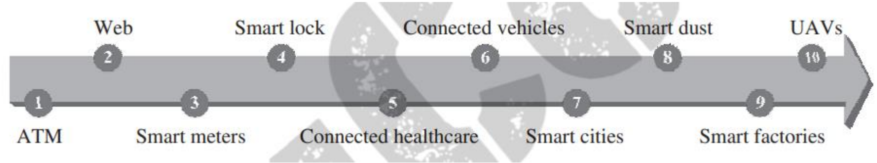
Model Question Paper-I/II with effect from 2023 – 24 (CBCS Scheme)

USN

Seven Semester B.E. Degree Examination Internet of Things (IOT)

TIME: 03 Hours **Max.Marks:100**

Note: Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE**.

		Module-1	***Bloom's Taxonomy Level**	**Marks**
Q.01	a	Explain Evolution of IoT. The technologies that laid the foundation of connected systems by achieving easy integration to daily lives, popular public acceptance, and massive benefits by using connected solutions can be considered as the founding solutions for the development of IoT.  Web Smart lock Connected vehicles Smart dust UAVs 2 4 6 8 10 1 3 5 7 9 ATM Smart meters Connected healthcare Smart cities Smart factories • ATM (1974) : 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 money dispensers. • Web (1991): World Wide Web is a global information sharing and communication platform. Since then, it has been massively responsible for the many revolutions in the field of computing and communication. • Smart Meters(2000) : The earliest smart meter was a power meter, which became operational.These power meters were capable of communicating remotely with the power grid. They enabled remote monitoring of subscribers' power usage and eased the process of billing and power allocation from grids. • 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. • Connected Healthcare: 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. • 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.	L1	6

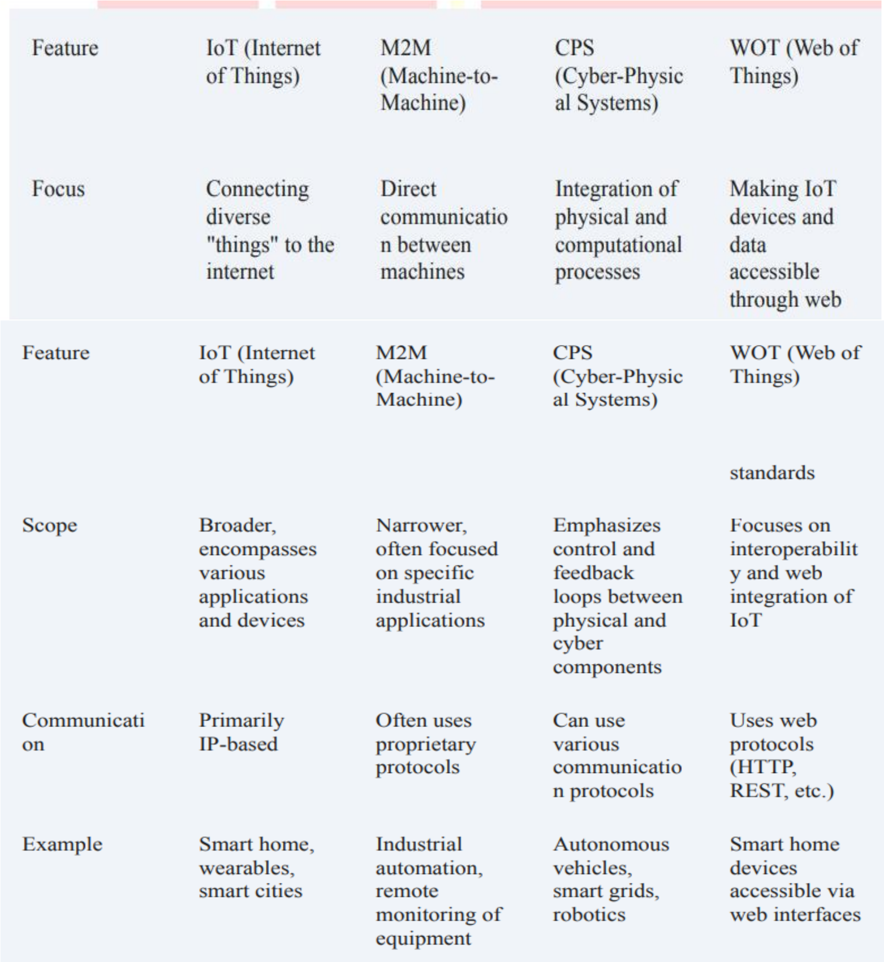
• Smart Cities: This is a city-wide implementation of smart sensing, monitoring, and actuation systems. Some other benefit are parking, transportation, and others.

• Smart Dust: They are microscopic computers. Smaller than a grain of sand each, they can be used in numerous beneficial ways, where regular computers cannot operate. Example: smart dust can be sprayed to measure chemicals in the soil or even to diagnose problems in the human body.

• Smart Factories: They 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 publicdomain solutions tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other tasks.

b Differentiate IoT versus M2M vs CPS vs WOT. L1 6

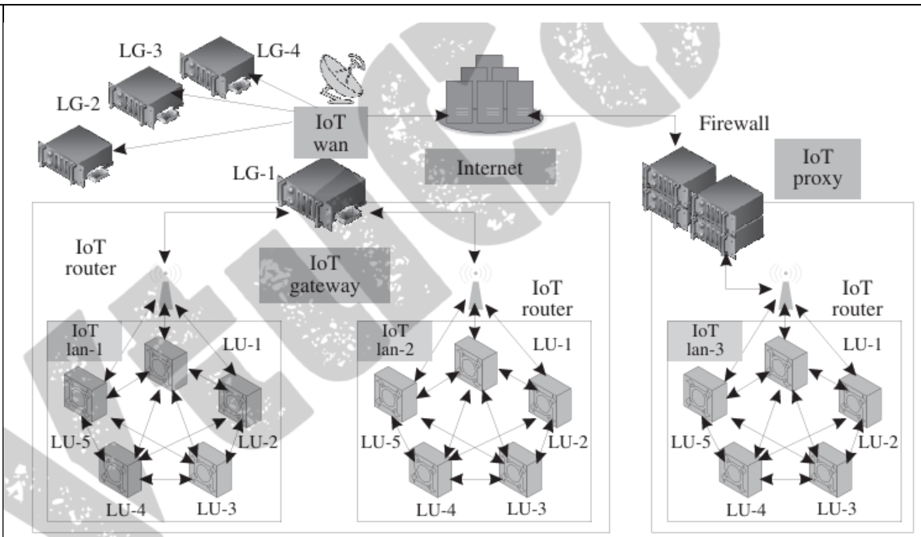


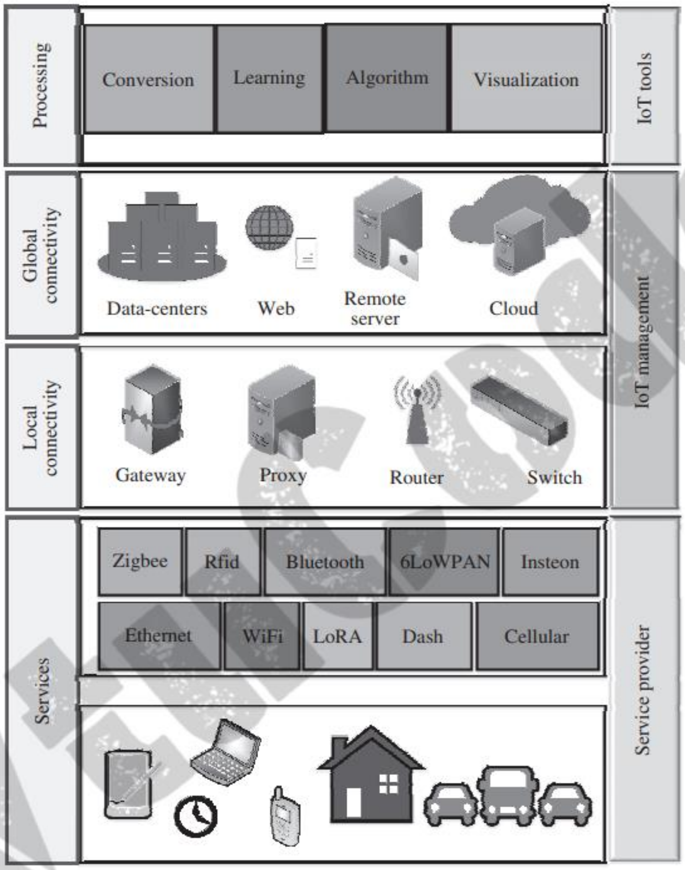
Feature	IoT (Internet of Things)	M2M (Machine-to-Machine)	CPS (Cyber-Physical Systems)	WOT (Web of Things)
Focus	Connecting diverse "things" to the internet	Direct communication between machines	Integration of physical and computational processes	Making IoT devices and data accessible through web standards
Scope	Broader, encompasses various applications and devices	Narrower, often focused on specific industrial applications	Emphasizes control and feedback loops between physical and cyber components	Focuses on interoperability and web integration of IoT
Communication	Primarily IP-based	Often uses proprietary protocols	Can use various communication protocols	Uses web protocols (HTTP, REST, etc.)
Example	Smart home, wearables, smart cities	Industrial automation, remote monitoring of equipment	Autonomous vehicles, smart grids, robotics	Smart home devices accessible via web interfaces

c Explain IoT Networking Components. L1 8

An IoT implementation is composed of several components, which may vary with their application domains. Broadly classify IoT network into six types:

1) IoT node, 2) IoT router, 3) IoT LAN, 4) IoT WAN, 5) IoT gateway, and 6) IoT proxy.

		 LG-3 LG-4 LG-2 IoT wan Internet Firewall IoT proxy LG-1 IoT router IoT gateway IoT router IoT router IoT lan-1 IoT lan-2 IoT lan-3 LU-1 LU-2 LU-3 LU-4 LU-5 (i)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. (ii) 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. (iv) 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.		
OR				
Q.02	a	What is IoT? Write the characteristics of IoT System. 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. 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. IoT systems can be characterized by the following features : • Associated architectures, which are also efficient and scalable. • No ambiguity in naming and addressing.	L1	5

		• Massive number of constrained devices, sleeping nodes, mobile devices, and non-IP devices. • Intermittent and often unstable connectivity.		
	b	With a neat diagram explain the interdependency technology for IoT Planes. We can divide the IoT paradigm into four planes: services, local connectivity, global connectivity, and processing.  Processing Conversion Learning Algorithm Visualization IoT tools Global connectivity Data-centers Web Remote server Cloud IoT management Local connectivity Gateway Proxy Router Switch Services Zigbee Rfid Bluetooth 6LoWPAN Insteon Ethernet WiFi LoRA Dash Cellular Service provider **Figure 4.8** The IoT planes, various enablers of IoT, and the complex interdependencies among them **Services Plane:** • The service plane is composed of two parts: 1) things or devices and 2) low-power connectivity. • The services offered in this layer are a combination of things and low-power connectivity. Example, any IoT application requires the basic setup of sensing, followed by rudimentary processing , 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 others. • The immediate low-power connectivity, which is responsible for connecting the things in local implementation, may be legacy protocols such as WiFi, 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. **Local connectivity plane:** • The local connectivity is responsible for distributing Internet access to multiple local IoT deployments. • Provides services such as address management, device management, security, sleep scheduling, and others. Example, in a smart home environment, the first floor and the ground floor may have local IoT implementations, which have	L2	10

various things connected to the network via low-power, low-range connectivity technologies. The traffic from these two floors merges into a single router or a gateway. The total traffic intended for the Internet from a smart home leaves through a single gateway or router, which may be assigned a single global IP address This helps in the significant conservation of already limited global IP addresses.

- The local connectivity plane falls under the purview of IoT management as it directly deals with strategies to use/reuse addresses based on things and applications. The modern-day “edge computing” paradigm is deployed in conjunction with these first two planes: services and local connectivity.

Global connectivity plane:

- The 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, datacenters, remote servers, Cloud, and others make up this plane. The paradigm of “fog computing” lies between the planes of local connectivity and global connectivity. It often serves to manage the load of global connectivity infrastructure by offloading the computation nearer to the source of the data itself, which reduces the traffic load on the global Internet.

Processing 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 are 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 learning cognition algorithms, visualization and analysis .
- Various computing paradigms such as “big data”, “machine learning”, and others, fall within the scope of this domain.

c Explain Addressing Strategies in IoT. L1 5

Feature	IPv4	IPv6
Developed	IETF 1974	IETF1998
Address length (bits)	32	128
No. of Addresses	2^{32}	2^{128}
Notation	Dotted decimal	Hexadecimal
Dynamic allocation of addresses	DHCP	DHCPv6, SLAAC
IPSec	Optional	Compulsory
Header size	Variable	Fixed
Header checksum	Yes	No
Header options	Yes	No
Broadcast addresses	Yes	No
Multicast addresses	No	Yes
Feature	Focus on reliable transmission	Focus on addressing

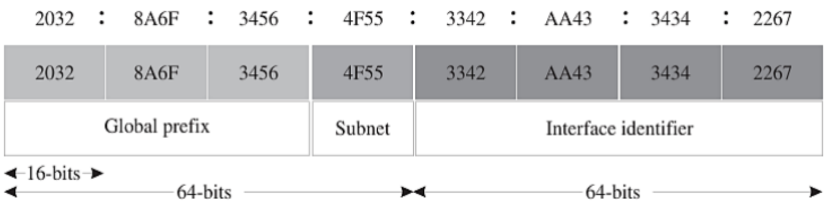


Fig.1.10 The IPv6 address format

The first three blocks are designated as the global prefix, which is globally unique. The next block is designated as the subnet prefix, which identifies the subnet of an interface/gateway through which LANs may be connected to the

Internet. Finally, the last four blocks (64 bits) of hexadecimal addresses are collectively known as the interface identifier (IID). IIDs may be generated based on MAC (media access control) identifiers of devices/nodes or using pseudo-random number generator algorithms. The IPv6 addresses can be divided into seven separate address types,

(i)**Global Unicast (GUA):** These addresses are assigned to single IoT entities/ interfaces; they enable the entities to transmit traffic to and from the Internet In regular IoT deployments, these addresses are assigned to gateways, proxies, or WANs.

(ii) **Multicast:** These addresses enable transmission of messages from a single networked entity to multiple destination entities simultaneously.

(iii) **Link Local (LL):** The operational domain of these addresses are valid only within a network segment such as LAN. These addresses may be repeated in other network segments/LANs, but are unique within that single network segment.

(iv) **Unique Local (ULA):** Similar to LL addresses, ULA cannot be routed over the Internet. These addresses may be repeated in other network segments/LANS but are unique within that single network segment.

(v) **Loopback:** It is also known as the localhost address. Typically, these addresses are used by developers and network testers for diagnostics and system checks.

(vi) **Unspecified:** Here, all the bits in the IPv6 address are set to zero and the destination address is not specified.

(vii) **Solicited-node Multicast**: It is a multicast address based on the IPv6 address of an IoT node or entity.

Module-2

Q.03 a With a neat diagram explain the working mechanism of actuator. L1 6

An actuator can be considered as a machine or system's component that can affect the movement or control the said mechanism or the system. Control systems affect changes to the environment or property they are controlling through actuators. The system activates the actuator through a control signal, which may be digital or analog. It elicits a response from the actuator, which is in the form of some form of mechanical motion. The control system of an actuator can be a mechanical or electronic system, a software-based system (e.g., an autonomous car control system), a human, or any other input. A remote user sends commands to a processor. The processor instructs a motor controlled robotic arm to perform the commanded tasks accordingly. The processor is primarily responsible for converting the human commands into sequential machine-language command sequences, which enables the robot to move. The robotic arm finally moves the designated boxes, which was its assigned task.

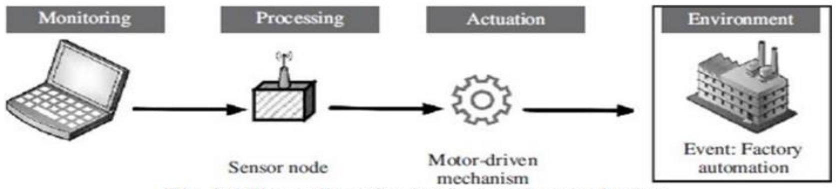


Fig. 2.5 The outline of a simple actuation mechanism

b Explain the types of actuators. L1 8

Actuators can be divided into seven classes: 1) Hydraulic, 2) pneumatic, 3) electrical, 4) thermal/magnetic, 5) mechanical, 6) soft, and 7) shape memory polymers.

1)Hydraulic actuators :

- It works on the principle of compression and decompression of fluids.
- These actuators facilitate mechanical tasks such as lifting loads through the use of hydraulic power derived from fluids in cylinders or fluid motors.
- The mechanical motion applied to a hydraulic actuator is converted to either linear, rotary, or oscillatory motion.

• The almost incompressible property of liquids is used in hydraulic actuators for exerting significant force.

• These hydraulic actuators are also considered as stiff systems.

2)Pneumatic actuators :

• It works on the principle of compression and decompression of gases.

• These actuators use a vacuum or compressed air at high pressure and convert it into either linear or rotary motion.

• Pneumatic rack and pinion actuators are commonly used for valve controls of water pipes. Pneumatic actuators are considered as compliant systems.

• The actuators using pneumatic energy for their operation are typically characterized by the quick response to starting and stopping signals.

• Small pressure changes can be used for generating large forces through these actuators. Pneumatic brakes are an example of this type of actuator which is so responsive that they can convert small pressure changes applied by drives to generate the massive force required to stop or slow down a moving vehicle. Pneumatic actuators are responsible for converting pressure into force.

• The power source in the pneumatic actuator does not need to be stored in reserve for its operation.

3)Electric actuators:

• The electric motors are used to power an electric actuator by generating mechanical torque. This generated torque is translated into the motion of a motor's shaft or for switching (as in relays).

• For example, actuating equipment's such as solenoid valves control the flow of water in pipes in response to electrical signals.

• This class of actuators is considered one of the cheapest, cleanest and speedy actuator types available.

4)Thermal or magnetic actuators:

• The use of thermal or magnetic energy is used for powering this class of actuators.

• These actuators have a very high-power density and are typically compact, lightweight, and economical.

• One classic example of thermal actuators is shape memory materials (SMMs) such as shape memory alloys (SMAs). • These actuators do not require electricity for actuation. They are not affected by vibration and can work with liquid or gases. • Magnetic shape memory alloys (MSMAs) are a type of magnetic actuators.

5)Mechanical actuators:

• In this, the rotary motion of the actuator is converted into linear motion to execute some movement.

• The use of gears, rails, pulleys, chains, and other devices are necessary for these actuators to operate.

• These actuators can be easily used in conjunction with pneumatic, hydraulic, or electrical actuators.

• They can also work in a standalone mode.

• The best example of a mechanical actuator is a rack and pinion mechanism.

6)Soft actuators:

• This (e.g., polymer-based) consists of elastomeric polymers that are used as embedded fixtures in flexible materials such as cloth, paper, fiber, particles, and others.

• The conversion of molecular level microscopic changes into tangible macroscopic deformations is the primary working principle of this class of actuators.

• These actuators have a high stake in modern-day robotics.

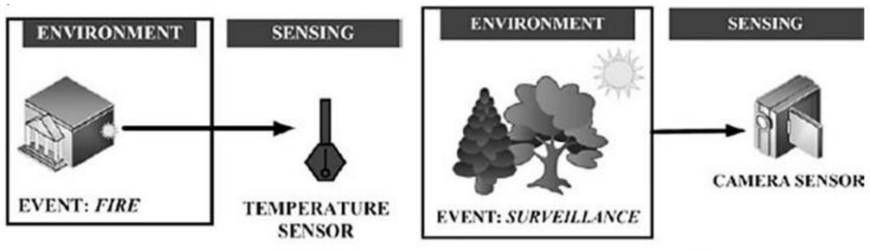
• They are designed to handle fragile objects such as agricultural fruit harvesting or performing precise operations like manipulating the internal organs during robotassisted surgeries.

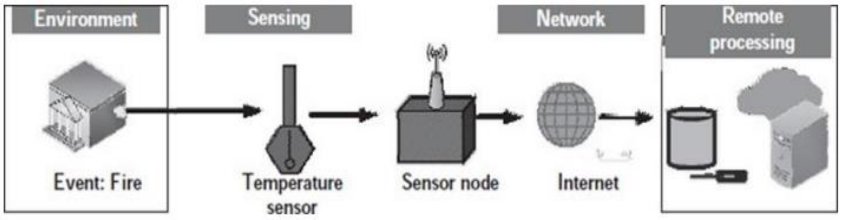
7) Shape Memory Polymers:

• These are considered as smart materials that respond to some external stimulus by changing their shape, and then revert to their original shape once

		the affecting stimulus is removed. • Features such as high strain recovery, biocompatibility, low density, and biodegradability characterize these materials. • Modern-day SMPs have been designed to respond to a wide range of stimuli such as pH changes, heat differentials, light intensity, and frequency changes, magnetic changes, and others. • Photopolymer/light-activated polymers (LAP) are a particular type of SMP, which require light as a stimulus to operate. LAP-based actuators are characterized by their rapid response times. Using only the variation of light frequency or its intensity, LAPs can be controlled remotely without any physical contact.		
	c	Define sensor and explain the characteristics of sensor. Sensors are devices that can measure, or quantify, or respond to the ambient changes in their environment or within the intended zone of their deployment. They generate responses to external stimuli or physical phenomenon through characterization of the input functions and their conversion into typically electrical signals. **Key characteristics of a sensor include:** ● Accuracy: How close the measured value is to the true value. ● Precision: The repeatability of measurements. ● Sensitivity: The change in output for a given change in input. ● Resolution: The smallest change in input that can be detected. ● Range: The minimum and maximum values of the input that the sensor can measure. ● Linearity: How linear the relationship is between the input and output. ● Response Time: How quickly the sensor responds to a change in input. ● Stability: The ability of the sensor to maintain its performance over time. ● Operating Temperature: The temperature range within which the sensor can operate reliably. **Properties are:** • Sensor Resolution: The smallest change in the measurable quantity that a sensor can detect is referred to as the resolution of a sensor. For digital sensors, the smallest change in the digital output that the sensor is capable of quantifying is its sensor resolution. The more the resolution of a sensor, the more accurate is the precision. A sensor's accuracy does not depend upon its resolution. For example, a temperature sensor A can detect up to 0.50 C changes in temperature, whereas another sensor B can detect up to 0.250 C changes in temperature. Therefore, the resolution of sensor B is higher than the resolution of sensor A. • Sensor Accuracy: The accuracy of a sensor is the ability of that sensor to measure the environment of a system as close to its true measure as possible. For example, a weight sensor detects the weight of a 100 kg mass as 99.98 kg. • Sensor Precision: The principle of repeatability governs the precision of a sensor. Only if, upon multiple repetitions, the sensor is found to have the same error rate, can it be deemed as highly precise. For example, consider if the same weight sensor described earlier reports measurements of 98.28 kg, 100.34 kg, and 101.11 kg upon three repeat measurements for a mass of actual weight of 100 kg. Here, the sensor precision is not deemed high because of significant variations in the temporal measurements for the same object under the same conditions.	L2	6
		OR		
Q.04	a	List and explain the characteristics of Actuators. A set of four characteristics can define all actuators: 1. Weight: • The physical weight of actuators limits its application scope. • For example, the use of heavier actuators is generally preferred for industrial applications and applications requiring no mobility of the IoT deployment. • In contrast, lightweight actuators typically find common usage in portable	L2	8

		systems in vehicles, drones, and home IoT applications. • It is to be noted that this is not always true. Heavier actuators also have selective usage in mobile systems, for example, landing gears and engine motors in aircraft. 2. Power Rating: • This helps in deciding the nature of the application with which an actuator can be associated. • The power rating defines the minimum and maximum operating power an actuator can safely withstand without damage to itself. Generally, it is indicated as the power-toweight ratio for actuators. • For example, smaller servo motors used in hobby projects typically have a maximum rating of 5 VDC, 500 mA, which is suitable for an operations-driven battery-based power source. Exceeding this limit might be detrimental to the performance of the actuator and may cause burnout of the motor. • In contrast to this, servo motors in larger applications have a rating of 460 VAC, 2:5 A, which requires standalone power supply systems for operations. It is to be noted that actuators with still higher ratings are available and vary according to application requirements. 3. Torque to Weight Ratio: • The ratio of torque to the weight of the moving part of an instrument/device is referred to as its torque/weight ratio. • This indicates the sensitivity of the actuator. Higher is the weight of the moving part; lower will be its torque to weight ratio for a given power. 4. Stiffness and Compliance : • The resistance of a material against deformation is known as its stiffness, whereas compliance of a material is the opposite of stiffness. • Stiffness can be directly related to the modulus of elasticity of that material. Stiff systems are considered more accurate than compliant systems as they have a faster response to the change in load applied to it. • For example, hydraulic systems are considered as stiff and non-compliant, whereas pneumatic systems are considered as compliant.		
	b	Explain the major factors influence the choice of sensors in IoT-based Sensing solutions. (i) Sensing Range: • The sensing range of a sensor node defines the detection fidelity of that node. • Typical approaches to optimize the sensing range in deployments include fixed kcoverage and dynamic k-coverage. • A lifelong fixed k-coverage tends to usher in redundancy as it requires a large number of sensor nodes, the sensing range of some of which may also overlap. In contrast, dynamic coverage incorporates mobile sensor nodes post detection of an event, which, however, is a costly solution and may not be deployable in all operational areas and terrains. • The sensing range of a sensor may also be used to signify the upper and lower bounds of a sensor’s measurement range. • For example, a proximity sensor has a typical sensing range of a couple of meters. In contrast, a camera has a sensing range varying between tens of meters to hundreds of meters. • As the complexity of the sensor and its sensing range goes up, its cost significantly increases. (ii) Accuracy and Precision: • The accuracy and precision of measurements provided by a sensor are critical in deciding the operations of specific functional processes. • Typically, off-the-shelf consumer sensors are low on requirements and often very cheap. However, their performance is limited to regular application domains. • For example, a standard temperature sensor can be easily integrated with	L1	8

		conventional components for hobby projects and day-to-day applications, but it is not suitable for industrial processes. Regular temperature sensors have a very low-temperature sensing range, as well as relatively low accuracy and precision. The use of these sensors in industrial applications, where a precision of up to 3–4 decimal places is required, cannot be facilitated by these sensors. • Industrial sensors are typically very sophisticated, and as a result, very costly. However, these industrial sensors have very high accuracy and precision score, even under harsh operating conditions. (iii)Energy : • The energy consumed by a sensing solution is crucial to determine the lifetime of that solution and the estimated cost of its deployment. • If the sensor or the sensor node is so energy inefficient that it requires replenishment of its energy sources quite frequently, the effort in maintaining the solution and its cost goes up; whereas its deployment feasibility goes down. • Consider a scenario where sensor nodes are deployed on the top of glaciers. Once deployed, access to these nodes is not possible. If the energy requirements of the sensor nodes are too high, such a deployment will not last long, and the solution will be highly infeasible as charging or changing of the energy sources of these sensor nodes is not an option. (iv)Device Size : • Modern-day IoT applications have a wide penetration in all domains of life. Most of the applications of IoT require sensing solutions which are so small that they do not hinder any of the regular activities that were possible before the sensor node deployment was carried out. • Larger the size of a sensor node, larger is the obstruction caused by it, higher is the cost and energy requirements, and lesser is its demand for the bulk of the IoT applications. • Consider a simple human activity detector. If the detection unit is too large to be carried or too bulky to cause hindrance to regular normal movements, the demand for this solution would be low. It is because of this that the onset of wearables took off so strongly. The wearable sensors are highly energy-efficient, small in size, and almost part of the wearer's regular wardrobe.		
	c	With a neat diagram explain scalar and Multimedia sensing techniques.  ENVIRONMENT SENSING EVENT: FIRE TEMPERATURE SENSOR ENVIRONMENT SENSING EVENT: SURVEILLANCE CAMERA SENSOR (a) Scalar sensing (b) Multimedia sensing 1)Scalar sensing: • Scalar sensing encompasses the sensing of features that can be quantified simply by measuring changes in the amplitude of the measured values with respect to time. • Quantities such as ambient temperature, current, atmospheric pressure, rainfall, light, humidity, flux, and others are considered as scalar values as they normally do not have a directional or spatial property assigned with them. • The sensors used for measuring these scalar quantities are referred to as scalar sensors, and the act is known as scalar sensing. 2) Multimedia sensing : • Multimedia sensing encompasses the sensing of features that have a spatial variance property associated with the property of temporal variance. • Unlike scalar sensors, multimedia sensors are used for capturing the changes	L1	4

		in amplitude of a quantifiable property concerning space (spatial) as well as time (temporal). • Quantities such as images, direction, flow, speed, acceleration, sound, force, mass, energy, and momentum have both directions as well as a magnitude. Additionally, these quantities follow the vector law of addition and hence are designated as vector quantities. They might have different values in different directions for the same working condition at the same time. • The sensors used for measuring these quantities are known as vector sensors.		
		Module-3		
Q.05	a	List and explain common data types in IoT applications. 1)Structured data : • These are typically text data that have a pre-defined structure. These are primarily created by using length-limited data fields such as phone numbers, social security numbers, and other such information. • Structured data are associated with relational database management systems (RDBMS). • Even if the data is human or machine generated, these data are easily searchable by querying algorithms as well as human generated queries. • Common usage of this type of data is associated with flight or train reservation systems, banking systems, inventory controls, and other similar systems. • Established languages such as Structured Query Language (SQL) are used for accessing these data in RDBMS. • However, in the context of IoT, structured data holds a minor share of the total generated data over the Internet. 2) Unstructured data: • In simple words, all the data on the Internet, which is not structured, is categorized as unstructured. • These data types have no pre-defined structure and can vary according to applications and data-generating sources. • Some of the common examples of human-generated unstructured data include text, emails, videos, images, phone recordings, chats, and others. • Some common examples of machine-generated unstructured data include sensor data from traffic, buildings, industries, satellite imagery, surveillance videos, and others. • As already evident from its examples, this data type does not have fixed formats associated with it, which makes it very difficult for querying algorithms to perform a look-up. • Querying languages such as NoSQL are generally used for this data type.	L1	5
	b	With a neat diagram explain offsite processing topology.  Environment Sensing Network Remote processing Event: Fire Temperature sensor Sensor node Internet Fig.3.3 Event detection using an off-site remote processing topology • The off-site processing paradigm, as opposed to the on-site processing paradigms, allows for latencies (due to processing or network latencies); it is significantly cheaper than on-site processing topologies. • This difference in cost is mainly due to the low demands and requirements of processing at the source itself. • Often, the sensor nodes are not required to process data on an urgent basis, so having a dedicated and expensive on-site processing infrastructure is not sustainable for largescale deployments typical of IoT deployments.	L1	10

		• In the off-site processing topology, the sensor node is responsible for the collection and framing of data that is eventually to be transmitted to another location for processing. • Unlike the on-site processing topology, the off-site topology has a few dedicated high processing enabled devices, which can be borrowed by multiple simpler sensor nodes to accomplish their tasks. At the same time, this arrangement keeps the costs of largescale deployments extremely manageable. • In the off-site topology, the data from these sensor nodes (data generating sources) is transmitted either to a remote location (which can either be a server or a cloud) or to multiple processing nodes. Multiple nodes can come together to share their processing power in order to collaboratively process the data (which is important in case a feasible communication pathway or connection to a remote location cannot be established by a single node).		
	c	Write a short note on offloading considerations. There are a few offloading parameters which need to be considered while deciding upon the offloading type to choose. Some of these parameters are as follows. • Bandwidth: The maximum amount of data that can be simultaneously transmitted over the network between two points is the bandwidth of that network. The bandwidth of a wired or wireless network is also considered to be its data-carrying capacity and often used to describe the data rate of that network. • Latency: It is the time delay incurred between the start and completion of an operation. In the present context, latency can be due to the network (network latency) or the processor (processing latency). In either case, latency arises due to the physical limitations of the infrastructure, which is associated with an operation. The operation can be data transfer over a network or processing of a data at a processor. • Criticality: It defines the importance of a task being pursued by an IoT application. The more critical a task is, the lesser latency is expected from the IoT solution. For example, detection of fires using an IoT solution has higher criticality than detection of agricultural field parameters. The former requires a response time in the tune of milliseconds, whereas the latter can be addressed within hours or even days. • Resources: It signifies the actual capabilities of an offload location. These capabilities may be the processing power, the suite of analytical algorithms, and others. For example, it is futile and wasteful to allocate processing resources reserved for realtime multimedia processing (which are highly energy-intensive and can process and analyze huge volumes of data in a short duration) to scalar data (which can be addressed using nominal resources without wasting much energy). • Data volume: The amount of data generated by a source or sources that can be simultaneously handled by the offload location is referred to as its data volume handling capacity. Typically, for large and dense IoT deployments, the offload location should be robust enough to address the processing issues related to massive data volumes.	L1	5

		OR		
Q.06	a	With a neat diagram explain onsite processing topology. • The on-site processing topology signifies that the data is processed at the source itself. • This is crucial in applications that have a very low tolerance for latencies. These latencies may result from the processing hardware or the network (during transmission of the data for processing away from the processor). • Applications such as those associated with healthcare and flight control systems (realtime systems) have a breakneck data generation rate. These additionally show rapid temporal changes that can be missed (leading to	L1	5

catastrophic damages) unless the processing infrastructure is fast and robust enough to handle such data.

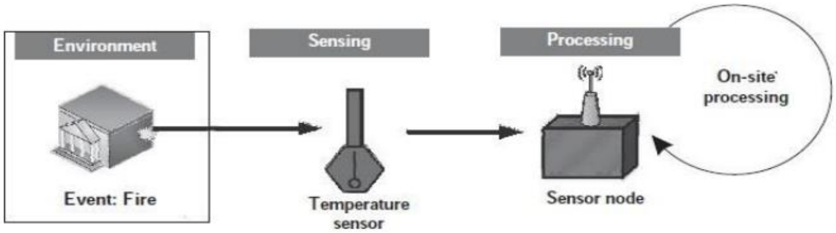


Fig. 3.2 Event detection using an on-site processing topology

b Explain IoT Device Design and Selection Considerations. L2 8

The main consideration of minutely defining an IoT solution is the selection of the processor for developing the sensing solution . This selection is governed by many parameters that affect the usability, design, and affordability of the designed IoT sensing and processing solution. The main factor governing the IoT device design and selection for various applicationsis the processor.

The other important considerations are as follows,

• Size: This is one of the crucial factors for deciding the form factor and the energy consumption of a sensor node. It has been observed that larger the form factor, larger is the energy consumption of the hardware. Additionally, large form factors are not suitable for a significant bulk of IoT applications, which rely on minimal form factor solutions (e.g., wearables).

• Energy: The energy requirements of a processor is the most important deciding factor in designing IoT-based sensing solutions. Higher the energy requirements, higher is the energy source (battery) replacement frequency. This principle automatically lowers the long-term sustainability of sensing hardware, especially for IoT-based applications.

• Cost: The cost of a processor, besides the cost of sensors, is the driving force in deciding the density of deployment of sensor nodes for IoT-based solutions. Cheaper cost of the hardware enables a much higher density of hardware deployment by users of an IoT solution. For example, cheaper gas and fire detection solutions would enable users to include much more sensing hardware for a lesser cost.

• Memory: The memory requirements (both volatile and non-volatile memory) of IoT devices determines the capabilities the device can be armed with. Features such as local data processing, data storage, data filtering, data formatting, and a host of other features rely heavily on the memory capabilities of devices. The devices with higher memory tend to be costlier for obvious reasons.

• Processing power: As covered in earlier sections, processing power is vital in deciding what type of sensors can be accommodated with the IoT device/node, and what processing features can integrate on-site with the IoT device. The processing power also decides the type of applications the device can be associated with. The applications that handle video and image data require IoT devices with higher processing power as compared to applications requiring simple sensing of the environment.

• I/O rating: The input–output (I/O) rating of IoT device, primarily the processor, is the deciding factor in determining the circuit complexity, energy usage, and requirements for support of various sensing solutions and sensor types. Newer processors have a meager I/O voltage rating of 3.3 V, as compared to 5 V for the somewhat older processors. This translates to requiring additional voltage and logic conversion circuitry to interface legacy technologies and sensors with the newer processors. Despite low power consumption due to reduced I/O voltage levels, this additional voltage and circuitry not only affects the complexity of the circuits but also affects the costs.

• Add-ons: The support of various add-ons a processor or for that matter, an IoT device provides, such as analog to digital conversion (ADC) units, in-built

		clock circuits, connections to USB and ethernet, inbuilt wireless access capabilities, and others helps in defining the robustness and usability of a processor or IoT device in various application scenarios.		
	c	Write a short note on offload location and offload decision making. **Offload location:** The choice of offload location decides the applicability, cost, and sustainability of the IoT application and deployment. The offload location divided into four types: • Edge: Offloading processing to the edge implies that the data processing is facilitated to a location at or near the source of data generation itself. Offloading to the edge is done to achieve aggregation, manipulation, bandwidth reduction, and other data operations directly on an IoT device. • Fog: Fog computing is a decentralized computing infrastructure that is utilized to conserve network bandwidth, reduce latencies, restrict the amount of data unnecessarily flowing through the Internet, and enable rapid mobility support for IoT devices. The data, computing, storage and applications are shifted to a place between the data source and the cloud resulting in significantly reduced latencies and network bandwidth usage. • Remote Server: A simple remote server with good processing power may be used with IoT based applications to offload the processing from resource constrained IoT devices. Rapid scalability may be an issue with remote servers, and they may be costlier and hard to maintain in comparison to solutions such as the cloud. • Cloud: Cloud computing is a configurable computer system, which can get access to configurable resources, platforms, and high-level services through a shared pool hosted remotely. Cloud enables massive scalability of solutions as they can enable resource enhancement allocated to a user or solution in an on-demand manner, without the user having to go through the pains of acquiring and configuring new and costly hardware. **Offload decision making** : The choice of where to offload and how much to offload is one of the major deciding factors in the deployment of an offsite-processing topology-based IoT deployment architecture. Some of these approaches are as follows. • Naive Approach: This approach is typically a hard approach, without too much decision making. It can be considered as a rule-based approach in which the data from IoT devices are offloaded to the nearest location based on the achievement of certain offload criteria. Although easy to implement, this approach is never recommended, especially for dense deployments, or deployments where the data generation rate is high, or the data being offloaded in complex to handle (multimedia or hybrid data types). Generally, statistical measures are consulted for generating the rules for offload decision making. • Bargaining based approach: This approach, although a bit processing-intensive during the decision-making stages, enables the alleviation of network traffic congestion, enhances service QoS (quality of service) parameters such as bandwidth, latencies, and others. At times, while trying to maximize multiple parameters for the whole IoT implementation, in order to provide the most optimal solution or QoS, not all parameters can be treated with equal importance. Bargaining based solutions try to maximize the QoS by trying to reach a point where the qualities of certain parameters are reduced, while the others are enhanced. Example: Game theory . • Learning based approach: The learningbased approaches generally rely on past behavior and trends of data flow through the IoT architecture. The optimization of QoS parameters is pursued by learning from historical trends and trying to optimize previous solutions further and enhance the collective behavior of the IoT implementation. The memory requirements and processing requirements are high during the decision-making stages. The most common example of a learning-based approach is machine learning.	L1	7

<table>
<tr><th></th><th></th><th>Module-4</th><th></th><th></th></tr>
<tr><td>Q.07</td><td>a</td><td>

Explain the IEEE 802.15.4.

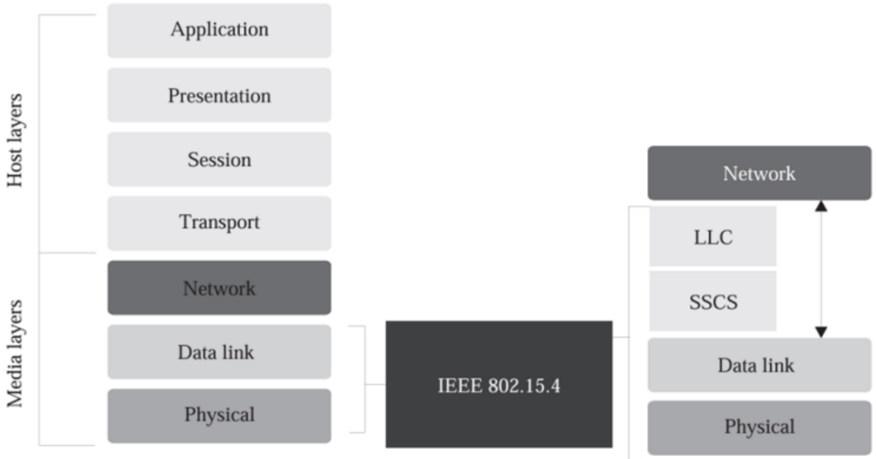


Fig. 4.1 The operational part of IEEE 802.5.4's protocol stack in comparison to the OSI stack.

• The IEEE 802.15.4 standard represents the most popular standard for low data rate wireless personal area networks (WPAN).

• This standard was developed to enable monitoring and control applications with lower data rate and extend the operational life for uses with low-power consumption.

• This standard uses only the first two layers—physical and data link—for operation along with two new layers above it: 1) logical link control (LLC) and 2) servicespecific convergence sublayer (SSCS). The additional layers help in the communication of the lower layers with the upper layers.

• The IEEE 802.15.4 standard was curated to operate in the ISM (industrial, scientific, and medical) band.

• The direct sequence spread spectrum (DSSS) modulation technique is used for communication purposes, enabling a wider bandwidth of operation with enhanced security by the modulating pseudo-random noise signal. This standard exhibit high tolerance to noise and interference and offers better measures for improving link reliability.

• Typically, the low-speed versions of the IEEE 802.15.4 standard use binary phase shift keying (BPSK), whereas the versions with high data rate implement offset quadrature phase shift keying (O-QPSK) for encoding the message to be communicated.

• Carrier sense multiple access with collision avoidance (CSMA-CA) is the channel access method used for maintaining the sequence of transmitted signals and preventing deadlocks due to multiple sources trying to access the same channel.

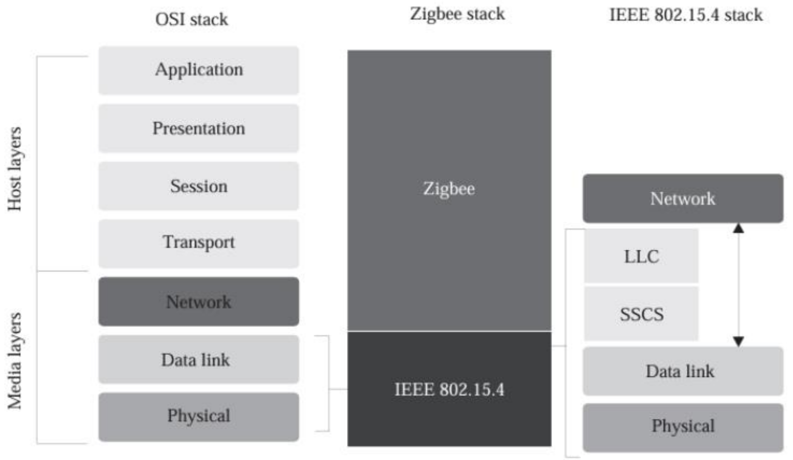
• The transmission, for most cases, is line of sight (LOS), with the standard transmission range varying between 10 m to 75 m. The best-case transmission range achieved outdoors can be up to 1000 m.

• This standard typically defines two networking topologies: 1) Star and 2) mesh.

• There are seven variants identified with in IEEE 802.15.4—A, B. C, D, E, F, and G. Variants A/B are the base versions, C is assigned for China, and D for Japan. Variants E, F, and G are assigned respectively for industrial applications, active RFID (radio frequency identification) uses, and smart utility systems.

• The IEEE 802.15.4 standard supports two types of devices: 1) reduced function device (RFD) and 2) full function devices (FFD). FFDs can talk to all types of devices and support full protocol stacks. However, these devices are costly and energy consuming due to increased requirements for support of full stacks.

</td><td>L1</td><td>8</td></tr>
<tr><td></td><td>b</td><td>Explain the protocol stack of Zigbee and Describe the Zigbee Network layer.</td><td>L2</td><td>5</td></tr>
</table>

		 OSI stack Zigbee stack IEEE 802.15.4 stack Host layers Media layers Application Presentation Session Transport Network Data link Physical Zigbee IEEE 802.15.4 Network LLC SSCS Data link Physical Fig.4.5 The Zigbee protocol stack in comparison to the OSI stack Physical Layer: This layer is tasked with transmitting and receiving signals, and Performing modulation and demodulation operations on them, respectively. The Zigbee physical layer consists of 3 bands made up of 27 channels: the 2.4 GHz band has 16 channels at 250 kbps the 868.3 MHz has one channel at 20 kbps; and the 902-928 MHz has ten channels at 40 kbps. MAC Layer: This layer ensures channel access and reliability of data transmission. CSMACA is used for channel access and intra-channel interference avoidance. This layer handles communication synchronization using beacon frames. Network Layer: This layer handles operations such as setting up the network, connecting and disconnecting the devices, configuring the devices, and routing. Application Support Sub-Layer: This layer handles the interfacing services, control services, bridge between network and other layers, and enables the necessary services to interface with the lower layers. This layer is primarily tasked with data management services and is responsible for service-based device matching. Application Framework: Two types of data services are provided by the application framework: provision of a key-value pair and generation of generic messages. A key-value pair is used for getting attributes within the application objects, whereas a generic message is a developer-defined structure.		
	c	What is RFID? Explain its working. • RFID stands for radio frequency identification. • This technology uses tags and readers for communication. RFID tags have data encoded onto them digitally. The RFID readers can read the values encoded in these tags without physically touching them. • RFIDs are functionally similar to barcodes as the data read from tags are stored in a database. However, RFID does not have to rely on, line of sight operation, unlike barcodes. • The automatic identification and data capture (AIDC) technology can be considered as the precursor of RFID. Similar to AIDC techniques, RFID systems are capable of automatically categorizing objects. Categorization tasks such as identifying tags, reading data, and feeding the read data directly into computer systems through radio waves outline the operation of RFID systems. • RFID systems are made Up of three components: 1) RFID tag or smart label, 2) RFID reader, and 3) an antenna. • In RFID, the tags consist of an integrated circuit and an antenna, enclosed in a protective casing to protect from wear and tear and environmental effects. These tags can be either active or passive. Passive tags find common usage in a variety of applications due to its low cost; however, it has to be powered using an RFID reader before data transmission. Active tags have their own	L1	7

power sources and do not need external activation by readers.

• Tags are used for transmitting the data to an RFID interrogator or an RFID reader. The radio waves are then converted to a more usable form of data by this reader.

• A host computer system accesses the collected data on the reader by a communication technology such as Wi-Fi or Ethernet.

• The data on the host system is finally updated onto a database. RFID applications span across domains such as inventory management, asset tracking, personnel tracking, and supply chain management.

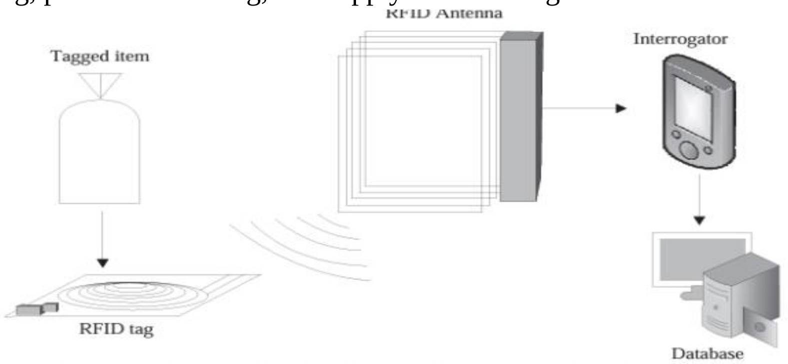


Fig.4.12 An outline of the RFID operation and communication

OR

Q.08 a With a neat diagram explain deployment and communication architecture of LoRa. L1 8

• LoRa or long range is a patented wireless technology for communication developed by Cycleo of Grenoble, France for cellular-type communications aimed at providing connectivity to M2M and IoT solutions.

• It is a sub-GHz wireless technology that operationally uses the 169 MHz, 433 MHz, 868 MHz, and 915 MHz frequency bands for communication.

• LoRa uses bi-directional communication links symmetrically and a spread spectrum with a 125 kHz wideband for operating.

• Applications such as electric grid monitoring are typically suited for utilizing LoRa for communications.

• Typical communication of LoRa devices ranges from 15 to 20 km, with support for millions of devices.

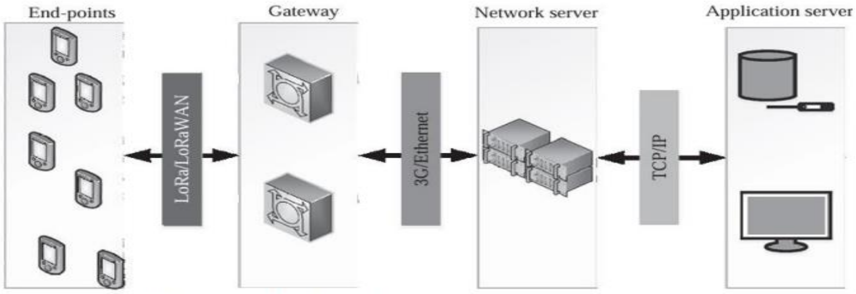


Figure 4.21 A typical LoRa deployment and communication architecture

• LoRa achieves high receiver sensitivity by utilizing frequency-modulated chirp coding gain.

• LoRa devices provide excellent support for mobility, which makes them very useful for applications such as asset tracking and asset management.

b Explain the IEEE 802.11Wi-Fi stack and Wi-Fi deployment architecture. L1 5

• Wi-Fi or WiFi is technically referred to by its standard, IEEE 802.11, and is a wireless technology for wireless local area networking of nodes and devices built upon similar standards (Figure 4.25).

• Wi-Fi utilizes the 2.4 GHz ultra-high frequency (UHF) band or the 5.8 GHz super high frequency (SHF) ISM radio bands for communication. For operation, these bands in Wi-Fi are subdivided into multiple channels. The communication over each of these channels is achieved by multiple devices simultaneously using time-sharing based TDMA multiplexing. It uses

CSMA/CA for channel access.

• Various versions of IEEE 802.11 have been popularly adapted, such as a/b/g/n. The IEEE 802.11a achieves a data rate of 54 Mbps and works on the 5 GHz band using OFDM for communication. IEEE802.11bachieves a data rate of 11 Mbps and operates on the 2.4 GHz band.

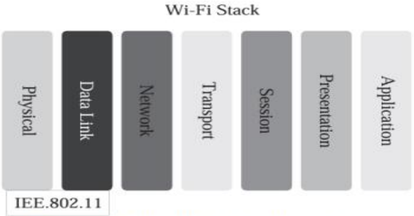


Figure 4.25 The IEEE 802.11 Wi-Fi stack

Wi-Fi devices can network using a technology referred to as wireless LAN (WLAN), as shown in Figure 4.26. A Wi-Fi enabled device must connect to a wireless access point, which connects the device to the WLAN. WLAN is then responsible for forwarding the messages from the devices to and fro between the devices and the Internet.

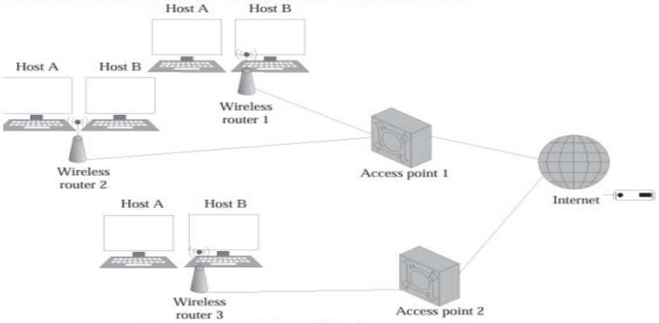


Figure 4.26 The Wi-Fi deployment architecture

c

Explain Bluetooth protocol stack.

L1

7

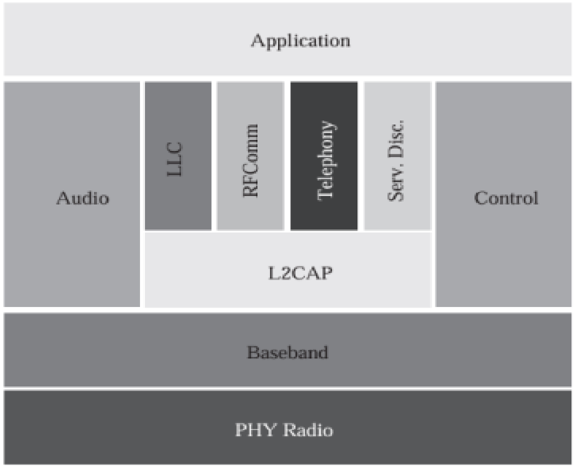
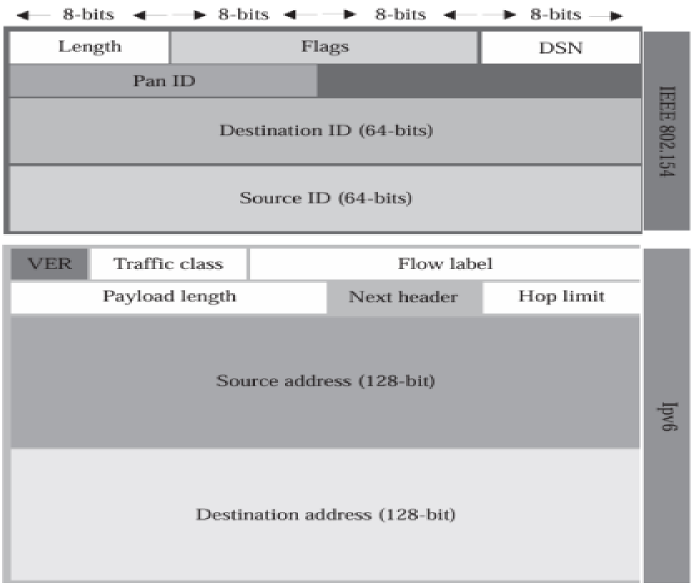


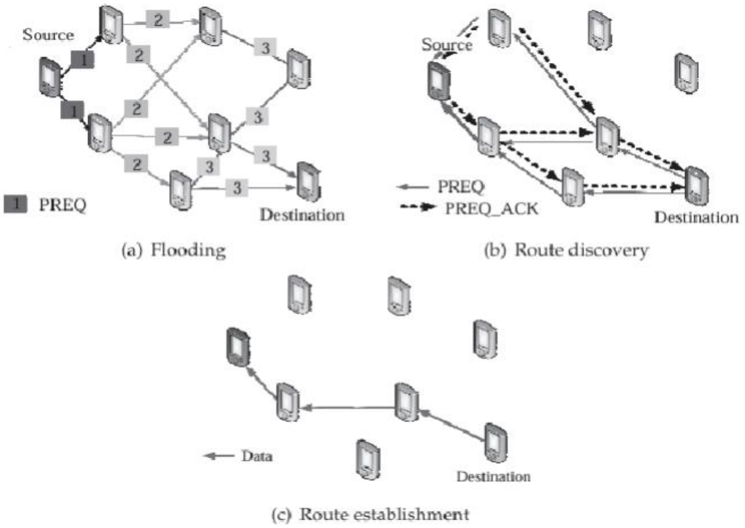
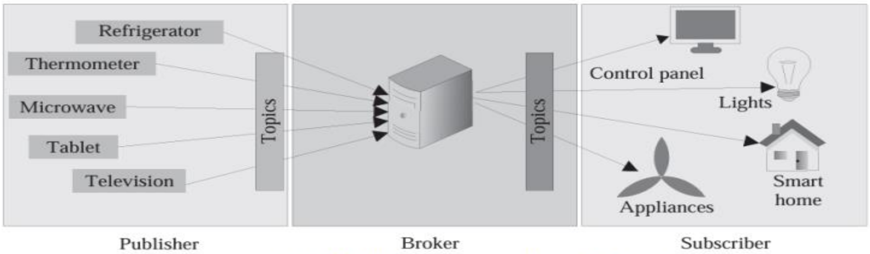
Figure 4.28 The Bluetooth protocol stack

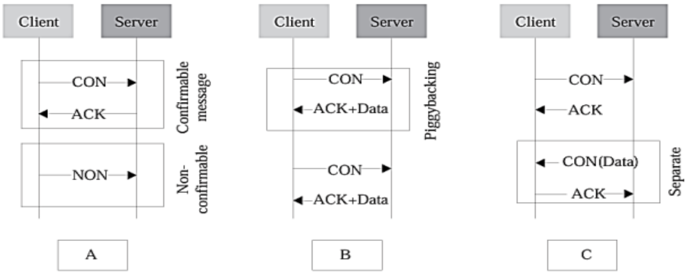
The Bluetooth protocol stack. Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), Host Controller Interface (HCI), Radio Frequency Communications (RFCOMM), and Service Discovery Protocol (SDP) are some of the wellknown protocols associated with Bluetooth. These protocols can be enumerated as follows:

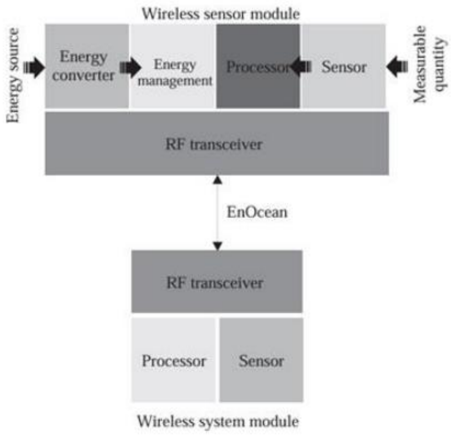
(i) Link Manager Protocol: It manages the establishment, authentication, and links configuration. LMPs consist of some protocol data units (PDU), between which transmission occurs for availing services such as name requests, link address requests, connection establishment, connection authentication, mode negotiation, and data transfer.

(ii) Host Controller Interface: It enables access to hardware status and control registers and connects the controller with the link manager. The automatic discovery of Bluetooth devices in its proximity is one of the essential tasks of HCI.

		(iii) L2CAP: It multiplexes logical connections between two devices. It is also tasked with data segmentation, flow control, and data integrity checks. (iv) Service Discovery Protocol: It is tasked with the discovery of services provided by other Bluetooth devices. (v) Radio Frequency Communications: It is a cable replacement protocol, which generates a virtual stream of serial data. This protocol supports many telephony related profiles as AT commands and Object Exchange Protocol (OBEX) over Bluetooth. (vi) Telephony Control Protocol– Binary (TCS BIN): It is a bit-oriented protocol to control call signaling prior to initiation of voice or data communications between devices.		
		Module-5		
Q.09	a	Explain the 6LoWPAN packet structure.  8-bits 8-bits 8-bits 8-bits Length Flags DSN Pan ID Destination ID (64-bits) Source ID (64-bits) IEEE 802.154 VER Traffic class Flow label Payload length Next header Hop limit Source address (128-bit) Destination address (128-bit) Ipv6 Figure 5.4 shows the 6LoWPAN packet structure. The 6LoWPAN stack rests on top of the IEEE 802.15.4 PHY and MAC layers, which are generally associated with low-rate wireless personal area networks (LR-WPAN). The network layer in 6LoWPAN enabled devices (layer 3) serves as an adaptation layer for extending IPv6 capabilities to IEEE 802.15.4 based devices. PHY and MAC layers: The PHY layer consists of 27 wireless channels, each having their separate frequency band and varying data rates. The MAC layer defines the means and methods of accessing the defined channels and use them for communication. The 6LoWPAN MAC layer is characterized by the following: (i) Ipv6 Beaconing tasks for device identification. These tasks include both beacon generation and beacon synchronization. (ii) Channel access control is provided by CSMA/CA. (iii) PAN membership control functions. Membership functions include association and dissociation tasks. Adaptation layer: As mentioned previously, 6LoWPAN accommodates and retro-fits the IPv6 packet to the IEEE 802.15.4 packet format. Address Format: The 6LoWPAN address format is made up of two parts: 1) the short (16-bit) address and 2) the extended (64-bit) address. The short address is PAN specific and is used for identifying devices within a PAN only, which makes its operational scope highly restricted and valid within a local network only.	L1	7

	b	Describe the LOADing routing.  Source 1 2 3 PREQ Destination PREQ_ACK Data (a) Flooding (b) Route discovery (c) Route establishment Figure 5.3The LOADng routing mechanism • When a data packet from a local data source is received for transmission to a destination whose routing entry is not present with it, a LOADng router sends an RREQ over all of its LOADng interfaces. The various forward interfaces are numbered to identify the destination from the source LOADng node. • The destination address obtained from the local source is encoded by the RREQ in the packet. • Upon receiving an RREQ, the routing set that manages the routing entries at each LOADng router updates or inserts an entry. This also makes it possible to keep track of the reverse journey between the source and the destination. • If the packets are intended for a local interface of a LOADng router, the received RREQ initiates a check of the destination address, and an RREP is sent back using the reverse route if the packets are intended for a local interface of a LOADng router. • If the target address is not local, it is sent in a hop-by-hop unicast manner to other LOADng interfaces through flooding. • When an RREP is received, the forward path toward the RREP's origin is noted in the routing entry, along with the LOADng router that transmitted the message. RREQ and RREP messages are also used to update the route metrics.	L1	6
	c	Explain the working of MQTT. • Message queue telemetry transport is a simple, lightweight publish subscribe protocol, designed mainly for messaging in constrained devices and networks. • It provides a one-to-many distribution of messages. • MQTT works reliably and flawlessly over high latency and limited bandwidth of unreliable networks without the need for significant device resources and device power.  Refrigerator Thermometer Microwave Tablet Television Topics Topics Control panel Lights Smart home Appliances Publisher Broker Subscriber Figure 5.14 MQTT operation and its stakeholders The MQTT paradigm consists of numerous clients connecting to a server; this server is referred to as a broker. The clients can have the roles of information publishers (sending messages to the broker) or information subscribers (retrieving	L1	7

		messages from the broker). MQTT is built upon the principles of hierarchical topics and works on TCP for communication over the network. Brokers receive new messages in the form of topics from publishers. A publisher first sends a control message along with the data message. Once updated in the broker, the broker distributes this topic’s content to all the subscribers of that topic for which the new message has arrived.		
OR				
Q.10	a	What is CoAP? Describe the working of CoAP. Constrained Application Protocol is a lightweight protocol designed for IoT, particularly for devices with limited resources such as low processing power, low memory, and low bandwidth. CoAP is used to enable communication between devices in constrained environments, typically in scenarios where traditional protocols like HTTP are too heavy.  Client Server CON ACK NON Confirmable message Non-confirmable Client Server CON ACK+Data CON ACK+Data Piggybacking Client Server CON ACK CON(Data) ACK Separate A B C Figure 8.18 Various CoAP response response models. (A): CON and NON messages, (B): Piggyback messages, and (C): Separate messages Key Features of CoAP: • Lightweight: CoAP is designed to work with resource-constrained devices and networks. It has a minimal header size and reduces the overhead typically seen in more general-purpose protocols like HTTP. • UDP-Based: Unlike HTTP, which runs over TCP, CoAP uses UDP. UDP is faster and more lightweight than TCP because it doesn't establish a connection before data transfer. However, it also does not guarantee reliability, but CoAP compensates for this by implementing its own mechanisms for message acknowledgment and retransmission. • Request-Response Model: CoAP uses a simple request-response model similar to HTTP. Devices can send requests (like GET, POST, PUT, DELETE) and receive responses from other devices or servers. • Asynchronous Communication: CoAP supports asynchronous communication, which means that devices can send requests and continue working while waiting for a response, making it efficient for real-time IoT applications. • Reliable Messaging: CoAP provides reliability using a mechanism called Confirmable (CON) and Non-Confirmable (NON) messages. Confirmable messages (CON): These messages require an acknowledgment. If the acknowledgment is not received, the message is retransmitted. •Non-Confirmable messages (NON): These messages do not require an acknowledgment and are used when reliability isn't critical (e.g., sensor data). • Low Overhead: CoAP uses a compact binary encoding for messages, which reduces the size of the data transmitted between devices, making it well-suited for low-bandwidth networks. • Multicast Support: CoAP supports multicast communication, which is useful for sending messages to multiple devices in a network simultaneously, which can reduce power consumption and improve efficiency. • Security: CoAP provides built-in support for security using DTLS (Datagram Transport Layer Security), which is a version of TLS (Transport Layer Security) for UDP. This allows for end-to-end encryption and authentication between devices.	L1	7
	b	What are the various types of interoperability encountered in IoT environment.	L1	6

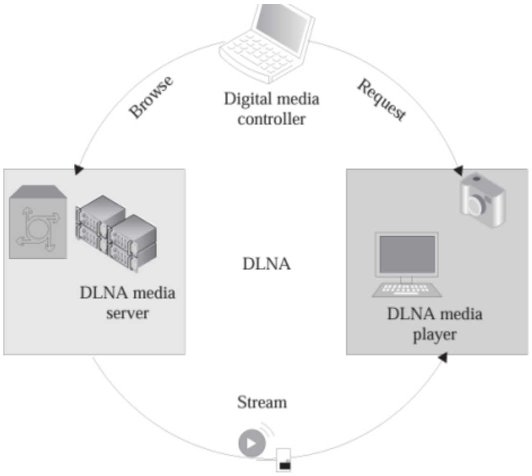
		(i) Device: The existence of a vast plethora of devices and device types in an IoT ecosystem necessitates device interoperability. Devices can be categorized as low-end, mid-end, and highend devices based on their processing power, energy, and communication requirements. Lowend devices are supposed to be deployed in bulk, with little or no chance of getting their energy supplies replenished, depending on the application scenario. These devices rely on low-power communication schemes and radios, typically accompanied by low-data rates. The interface of such devices with high-end devices (e.g., smartphones, tablets) requires device-level interoperability. (ii) Platform: The variations in the platform may be due to variations in operating systems (Contiki, RIOT, TinyOS, OpenWSN), data structures, programming languages (Python, Java, Android, C++), or/and application development environment. For example, the Android platform is quite different from the iOS one, and devices running these are not compatible with one another. (iii) Semantic: Semantic conflicts arise during IoT operations, mainly due to the presence of various data models (XML, CSV, JSON), information models (C, F, K, or different representations of the same physical quantity), and ontologies. There is a need for semantic interoperability, especially in a WoT environment, which can enable various agents, applications, and services to share data or knowledge in a meaningful manner. (iv) Syntactic: Syntactic interoperability is a necessity due to the presence of conflicts between data formats, interfaces, and schemas. The variation in the syntactical grammar between a sender and a receiver of information results in massive stability issues, redundancies, and unnecessary data handling efforts. (v) Network: The large range of connectivity solutions, both wired and wireless, at the disposal of developers and manufacturers of IoT devices and components, further necessitates network interoperability. Starting from the networks and sub-networks on the ground, to the uplink connectivity solutions, there is a need for uniformity or means of integrating to devices enable seamless and interoperable operations.		
	c	Describe the following standards: (i) EnOcean (ii) DLNA. (i) EnOcean:  Wireless sensor module Energy source Energy converter Energy management Processor Sensor Measurable quantity RF transceiver EnOcean RF transceiver Processor Sensor Wireless system module • EnOcean is a wireless technology designed for building automation systems, primarily based on the principle of energy harvesting. • Due to the robustness and popularity of EnOcean, it is being used in domains such as industries, transportation, logistics, and homes. • As of 2012, EnOcean was adopted as a wireless standard under ISO/IEC 14543-3-10, providing detailed coverage of the physical, data link, and networking layers. EnOceanbased devices are batteryless. • They use ultra-low power consuming electronics along with micro energy converters to enable wireless communication among themselves; the devices include networking components such as wireless sensors, switches, controllers,	L1	7

and gateways.

• The energy harvesting modules in EnOcean use micro-level variations and differences in electric, electromagnetic, solar, or other forms of energy to transform the energy into usable energy through highly efficient energy converters.

• The wireless signals from the battery less EnOcean sensors and switches, which are designed to be maintenance-free, can operate up to 30 meters in buildings and homes and up to 300 meters in the open.

(ii) DLNA:



• The Digital Living Network Alliance (DLNA), previously known as the Digital Home Working Group (DHWG), was proposed by a consortium of consumer electronics companies in 2003 to incorporate interoperability guidelines for digital media sharing among multimedia devices such as smartphones, smart TVs, tablets, multimedia servers, and storage servers.

• Primarily designed for home networking, this standard relies majorly on WLAN for communicating with other devices in its domain and can easily incorporate cable, satellite, and telecom service providers to ensure data transfer link protection at either end.

• The inclusion of a digital rights management layer allows for multimedia data sharing among users while avoiding piracy of data.

• The consumers in DLNA, which may consist of a variety of devices such as TVs, phones, tablets, media players, PCs, and others, can view subscribable content without any Request additional add-ons or devices through VidiPath.