSI**) reference model and

4.2 The **Internet protocol suite**.

4.1 OSI Model

The ISO-OSI model is a conceptual framework that partitions any networked communication device into seven layers of abstraction, each performing distinct tasks based on the underlying technology and internal structure of the hosts. These seven layers, from bottom-up, are as follows:

1) Physical layer, 2) Data link layer, 3) Network layer, 4) Transport layer, 5) Session layer, 6) Presentation layer, and 7) Application layer.

The major highlights of each of these layers are explained in this section.

1. Physical Layer: This is a media layer and is also referred to as layer 1 of the OSI model. The physical layer is responsible for taking care of the electrical and mechanical operations of the host at the actual physical level. These operations include or deal with issues relating to signal generation, signal transfer, voltages, the layout of cables, physical port layout, line impedances, and signal loss. This layer is responsible for the topological layout of the network (star, mesh, bus, or ring), communication mode (simplex, duplex, full duplex), and bit rate control operations. The protocol data unit associated with this layer is referred to as a symbol.

2.Data Link Layer: This is a media layer and layer 2 of the OSI model. The data link layer is mainly concerned with the establishment and termination of the connection between two hosts, and the detection and correction of errors during communication between two or more connected hosts. IEEE 802 divides the OSI layer 2 further into two sub-layers : Medium access control (MAC) and logical link control (LLC). MAC is responsible for access control and permissions for connecting networked devices; whereas LLC is mainly tasked with error checking, flow control, and frame synchronization. The protocol data unit associated with this layer is referred to as a frame.

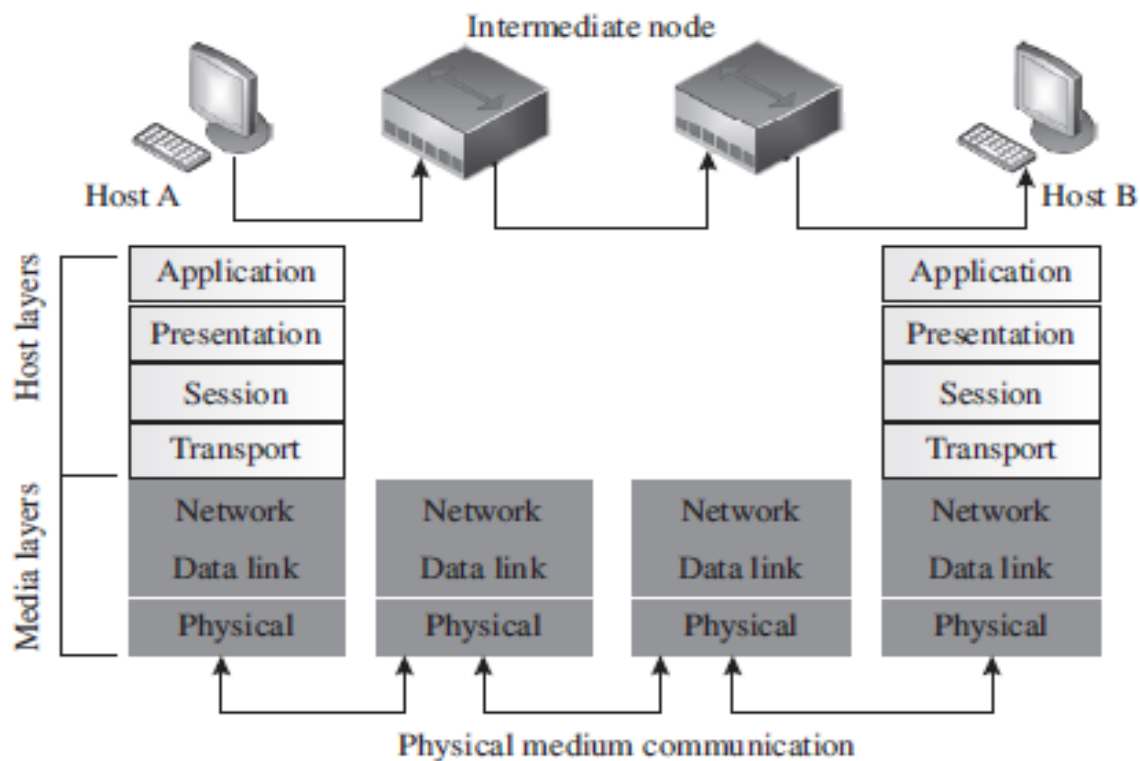
3.Network Layer: This layer is a media layer and layer 3 of the OSI model. It provides a means of routing data to various hosts connected to different networks through logical paths called virtual circuits. These logical paths may pass through other intermediate hosts (nodes) before reaching the actual destination host. The primary tasks of this layer include addressing, sequencing of packets, congestion control, error handling, and Internetworking. The protocol data unit associated with this layer is referred to as a packet.

4.Transport Layer: This is layer 4 of the OSI model and is a host layer. The transport layer is tasked with end-to-end error recovery and flow control to achieve a transparent transfer of data between hosts. This layer is responsible for keeping track of acknowledgments during variable-length data transfer between hosts. In case of loss of data, or when no acknowledgment is received, the transport layer ensures that the particular erroneous data segment is re-sent to the receiving host. The protocol data unit associated with this layer is referred to as a segment or datagram.

5.Session Layer: This is the OSI model's layer 5 and is a host layer. It is responsible for establishing, controlling, and terminating of communication between networked hosts. The session layer sees full utilization during operations such as remote procedure calls and remote sessions. The protocol data unit associated with this layer is referred to as data.

6.Presentation Layer: This layer is a host layer and layer 6 of the OSI model. It is mainly responsible for data format conversions and encryption tasks such that the syntactic compatibility of the data is maintained across the network, for which it is also referred to as the syntax layer. The protocol data unit associated with this layer is referred to as data.

7.Application Layer: This is layer 6 of the OSI model and is a host layer. It is directly accessible by an end-user through software APIs (application program interfaces) and terminals. Applications such as file transfers, FTP (file transfer protocol), e-mails, and other such operations are initiated from this layer. The application layer deals with user authentication, identification of communication hosts, quality of service, and privacy. The protocol data unit associated with this layer is referred to as data. A networked communication between two hosts following the OSI model is shown in Figure below



Internet protocol suite:

The Internet protocol suite is another conceptual framework that provides levels of abstraction for ease of understanding and development of communication and networked systems on the Internet. However, the Internet protocol suite predates the OSI model and provides only four levels of abstraction: 1) Link layer 2) Internet layer 3) transport layer, and 4) application layer.

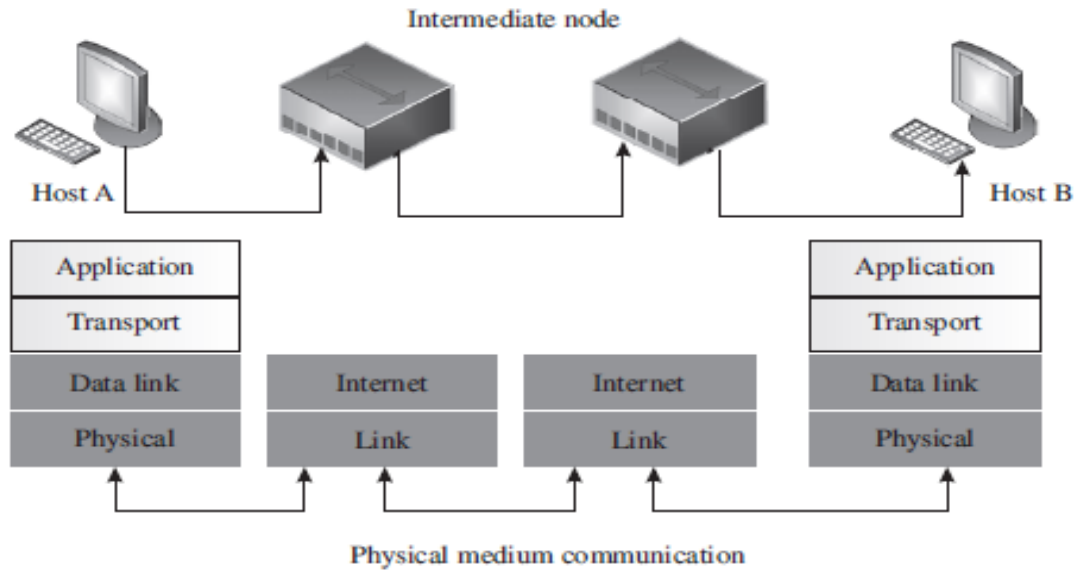
This collection of protocols is commonly referred to as the TCP/IP protocol suite (transmission control protocol (TCP) and Internet protocol (IP)).

1.Link Layer: The first and base layer of the TCP/IP protocol suite is also known as the network interface layer. This layer is synonymous with the collective physical and data link layer of the 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 the medium in use, frame format, and network access, enabling it to be used with a wide range of technologies such as the Ethernet, wireless LAN, and the asynchronous transfer mode (ATM).

2.Internet Layer: Layer 2 of the TCP/IP protocol suite is somewhat synonymous to the network layer of the OSI model. It is responsible for addressing, address translation, data packaging, data disassembly and assembly, routing, and packet delivery tracking operations. Some core protocols associated with this layer are address resolution protocol (ARP), Internet protocol (IP), Internet control message protocol (ICMP), and Internet group management protocol (IGMP). Traditionally, this layer was built upon IPv4, which is gradually shifting to IPv6, enabling the accommodation of a much more significant number of addresses and security measures.

3.Transport Layer: Layer 3 of the TCP/IP protocol suite is functionally synonymous with the transport layer of the OSI model. This layer is tasked with the functions of error control, flow control, congestion control, segmentation, and addressing in an end-to-end manner; it is also independent of the underlying network. Transmission control protocol (TCP) and user datagram protocol (UDP) are the core protocols upon which this layer is built, which in turn enables it to have the choice of providing connection-oriented or connectionless services between two or more hosts or networked devices.

4.Application Layer: The functionalities of the application layer, layer 4, of the TCP/IP protocol suite are synonymous with the collective functionalities of the OSI model's session, presentation, and application layers. This layer enables an end-user to access the services of the underlying layers and defines the protocols for the transfer of data. Hypertext transfer protocol (HTTP), file transfer protocol (FTP), simple mail transfer protocol (SMTP), domain name system (DNS), routing information protocol (RIP), and simple network management protocol (SNMP) are some of the core protocols associated with this layer.

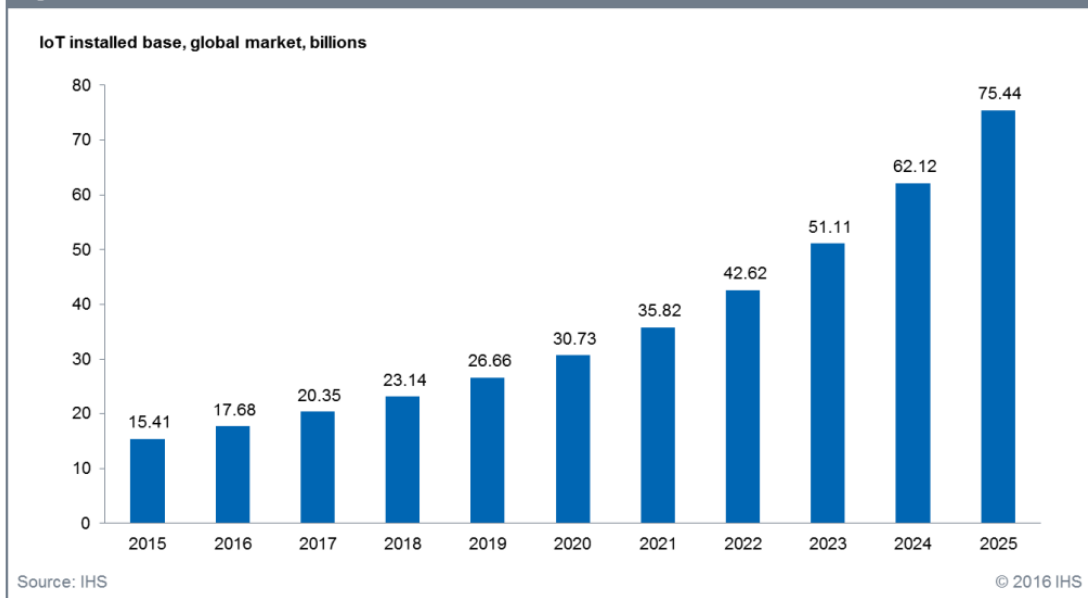


A networked communication between two hosts following the TCP/IP model is shown in above Figure

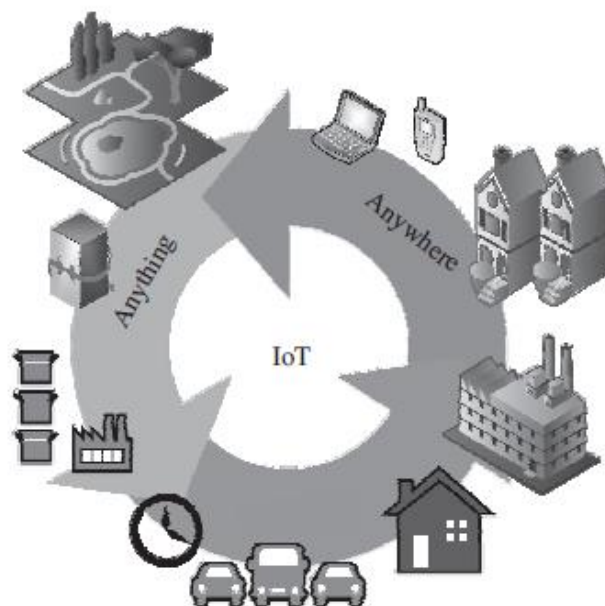
II. Emergence of IoT:

- ▶ The present-day Internet allows massively heterogeneous traffic through it.
- ▶ This network traffic consists of images, videos, music, speech, text, numbers, binary codes, machine status, banking messages, data from sensors and actuators, healthcare data, data from vehicles, home automation system status and control messages, military communications, and many more.
- ▶ This huge variety of data is generated from a massive number of connected devices, which may be directly connected to the Internet or connected through gateway devices.
- ▶ According to statistics from the Information Handling Services, the total number of connected devices globally is estimated to be around 25 billion. This figure is projected to triple within a short span of 5 years by the year 2025.

Figure 1. The IoT market will be massive



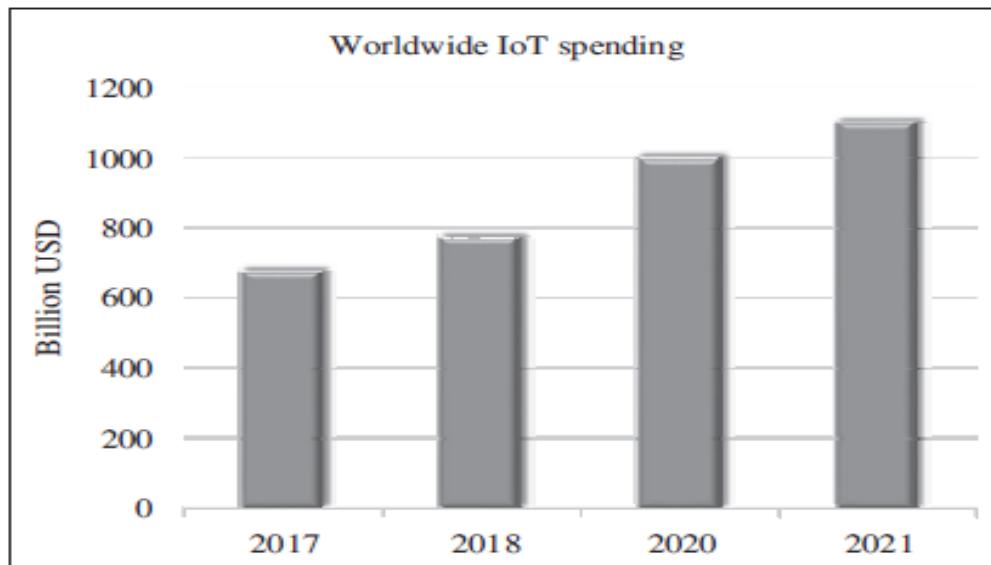
- ▶ IoT is an anytime, anywhere, and anything (as shown in Figure) network of Internet-connected physical devices or systems capable of sensing an environment and affecting the sensed environment intelligently.



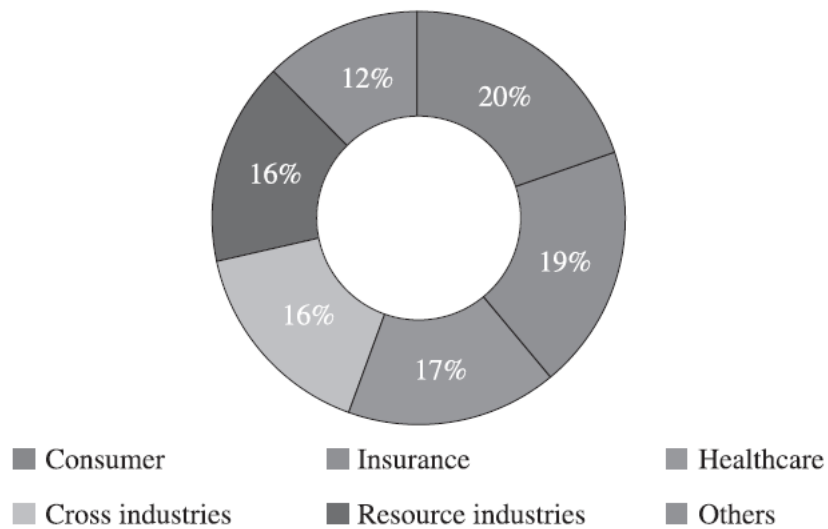
- The three characteristic features anytime, anywhere, and anything highlight the robustness and dynamic nature of IoT
- In other words, IoT may be considered to be made up of connecting devices, machines, and tools; these things are made up of sensors/actuators and processors, which connect to the Internet through wireless technologies.
- It is consider any technology enabling access to the Internet—be it wired or wireless—to be an IoT enabling technology.
- Most of the focus on the discussion of various IoT enablers will be restricted to wireless IoT systems due to the much more severe operating constraints and challenges faced by wireless devices as compared to wired systems.

I. IoT systems can be characterized by the following features:

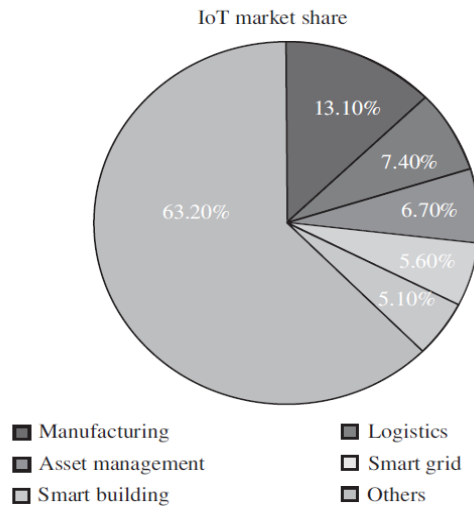
- The three characteristic features anytime, anywhere, and anything highlight the robustness and dynamic nature of IoT
- In other words, IoT may be considered to be made up of connecting devices, machines, and tools; these things are made up of sensors/actuators and processors, which connect to the Internet through wireless technologies.
- It is consider any technology enabling access to the Internet—be it wired or wireless—to be an IoT enabling technology.
- Most of the focus on the discussion of various IoT enablers will be restricted to wireless IoT systems due to the much more severe operating constraints and challenges faced by wireless devices as compared to wired systems.
- The global IoT spending across various organizations and industries and its subsequent projection until the year 2021



Worldwide IoT market growth
(2016–2021)



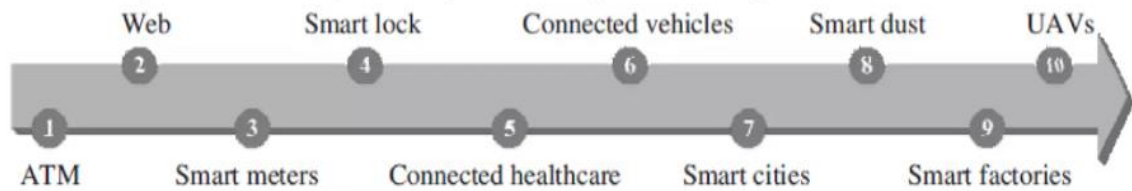
The compound annual growth rate (CAGR) of the IoT market



The IoT market share across various industries

Evolution of IoT

- The sequence of technological developments leading to modern-day IoT



- ATM: Automated Teller Machines, 1974, Cash Dispenser
- Web: 1991, World Wide Web, Global Information Sharing and Communication
- Smart Meters: 2000, Communicating to Power Grid, Monitoring, Billing and Power Allocation
- Digital Locks: Home Automation
- Connected Healthcare: Hospitals, Doctors & Relatives
- Connected Vehicles: Internet or other Vehicles, or Sensors and Actuators
- Smart Cities: Sensing, Monitoring & Actuation
- Smart Dust: Microscopic Computers - Measure Chemicals in the Soil
- Smart Factories: Monitor & Manage on their Own
- UAVs: Unmanned Aerial Vehicles - Agriculture, Surveys, Surveillance, Deliveries, etc

AVS/ISS-23/2020

Dr. Emmanuel D.

2.

These sequence of technical developments toward the emergence of IoT are described in brief:

- ▶ ATM-Automated teller machine
- ▶ Web
- ▶ Smart meters
- ▶ Digital locks
- ▶ Connected healthcare
- ▶ Connected vehicles
- ▶ Smart cities
- ▶ Smart Dust
- ▶ Smart factories
- ▶ UAVs-Unmanned aerial vehicles

ATM: {automated teller machines}

- ▶ ATMs or automated teller machines are cash distribution machines, which are linked to a user's bank account.
- ▶ ATMs dispense cash upon verification of the identity of a user and their account through a specially coded card.
- ▶ The central concept behind ATMs was the availability of financial transactions even
- ▶ when banks were closed beyond their regular work hours. These ATMs were ubiquitous money dispensers.
- ▶ The first ATM became operational and connected online for the first time in 1974.

Web: World Wide Web

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

Digital Locks:

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

Connected Healthcare:

- Here, healthcare devices connect to hospitals, doctors, and relatives to alert them of medical emergencies and take preventive measures.
- The devices may be simple wearable appliances, monitoring just the heart rate and pulse of the wearer, as well as regular medical devices and monitors in hospitals.
- The connected nature of these systems makes the availability of medical records and test results much faster, cheaper, and convenient for both patients as well as hospital authorities

Connected Vehicles:

- Connected vehicles may communicate to the Internet or with other vehicles, or even with sensors and actuators contained within it.
- These vehicles self-diagnose themselves and alert owners about system failures.

Smart Cities:

- This is a city-wide implementation of smart sensing, monitoring, and actuation systems.
- The city-wide infrastructure communicating amongst themselves enables unified and synchronized operations and information dissemination.
- Some of the facilities which may benefit are parking, transportation, and others.

Smart Dust:

- These are microscopic computers. Smaller than a grain of sand each, they can be used in numerous beneficial ways, where regular computers cannot operate.
- For example, smart dust can be sprayed to measure chemicals in the soil or even to diagnose problems in the human body.

Smart Factories:

- These factories can monitor plant processes, assembly lines, distribution lines, and manage factory floors all on their own.
- The reduction in mishaps due to human errors in judgment or unoptimized processes is drastically reduced.

UAVs:

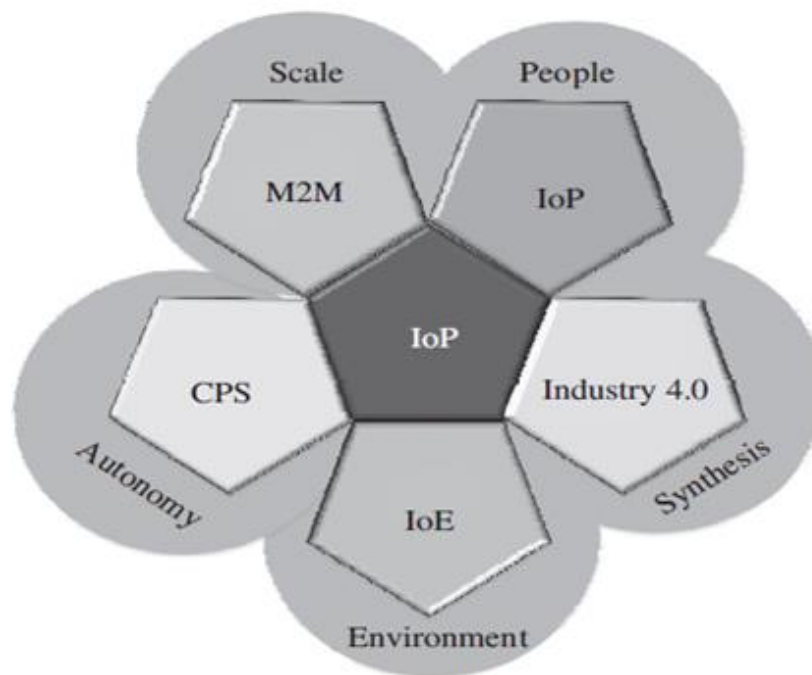
- UAVs or unmanned aerial vehicles have emerged as robust public domain solutions tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other tasks.

II. Interdependencies of IoT with other

- The present-day IoT spans across various domains and applications.
- The major highlight of this paradigm is its ability to function as a cross-domain technology enabler.
- Multiple domains can be supported and operated upon simultaneously over IoT-based platforms. Support for legacy technologies and standalone paradigms, along with modern developments, makes IoT quite robust and economical for commercial, industrial, as well as consumer applications.
- IoT is being used in vivid and diverse areas such as smart parking, smartphone detection, traffic congestion, smart lighting, waste management, smart roads, structural health, urban noise maps, river floods, water flow, silos stock calculation, water leakages, radiation levels, explosive and hazardous gases, perimeter access control, snow level monitoring, liquid presence, forest fire detection, air pollution, smart grid, tank level, photovoltaic installations, NFC (near-field communications) payments, intelligent shopping applications, landslide and avalanche

prevention, early detection of earthquakes, supply chain control, smart product management, and others.

- Figure shows the various technological interdependencies of IoT with other domains and networking paradigms such as M2M, CPS, the Internet of environment (IoE), the Internet of people (IoP), and Industry 4.0. Each of these networking paradigms is a massive domain on its own.
- but the omnipresent nature of IoT implies that these domains act as subsets of IoT. The paradigms are briefly discussed here:



The interdependence and reach of IoT over various application domains and networking paradigms

M2M (Machine-to-Machine)

- The M2M or the machine-to-machine paradigm signifies a system of connected machines and devices, which can talk amongst themselves without human intervention.

- ▶ The communication between the machines can be for updates on machine status (stocks, health, power status, and others), collaborative task completion, overall knowledge of the systems and the environment, and others.

CPS(Cyber Physical System)

- ▶ The CPS or the cyber physical system paradigm insinuates a closed control loop—from sensing, processing, and finally to actuation—using a feedback mechanism.
- ▶ CPS helps in maintaining the state of an environment through the feedback control loop, which ensures that until the desired state is attained, the system keeps on actuating and sensing. Humans have a simple supervisory role in CPS-based systems; most of the ground-level operations are automated.

IoE (Internet of Environment)

- ▶ The IoE paradigm is mainly concerned with minimizing and even reversing the ill-effects of the permeation of Internet-based technologies on the environment.
- ▶ The major focus areas of this paradigm include smart and sustainable farming, sustainable and energy-efficient habitats, enhancing the energy efficiency of systems and processes, and others.

Industry 4.0:

- ▶ Industry 4.0 is commonly referred to as the fourth industrial revolution pertaining to digitization in the manufacturing industry.
- ▶ This paradigm strongly puts forward the concept of smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT.
- ▶ This paradigm strongly puts forward the concept of smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT.
- ▶ The digitization and connectedness in Industry 4.0 translate to better resource and workforce management, optimization of production time and resources, and better upkeep and lifetimes of industrial systems.

IoP:

- ▶ IoP is a new technological movement on the Internet which aims to decentralize online social interactions, payments, transactions, and other tasks while maintaining confidentiality and privacy of its user's data.
- ▶ A famous site for IoP states that as the introduction of the Bitcoin has severely limited the power of banks and governments, the acceptance of IoP will limit the power of corporations, governments, and their spy agencies

IoT versus M2M

- ▶ M2M or the machine-to-machine paradigm refers to communications and interactions between various machines and devices.
- ▶ These interactions can be enabled through a cloud computing infrastructure, a server, or simply a local network hub.
- ▶ M2M collects data from machinery and sensors, while also enabling device management and device interaction.
- ▶ Telecommunication services providers introduced the term M2M, and technically emphasized on machine interactions via one or more communication networks (e.g., 3G, 4G, 5G, satellite, public networks).
- ▶ M2M is part of the IoT and is considered as one of its sub-domains, M2M standards occupy a core place in the IoT landscape.
- ▶ in terms of operational and functional scope, IoT is vaster than M2M and comprises a broader range of interactions such as the interactions between devices/things, things, and people, things and applications, and people with applications;
- ▶ M2M enables the amalgamation of workflows comprising such interactions within IoT.
- ▶ Internet connectivity is central to the IoT theme but is not necessarily focused on the use of telecom networks.

Abbreviation	Internet of Things	Machine to Machine communication
Intelligence	Devices include pieces that can make personal decisions without outside interference	Intelligent only to some extent
Type of connection used	Devices communicate via a network and other wireless communications	Point to point to communication
Communication protocols	TCP/IP protocols such as HTTP, HTTPS, FTP and Telnet	Traditional and less secure communication protocols are used
Data sharing	In order to improve the user experience, the data is shared between applications	Data is shared only between allowed connections
Internet	IoT is nothing without the presence of internet communication	Devices do not require internet
scope	IoT has a bright future and is capable of connecting billions of devices.	Limited scope for devices
Examples	Smart wearables, smart cities, smart cars, smart homes and so on	Sensors and data information


IoT versus CPS

- ▶ Cyber physical systems (CPS) encompasses sensing, control, actuation, and feedback as a complete package. In other words, a digital twin is attached to a CPS-based system.
- ▶ a digital twin is a virtual system–model relation, in which the system signifies a physical system or equipment or a piece of machinery, while the model represents the mathematical model or representation of the physical system's behavior or operation.
- ▶ Many a time, a digital twin is used parallel to a physical system, especially in CPS as it allows for the comparison of the physical system's output, performance, and health. Based on feedback from the digital twin, a physical system can be easily given corrective directions/commands to obtain desirable outputs.
- ▶ In contrast, the IoT paradigm does not compulsorily need feedback or a digital twin system. IoT is more focused on networking than controls.
- ▶ Some of the constituent sub-systems in an IoT environment (such as those formed by CPS-based instruments and networks) may include feedback and controls too. In this light, CPS may be considered as one of the sub-domains of IoT,

▶ IoT versus WoT

- ▶ From a developer's perspective, the Web of Things (WoT) paradigm enables access and control over IoT resources and applications.
- ▶ These resources and applications are generally built using technologies such as HTML 5.0, JavaScript, Ajax, PHP, and others. REST (representational state transfer) is one of the key enablers of WoT.
- ▶ The use of RESTful principles and RESTful APIs (application program interface) enables both developers and deployers to benefit from the recognition, acceptance, and maturity of existing web technologies without having to redesign and redeploy solutions from scratch.
- ▶ Still, designing and building the WoT paradigm has various adaptability and security challenges, especially when trying to build a globally uniform WoT.

- ▶ As IoT is focused on creating networks comprising objects, things, people, systems, and applications, which often do not consider the unification aspect and the limitations of the Internet, the need for WoT, which aims to integrate the various focus areas of IoT into the existing Web is really invaluable.
- ▶ Technically, WoT can be thought of as an application layer-based hat added over the network layer. However, the scope of IoT applications is much broader; IoT also includes non-IP-based systems that are not accessible through the web.

Cyber-Physical Systems	IoT
A system that combines physics with cyber components, potentially networked and tightly interconnected.	A catch-all term for the growing number of physical devices around the world that are connected to the internet and to each other.
It seamlessly integrates computation, networking and physical processes.	Comprises things or objects that have unique identities and are connected to the Internet.
Sensors and actuators work in the feedback loop using human intervention.	It is purely automation meaning no human assistance is required.
	

IoT vs WoT: Connectivity

	IoT	WoT
Connectivity	Machine to Machine	LWM2M Machine to Web
Networking	TCP / UDP	HTTP / REST / CoAP
Things	Sensor Device	RESTful Objects
Data	Streaming Data	Time-Series Data
Discover	MQTT	Publish / Subscribe

IoT	WoT
<ul style="list-style-type: none"> IoT is a network of Things, which are anything that can be connected in some form to the Internet 	<ul style="list-style-type: none"> WoT is web network created for proper handling and using the potential of IoT platforms to provide better future
<ul style="list-style-type: none"> IoT is a hardware layer to connect everything to the Internet 	<ul style="list-style-type: none"> WoT is a software layer to connect everything to the web
<ul style="list-style-type: none"> IoT deals with sensors, actuators, computation and communication interfaces. From a box of oranges with an RFID tag, to a smart city and to everyThing in between, all these digitally augmented objects make up the IoT 	<ul style="list-style-type: none"> WoT deals with protocols and web servers. All those applications for IoT devices make up the WoT
<ul style="list-style-type: none"> There is a different protocol for each and every IoT devices 	<ul style="list-style-type: none"> WoT makes it easy by using single protocol for multiple IoT devices
<ul style="list-style-type: none"> IoT platforms are hard to program due to multiple protocols 	<ul style="list-style-type: none"> Due to common API's to handle the protocol WoT programming is easier
<ul style="list-style-type: none"> IoT standards and prototypes are not public. They are privately funded and are not publicly accessible Insecure data transmission 	<ul style="list-style-type: none"> WoT is free for everyone and can be accessed anywhere, anytime
<ul style="list-style-type: none"> IoT is tightly coupled between the applications and networks 	<ul style="list-style-type: none"> whereas WoT in application layer is loosely coupled

III. 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.
- ▶ we can divide the IoT paradigm into four planes: services, local connectivity, global connectivity, and processing.
- ▶ If we consider a bottom-up view, the services offered fall under the control and purview of service providers. The service plane is composed of two parts:

- 1) things or devices and
- 2) low-power connectivity.

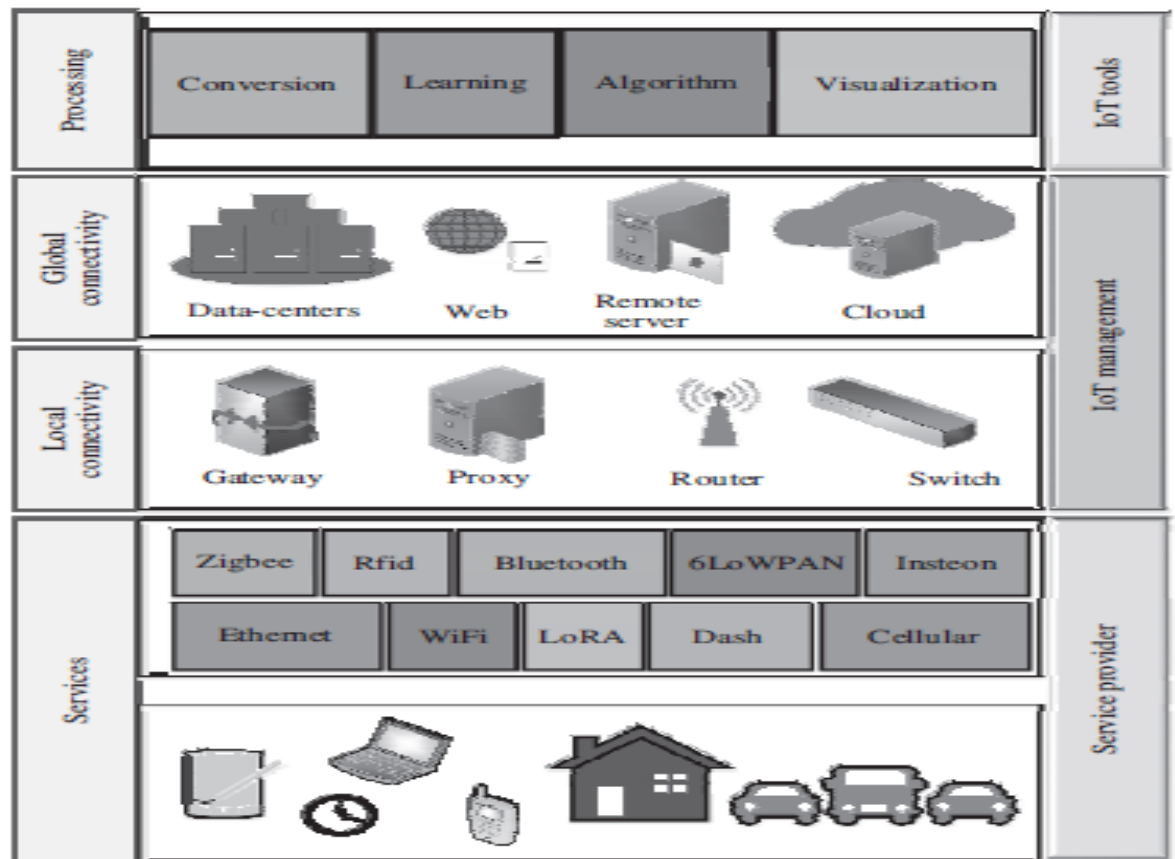


Figure 4.8 The IoT planes, various enablers of IoT, and the complex interdependencies

- ▶ Typically, the services offered in this layer are a combination of things and low power connectivity.

- ▶ For example, any IoT application requires the basic setup of sensing, followed by rudimentary processing (often), and a low-power, low-range network, which is mainly built upon the IEEE 802.15.4 protocol.
- ▶ The things may be wearables, computers, smartphones, household appliances, smart glasses, factory machinery, vending machines, vehicles, UAVs, robots, and other such contraptions (which may even be just a sensor).
- ▶ The immediate low-power connectivity, which is responsible for connecting the things in local implementation, may be legacy protocols such as Wi-Fi, Ethernet, or cellular.
- ▶ In contrast, modern-day technologies are mainly wireless and often programmable such as Zigbee, RFID, Bluetooth, 6LoWPAN, LoRA, DASH, Insteon, and others.
- ▶ The range of these connectivity technologies is severely restricted;
- ▶ they are responsible for the connectivity between the things of the IoT and the nearest hub or gateway to access the Internet.
- ▶ The local connectivity is responsible for distributing Internet access to multiple local IoT deployments.
- ▶ This distribution may be on the basis of the physical placement of the things, on the basis of the application domains, or even on the basis of providers of services.
- ▶ Services such as address management, device management, security, sleep scheduling, and others fall within the scope of this plane.
- ▶ For example, in a smart home environment, the first floor and the ground floor may have local IoT implementations, which have various things connected to the network via low-power, low-range connectivity technologies.
- ▶ the penultimate plane of global connectivity plays a significant role in enabling IoT in the real sense by allowing for worldwide implementations 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.

- ▶ The Web, data-centers, remote servers, Cloud, and others make up this plane.
- ▶ The final plane of processing can be considered as a top-up of the basic IoT networking framework.
- ▶ The continuous rise in the usefulness and penetration of IoT in various application areas such as industries, transportation, healthcare, and others is the result of this plane.
- ▶ The members in this plane may be termed as IoT tools, simply because they wring-out useful and human-readable information from all the raw data that flows from various IoT devices and deployments.

The various sub-domains of this plane include :

- ▶ Intelligence, Conversion (data and format conversion, and data cleaning), learning (making sense of temporal and spatial data patterns),
- ▶ cognition (recognizing patterns and mapping it to already known patterns)
- ▶ Algorithms (various control and monitoring algorithms),
- ▶ visualization (rendering numbers and strings in the form of collective trends, graphs, charts, and projections),
- ▶ Analysis (estimating the usefulness of the generated information,
- ▶ making sense of the information with respect to the application and place of data generation, and estimating future trends based on past and present patterns of information obtained).
- ▶ Various computing paradigms such as “big data”, “machine Learning”, and others, fall within the scope of this domain

IoT Networking Components

- ▶ An IoT implementation is composed of several components, which may vary with their application domains.
- ▶ generally, outline five broad categories of IoT networking components. any IoT network, into six types: 1) IoT node, 2) IoT router, 3) IoT LAN, 4) IoT WAN, 5) IoT gateway, and 6) IoT proxy.
- ▶ A typical IoT implementation from a networking perspective is shown in Figure 4.9. The individual components are briefly described below

- **IoT Node:** These are the networking devices within an IoT LAN. Each of these devices is typically made up of a sensor, a processor, and a radio, which communicates with the network infrastructure (either within the LAN or outside it).
- The nodes may be connected to other nodes inside a LAN directly or by means of a common

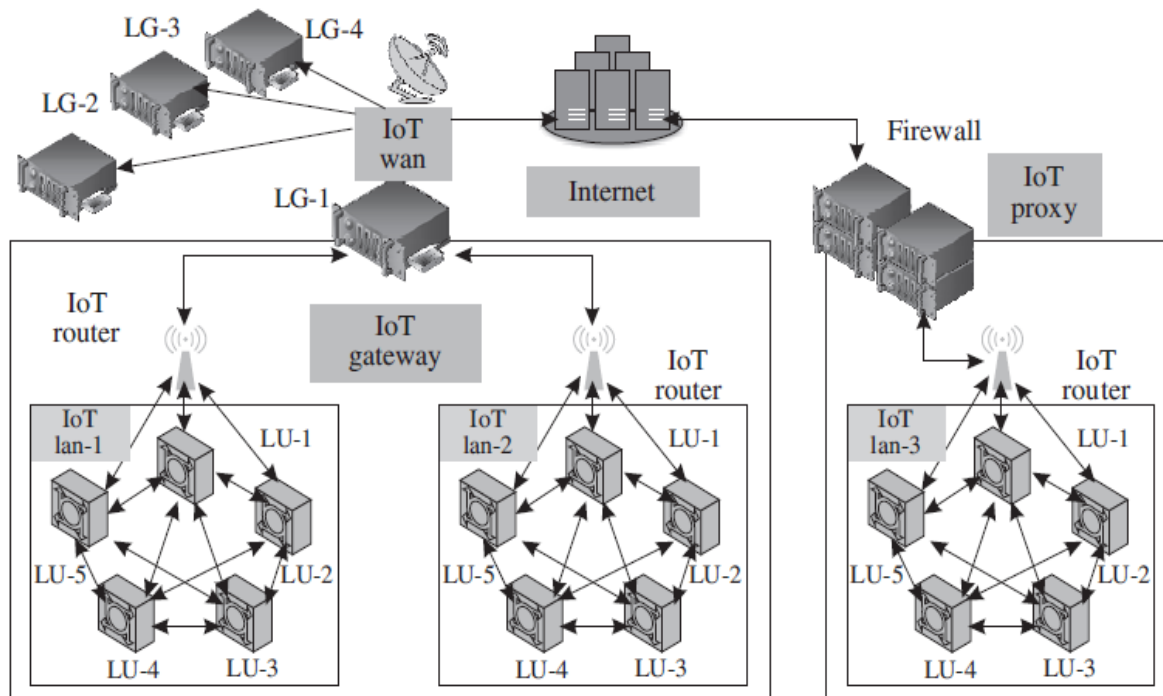


Figure 4.9 A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

gateway for that LAN. Connections outside the LAN are through gateways and proxies.

- **IoT Router:** An IoT router is a piece of networking equipment that is primarily tasked with the routing of packets between various entities in the IoT network; it keeps the traffic flowing correctly within the network. A router can be repurposed as a gateway by enhancing its functionalities.
- **IoT LAN:** The local area network (LAN) enables local connectivity within the purview of a single gateway. Typically, they consist of short-range connectivity technologies. IoT LANs may or may not be connected to the Internet. Generally, they are localized within a building or an organization.

- ▶ **IoT WAN:** The wide area network (WAN) connects various network segments such as LANs. They are typically organizationally and geographically wide, with their operational range lying between a few kilometers to hundreds of kilometers.
- ▶ IoT WANs connect to the Internet and enable Internet access to the segments they are connecting.
- ▶ **IoT Gateway:** An IoT gateway is simply a router connecting the IoT LAN to a WAN or the Internet. Gateways can implement several LANs and WANs. Their primary task is to forward packets between LANs and WANs, and the IP layer using only layer 3.
- ▶ (vi) **IoT Proxy:** Proxies actively lie on the application layer and performs application layer functions between IoT nodes and other entities. Typically, application layer proxies are a means of providing security to the network entities under it ; it helps to extend the addressing range of its network.
- ▶ The various IoT nodes within an IoT LAN are configured to talk to one another as well as talk to the IoT router whenever they are in the range of it.
- ▶ The devices have locally unique (LU-x) device identifiers. These identifiers are unique only within a LAN. There is a high chance that these identifiers may be repeated in a new LAN. Each IoT LAN has its own unique identifier, which is denoted by IoT LAN-x in Figure 4.9.
- ▶ A router acts as a connecting link between various LANs by forwarding messages from the LANs to the IoT gateway or the IoT proxy. As the proxy is an application layer device, it is additionally possible to include features such as firewalls, packet filters, and other security measures besides the regular routing operations.
- ▶ Various gateways connect to an IoT WAN, which links these devices to the Internet. There may be cases where the gateway or the proxy may directly connect to the Internet.
- ▶ This network may be wired or wireless; however, IoT deployments heavily rely on wireless solutions.

- ▶ This is mainly attributed to the large number of devices that are integrated into the network; wireless technology is the only feasible and neat-enough solution to avoid the hassles of laying wires and dealing with the restricted mobility rising out of wired connections.