Introduction to IOT

Unit 1

Dr Shobha K R
Dept of ETE, RIT

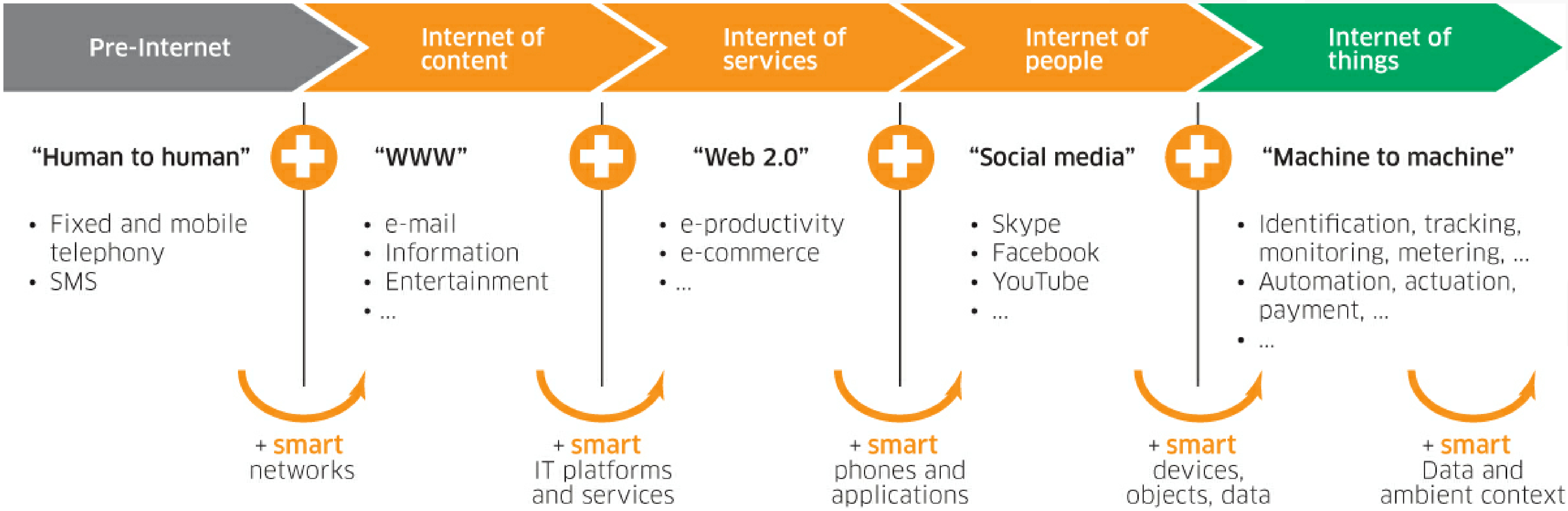
Definition of IoT

A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, often communicate data associated with users and their environments.

Characteristics of IoT

- Dynamic & Self-Adapting
  - ✓ Dynamically adapt with changing contexts
  - ✓ Take action based on operating conditions/user context / sensed environment
  - ✓ **Ex: Surveillance system**
- Self-Configuring
  - ✓ Setup networking
  - ✓ Upgrade software with minimal user intervention
- Interoperable Communication Protocols
  - ✓ Heterogeneous devices working together
- Unique Identity
  - ✓ Monitor status
  - ✓ Query device
  - ✓ Control remotely
- Integrated into Information Network
  - ✓ To communicate and exchange data with other devices and systems
  - ✓ Data analysis and prediction

Internet of Things - Evolution



Pre-Internet

"Human to human"

- Fixed and mobile telephony
- SMS

+ smart networks

Internet of content

"WWW"

- e-mail
- Information
- Entertainment
- ...

+ smart IT platforms and services

Internet of services

"Web 2.0"

- e-productivity
- e-commerce
- ...

+ smart phones and applications

Internet of people

"Social media"

- Skype
- Facebook
- YouTube
- ...

+ smart devices, objects, data

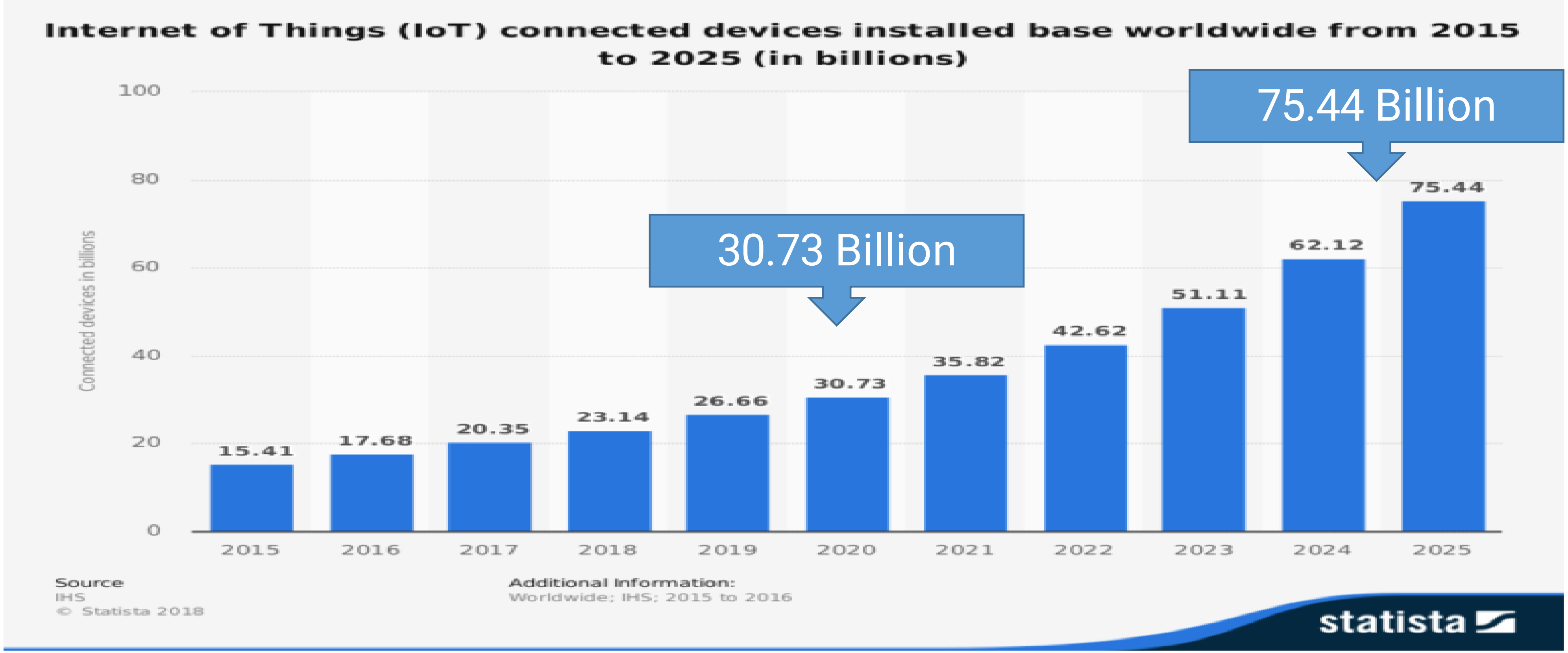
Internet of things

"Machine to machine"

- Identification, tracking, monitoring, metering, ...
- Automation, actuation, payment, ...
- ...

+ smart Data and ambient context

How many IoT devices will there be in 2025?

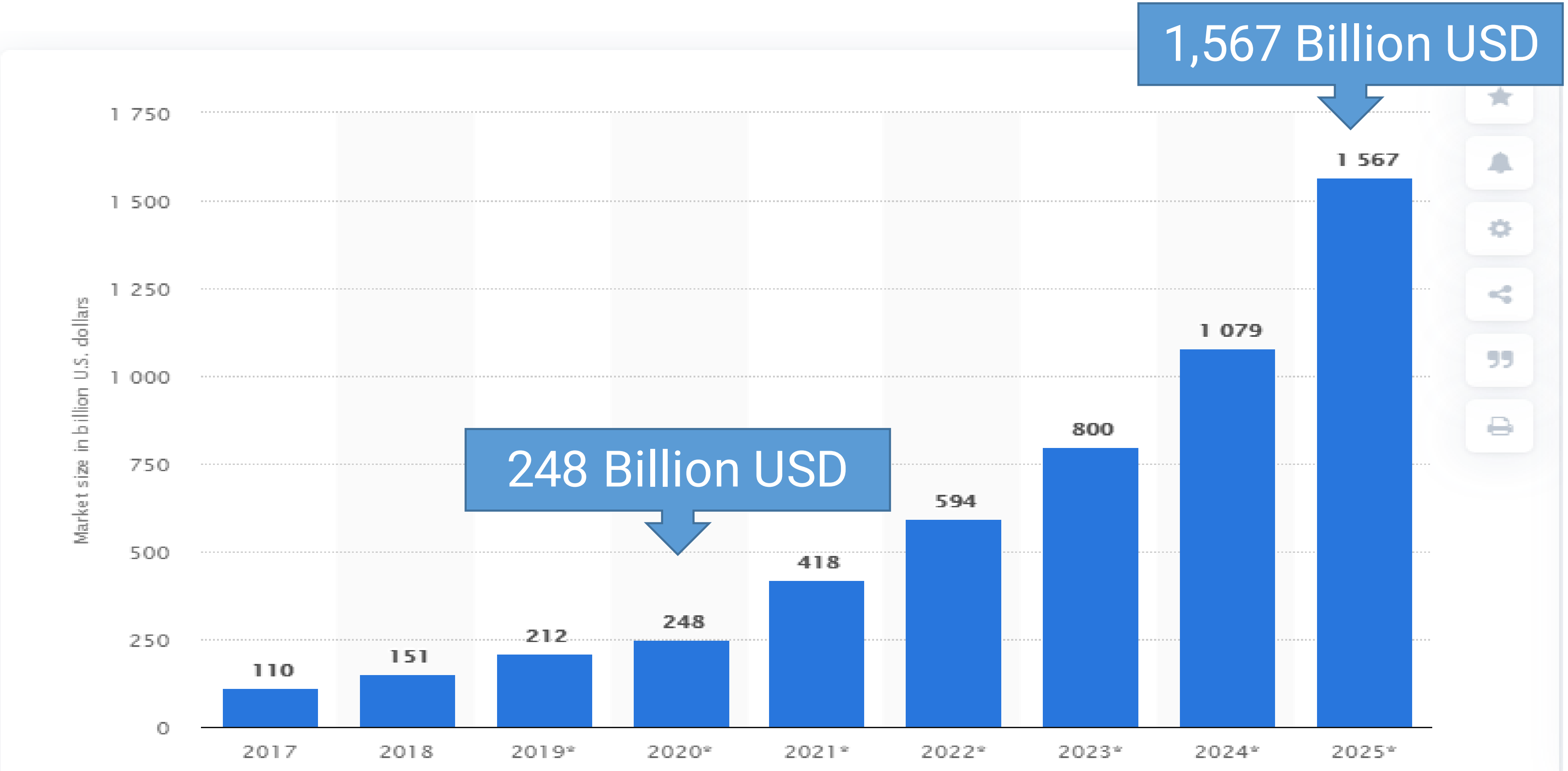


Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)

Source
IHS
© Statista 2018

Additional Information:
Worldwide; IHS; 2015 to 2016

Prediction of End User Investment in IOT?

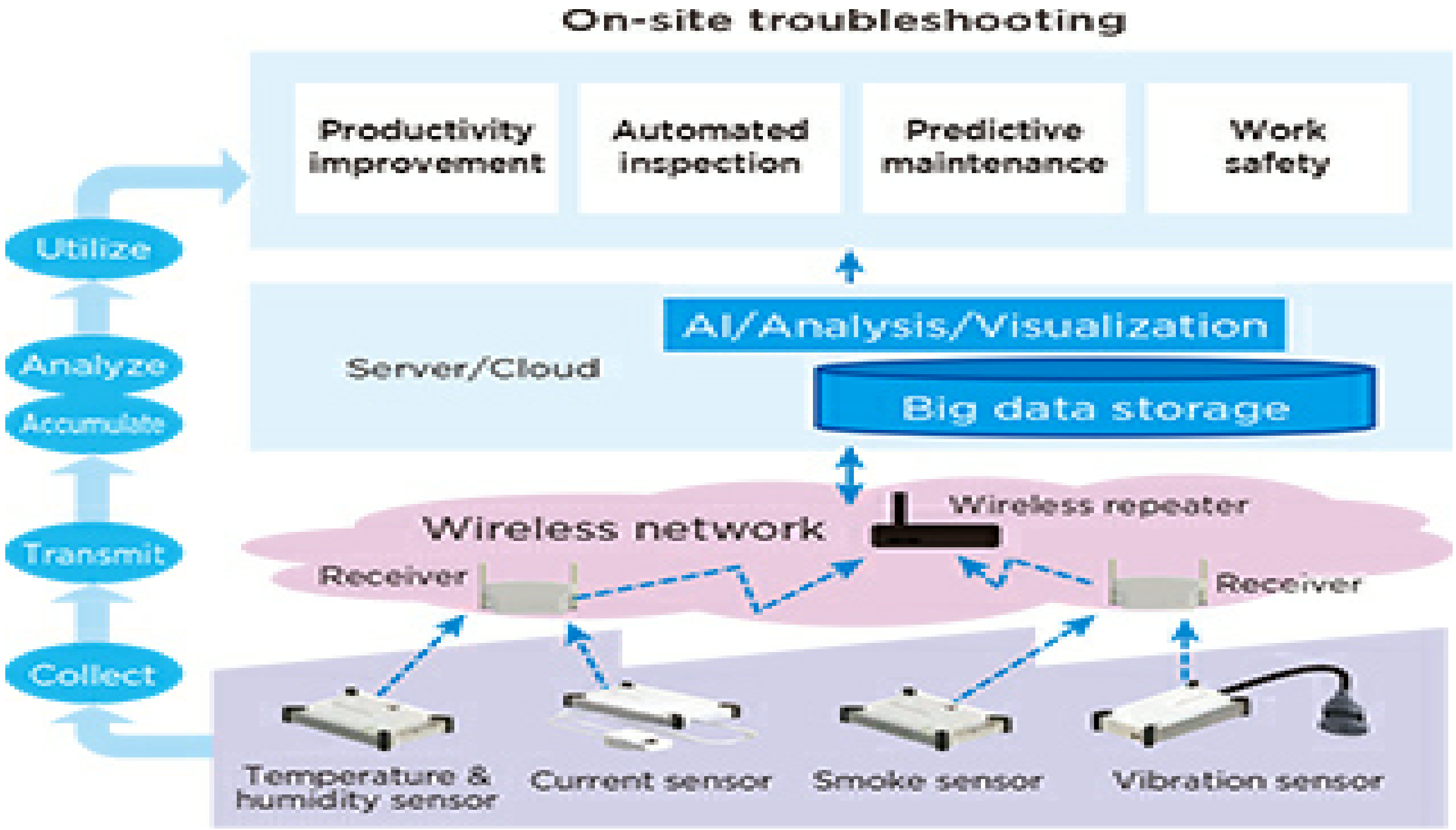


1,567 Billion USD

248 Billion USD

© Statista 2020

Internet of Things- Basic Architecture



Introduction

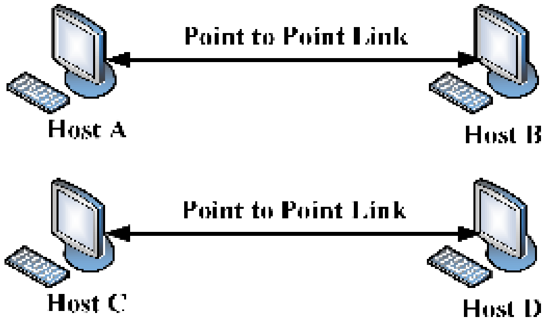
- Present era of data and information-centric operations, everything – starting from agriculture to military operations – relies heavily on information.
- The goodness of any particular information is as good as the variety and strength of the data, which generates this information.
- Networking refers to the networking 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 (IP addresses and MAC addresses).
- These hosts may be connected by a single path or through multiple paths for data sending and receiving.
- 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 - Type of Connection, Physical Topology, Reach of the Network.

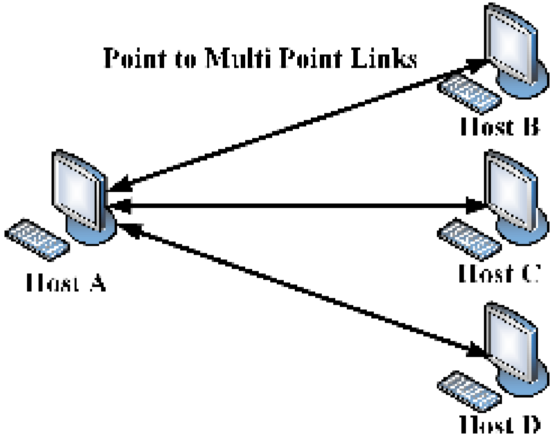
These classifications are helpful in deciding the requirements of network setup and provides insights into the appropriate selection of a network type for the setup.

Point to Point connection



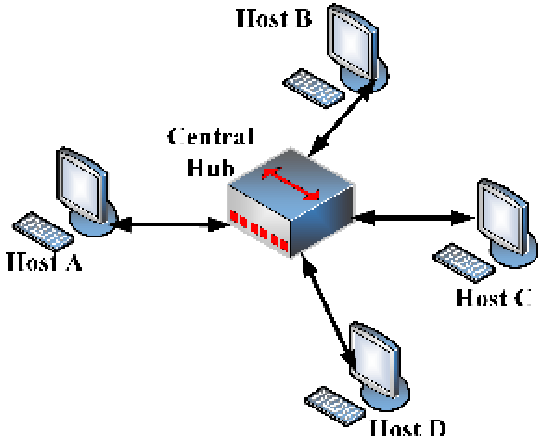
- Point to point connections are used to establish direct connections between two hosts.
- These networks were designed to work over duplex links, and are functional for both synchronous as well as asynchronous systems.
- Regarding computer networks, point to point connections find common usage for specific purposes such as in optical networks.

Point to Multipoint connection



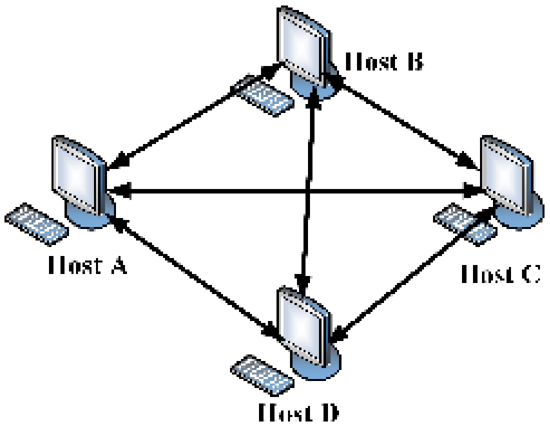
- More than two hosts share the same link. This configuration is similar to the one-to-many connection type.
- These types of connections find popular use in wireless networks and IP telephony.
- The channel is shared between the various hosts, either spatially (FDMA) or temporally (TDMA).

Star Topology



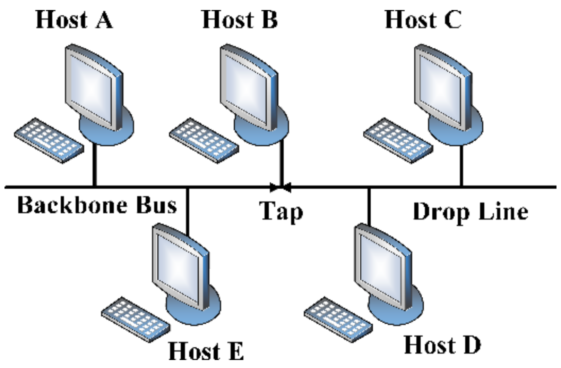
- For large-scale systems, the hub has to be essentially a powerful server to handle all the simultaneous traffic flowing through it.
- As there are fewer links (only one link per host), this topology is cheaper and easier to set up.
- The main advantage of the star topology is the easy installation of this network and the ease of fault identification within this network.

Mesh Topology



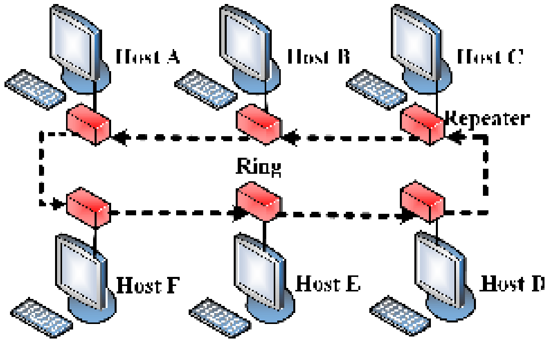
- This massive number of links makes this topology expensive.
- Allows for robustness and resilience of the system. Even in case a link is down or broken, the network is still fully functional as there remain other pathways for the traffic to flow through.

Bus Topology



- 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 its installation.
- There is a restriction on the length of the bus and the number of connections that can be simultaneously connected to the bus due to signal loss over the extended bus

Ring Topology



- The repeaters at each host capture the incoming signal intended for other hosts, regenerates the bit-stream, and passes it onto the next repeater.
- The fault identification and setup of this topology is quite simple and straightforward.
- The main disadvantage of this system is the high probability of a single point of failure.

Network Reachability

Computer networks are divided into four broad categories based on network reachability as,

- Personal Area Networks Local Area Networks Wide Area Networks
- Metropolitan Area Networks

Personal Area Networks

- PANs, as the name suggests, are restricted to individual usage mostly.
- 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 centimeters to a few meters.

Local Area Networks (LAN)

- A LAN is a collection of hosts connected to a single network through wired or wireless connections.
- However, LANs are restricted to buildings, organizations, or campuses. Typically, few leased lines connecting to the Internet provide web
- access to an organization or a campus, which is further redistributed to multiple hosts within the LAN enabling hosts, which are much more 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 between 100 Mbps to 1000 Mbps, with very high fault-tolerance levels.
- Commonly used network components in a LAN are servers, hubs, routers, switches, terminals, and computers

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 geographical location or city.
- An excellent example of a MAN is an Internet Service Provider (ISP) supplying Internet connectivity to various organizations within the reaches of 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.

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 the 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.

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 the ISO-OSI reference model and the Internet protocol suite.

ISO-OSI Model

The ISO-OSI model is a conceptual framework, which 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 in a bottom-up manner are

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

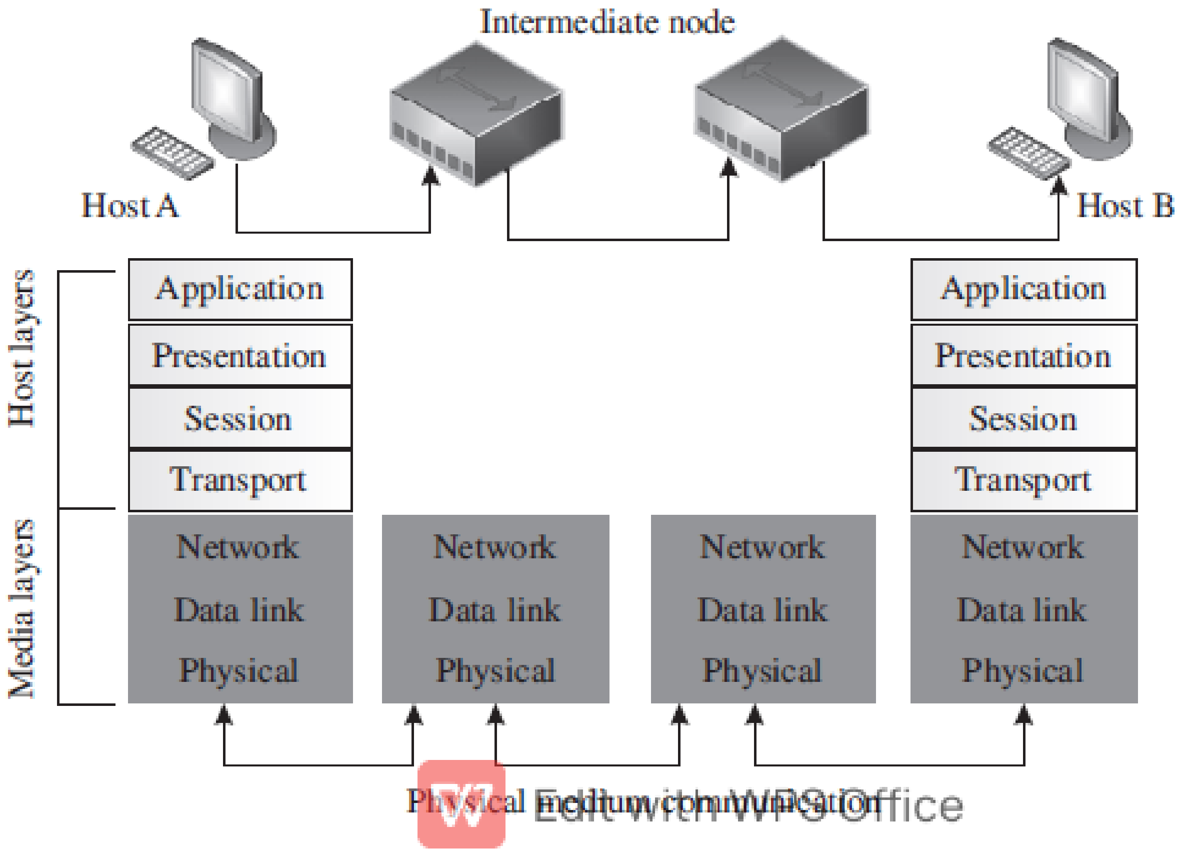
TCP/IP Suite

The Internet protocol suite is yet another conceptual framework, which 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,

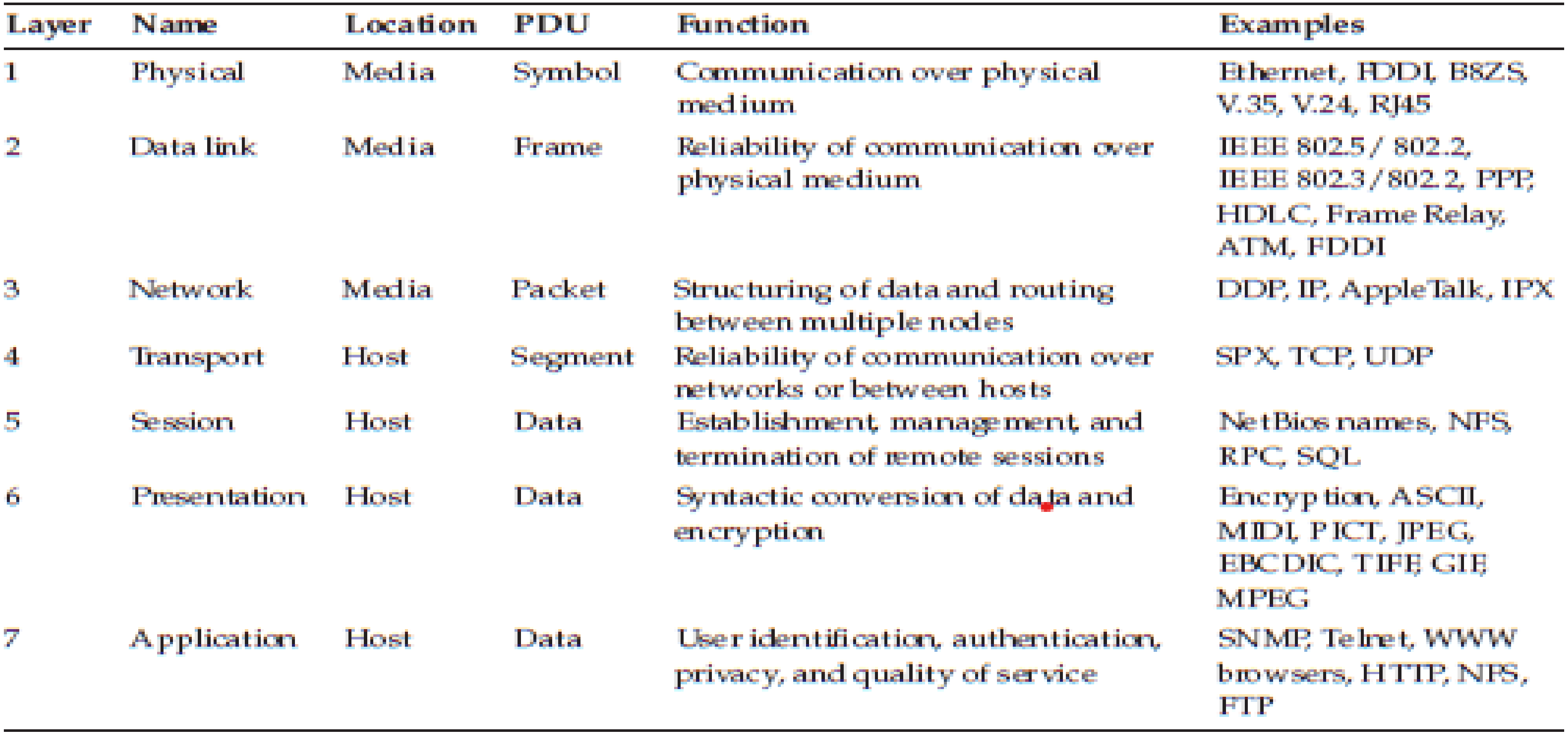
1. Link layer
2. Internet layer
3. Transport layer
4. Application layer

This collection of protocols is commonly referred to as the TCP/IP protocol suite as the foundation technologies of this suite are Transmission Control Protocol (TCP) and Internet Protocol (IP)

Networked communication between two hosts using the OSI model

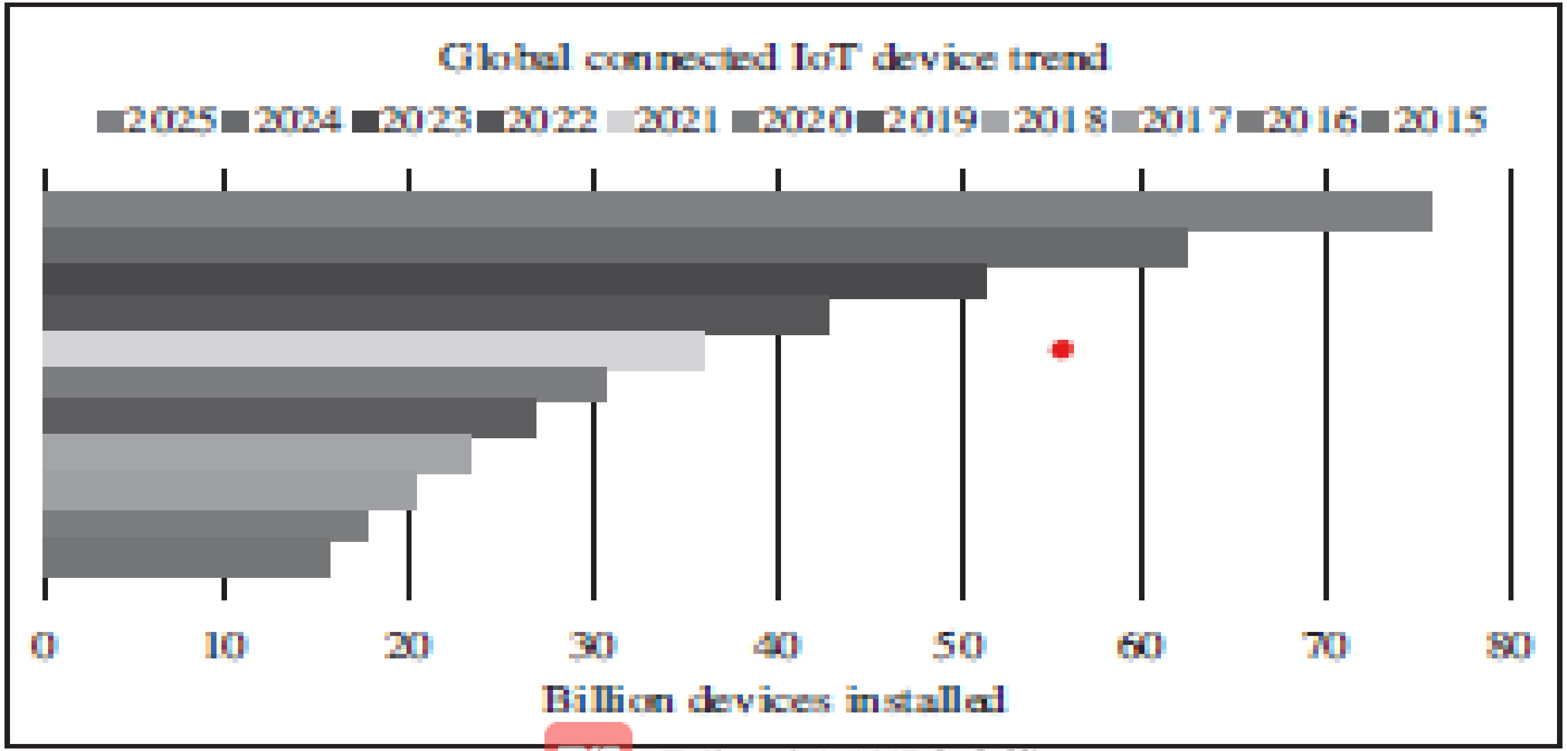


Summary of OSI and Its Features



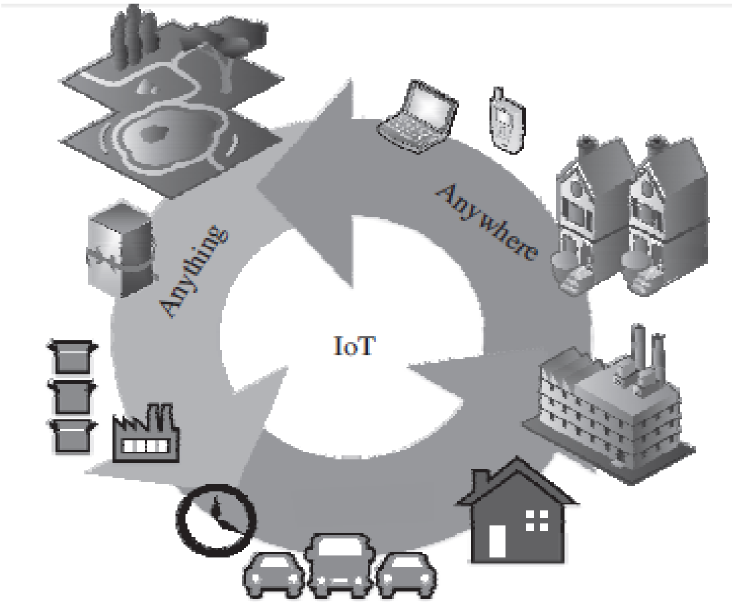
Layer	Name	Location	PDU	Function	Examples
1	Physical	Media	Symbol	Communication over physical medium	Ethernet, FDDI, B8ZS, V.35, V.24, RJ45
2	Data link	Media	Frame	Reliability of communication over physical medium	IEEE 802.5 / 802.2, IEEE 802.3 / 802.2, PPP, HDLC, Frame Relay, ATM, FDDI
3	Network	Media	Packet	Structuring of data and routing between multiple nodes	DDP, IP, AppleTalk, IPX
4	Transport	Host	Segment	Reliability of communication over networks or between hosts	SPX, TCP, UDP
5	Session	Host	Data	Establishment, management, and termination of remote sessions	NetBios names, NFS, RPC, SQL
6	Presentation	Host	Data	Syntactic conversion of data and encryption	Encryption, ASCII, MIDI, PICT, JPEG, EBCDIC, TIFF, GIF, MPEG
7	Application	Host	Data	User identification, authentication, privacy, and quality of service	SNMP, Telnet, WWW browsers, HTTP, NFS, FTP

10-years global trend and projection of connected devices



Basics of IOT

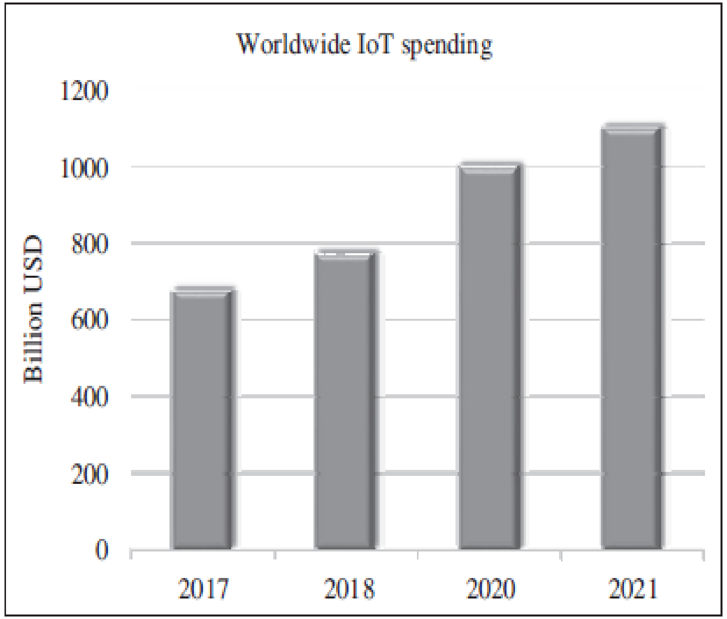
- IoT is an anytime, anywhere, and anything network of Internet-connected physical devices or systems capable of sensing an environment and affecting the sensed environment intelligently.
- This is generally achieved using low-power and low-form-factor embedded processors on-board the “things” connected to the Internet

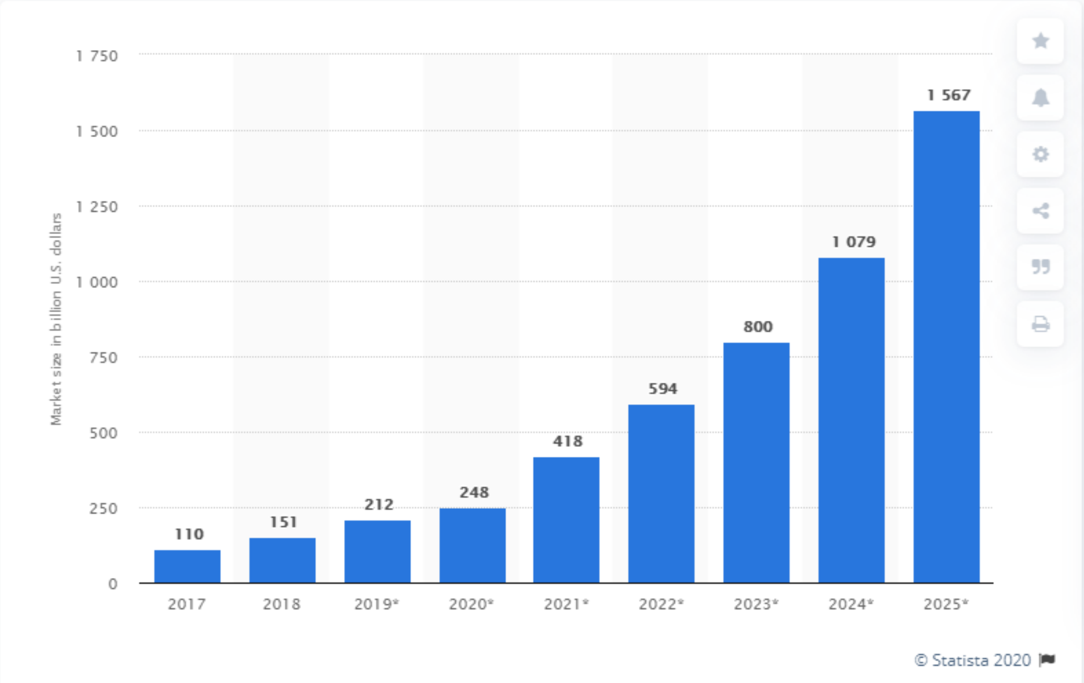


Typically, IoT systems can be characterized by the following features :

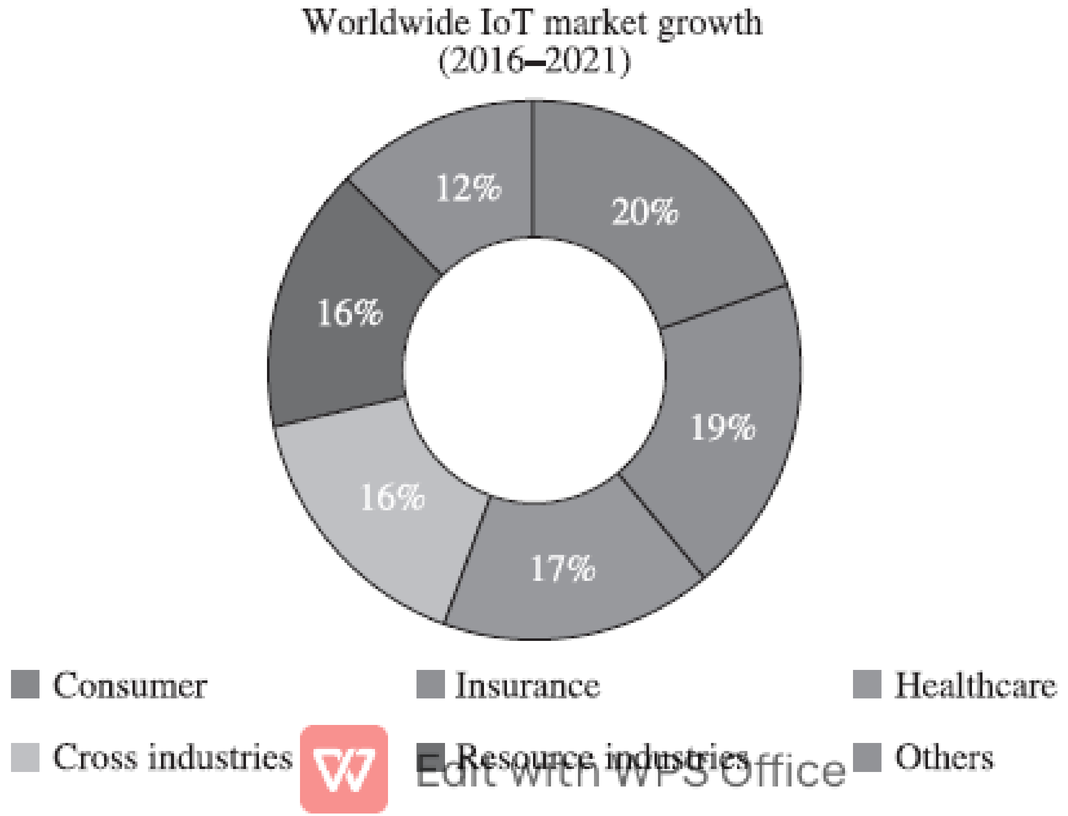
- Associated architectures, which are also efficient and scalable.
- No ambiguity in naming and addressing.
- Massive number of constrained devices, sleeping nodes, mobile devices, and non-IP devices.
- Intermittent and often unstable connectivity

The global IoT spending across various organizations and industries and its subsequent projection until the year 2021

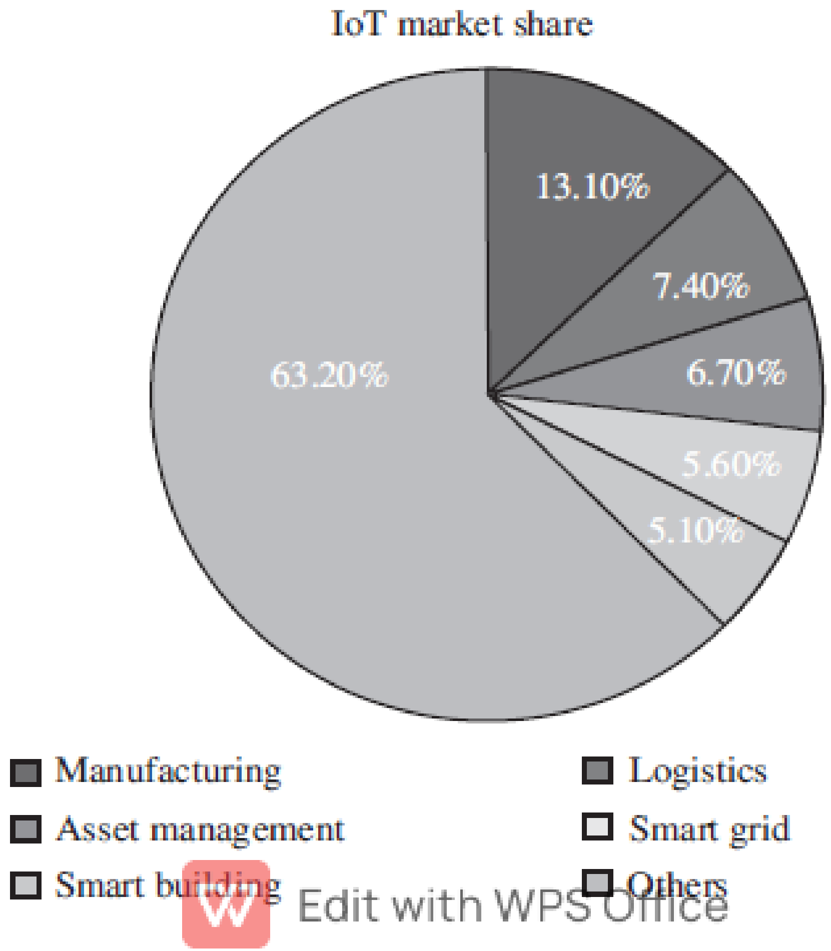




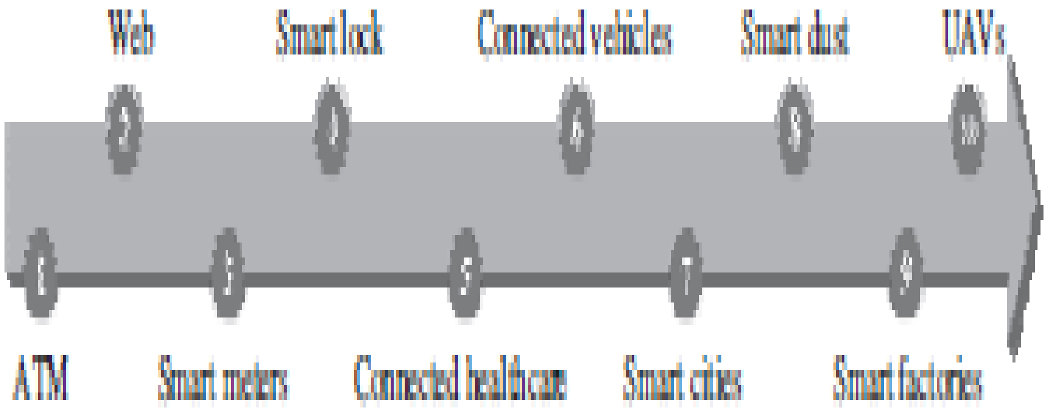
The Compound Annual Growth Rate (CAGR) of the IoT market



The IoT market share across various industries (statistics sourced from International Data Corporation)



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



- **ATM: Automated Teller Machines**
  - ✓ 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.
  - ✓ availability of financial transactions even when banks were closed beyond their regular work hours.
  - ✓ The first ATM became operational and connected online for the first time in 1974.
- Web: World Wide Web
  - ✓ global information sharing and communication platform.
  - ✓ started in1991.
  - ✓ responsible for the many revolutions in the field of computing and communication.
- Smart Meters:
  - ✓ started operation in 2000.
  - ✓ power meters are capable of communicating
  - ✓ remotely with the power grid.
  - ✓ Enables monitoring of power usage
  - ✓ easens the process of billing and power allocation from grids.

The Sequence of Technological Developments leading to the shaping of the modern- day IoT

Digital Locks

✓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,

Connected Healthcare

✓Healthcare devices connect 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.

✓Improves 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 the vehicle.

✓ can be used to self-diagnose themselves and alert owners about system failures.

Smart Cities:

✓city-wide implementation of smart sensing, monitoring,and actuation systems. dissemination.

✓parking, transportation, tracking, alert about accidents,Connected hospitals etc.

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

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.
- ✓smart dust can be sprayed to measure chemicals in the soil, or even to diagnose problems in the human body.

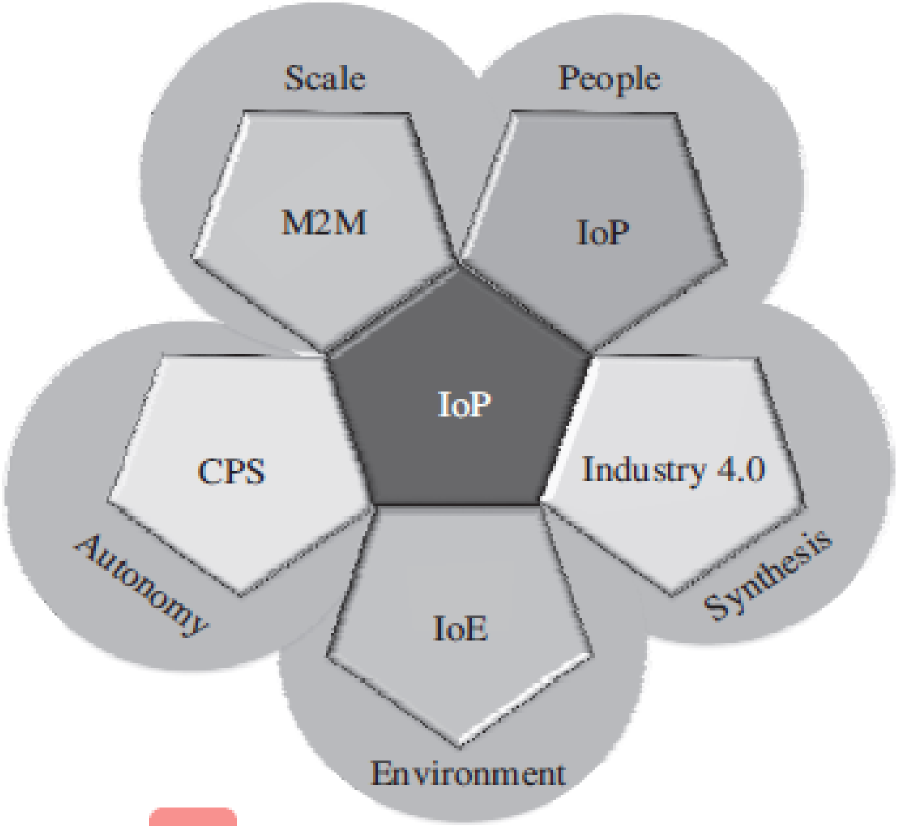
Smart Factories

- ✓factories can monitor plant processes, assembly lines, distribution lines, and manage factory floors all on their own.
- ✓Aids reduction in mishaps due to human errors in judgment or optimization of processes

Unmanned Aerial Vehicles

- ✓agriculture, surveys, surveillance, deliveries, stock maintenance, asset management etc

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



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, as shown in Figure 4.7. M2M standards occupy
- a core place in the IoT landscape. However, 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.

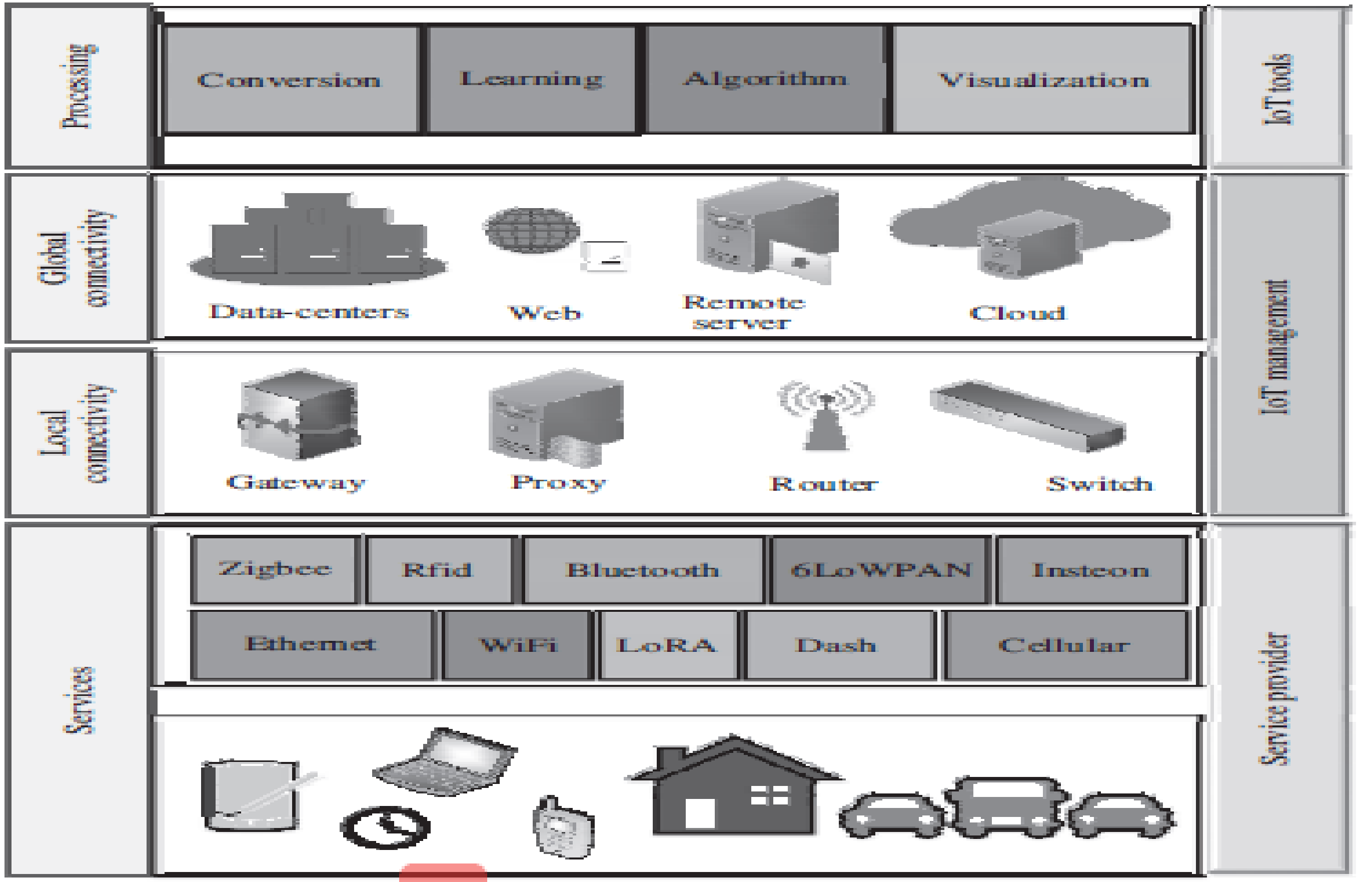
IoT versus CPS

- as a complete package. In other words, a digital twin is attached to a CPS-based
- system. As mentioned earlier, 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

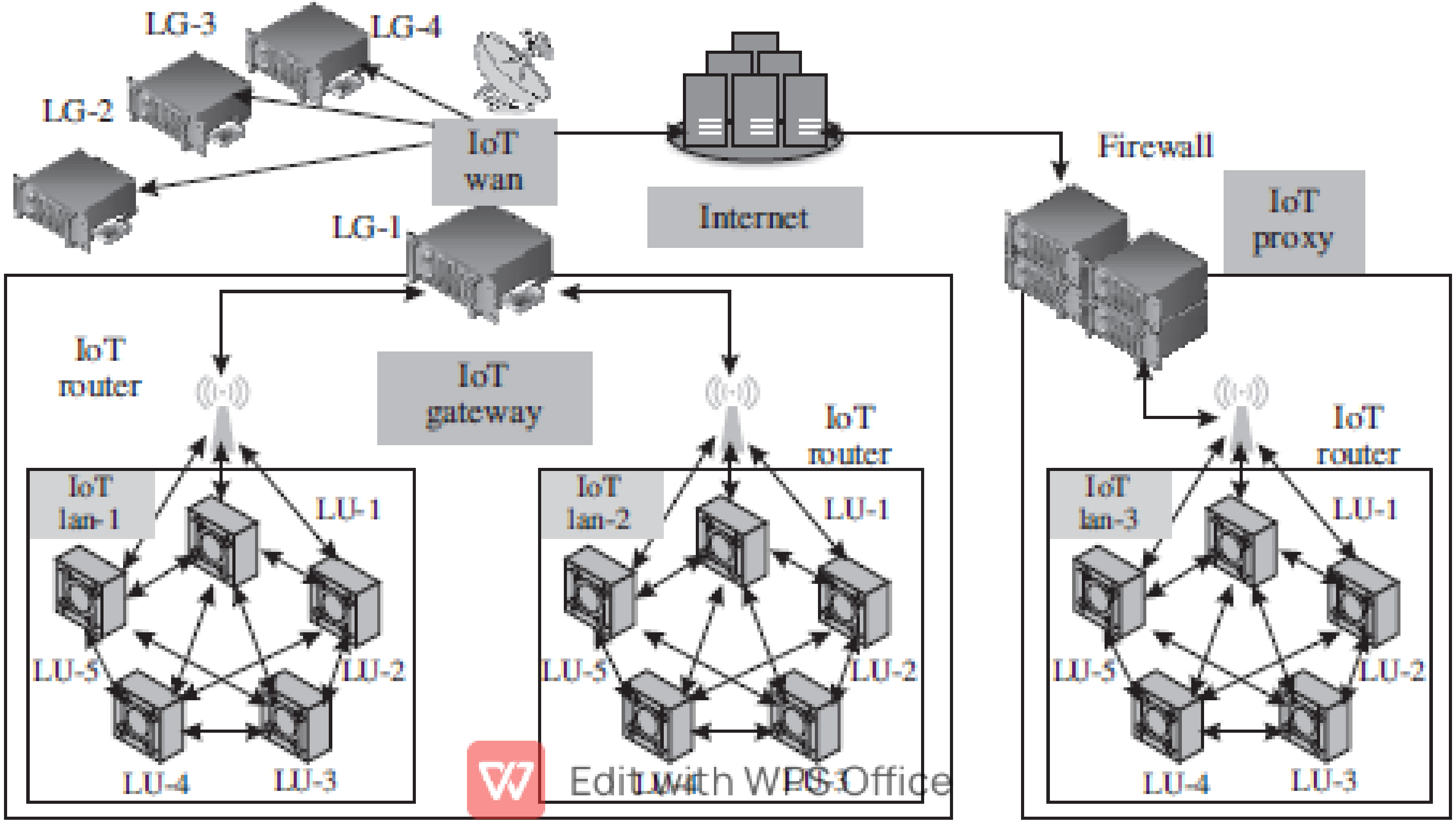
IoT versus WoT

- 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 ofWoT. 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 which includes non-IP-based systems that are
- not accessible through the web.

The IoT planes, various enablers of IoT, and their complex interdependencies



Typical IoT network ecosystem with various networking components



IoT Networking Components

- **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 gateway for that LAN. Connections outside the LAN are through gateways and proxies.
- **IoT Router**: An I oT 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.
- (iii) **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 Networking Components

- **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.
- (v) **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