USN										

CMR INSTITUTE OF TECHNOLOGY, BENGALURU. ACCREDITED WITH A+ GRADE BY NAAC

Model Question Paper Set 1

Sub:	Internet of Things					Sub Code:	22ETC15H	Branch:	
Date:		Duration:	180 min's	Max Marks:	100	Sem/Sec:	III / A, B, C, D, E, F and G		OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1	a) Name the four broad categories of computer network based on reachability and explain them briefly..	10	CO5	L2

Solution:

four broad categories of computer network based on reachability are **PAN, LAN, WAN and MAN**

Personal Area Networks (PAN): PANs, as the name suggests, are mostly restricted to individual usage.

- A good example of PANs may be connected wireless headphones, wireless speakers, laptops, smartphones, wireless keyboards, wireless mouse, and printers within a house.
- Generally, PANs are wireless networks, which make use of low-range and lowpower 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 linked to a single network through wired or wireless connections.

- However, LANs are restricted to buildings, organizations, or campuses. Typically, a few leased lines connected to the Internet provide web access to the whole organization or a campus;
- The lines are further redistributed to multiple hosts within the LAN enabling hosts. The hosts are much more in number than the actual direct lines to the Internet to access the web from within the organization. This also allows the organization to define various access control policies for web access within its hierarchy.
- Typically, the present-day data access rates within the LANs range from 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.

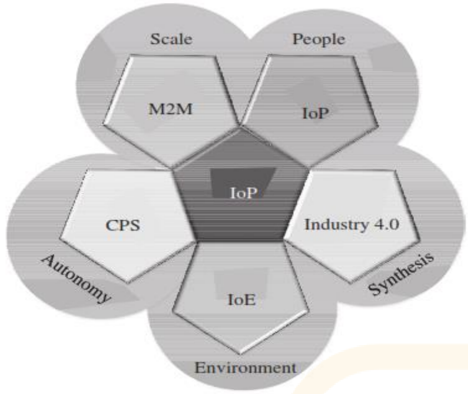
- MANs connect various organizations or buildings within a given geographic location or city.
- An excellent example of a MAN is an Internet service provider (ISP) supplying Internet connectivity to various organizations within a city.
- As MANs are costly, they may not be owned by individuals or even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

Wide Area Networks (WAN): WANs typically connect diverse geographic locations. However, they are restricted within the boundaries of a state or country.

- The data rate of WANs is in the order of a fraction of LAN's data rate.
- Typically, WANs connecting two LANs or MANs may use public switched telephone networks (PSTNs) or satellite-based links.
- Due to the long transmission ranges, WANs tend to have more errors and noise during transmission and are very costly to maintain. The fault tolerance of WANs are also generally low.

	b) Differentiate between IoT and M2M.	10	CO4	L2

Solution:



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 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.

c) With a neat diagram explain the network communication between two hosts following the OSI model.

Solution:

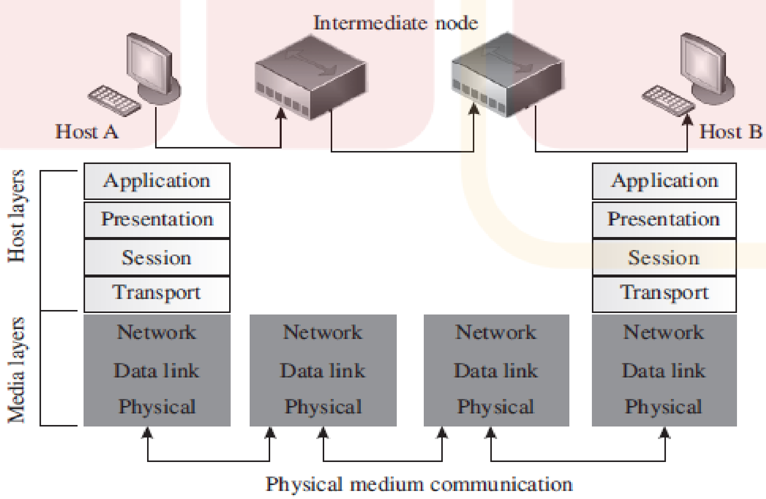


Figure 1.3 Networked communication between two hosts following the OSI model

1. In higher layers, each layer of the sender adds its information to the message received from above that layer and moves the entire package just below the layer as shown in the figure.
2. Each layer added its information in the form of headers. Headers are added at the level of the messages (6, 5, 4, 3, and 2). A header is added at the Data Link layer (layer 2).
3. At the physical layer, communication is direct i.e. the sender sends a stream of bits to the receiver. At the physical layer (layer 1) the entire package is

	converted into a form that can be transferred to the receiver. On the receiver side, each process is accompanied layer-by-layer to receive and delete message data. 4. Always the upper OSI layers are implemented in the software (Transport layer, Session layer, Presentation layer, Application layer (4, 5,) and the lower layers are a combination of hardware and software (layer 2, 3), except for the physical layer which is mostly hardware. Layer 1, 2, and 3 (ie physical layer, data link layer, and network layer) are network support layers. They deal with physical aspects of moving data such as electrical specifications, physical connections, physical address, and transport time and reliability from one device to another. Layer 4, Transport layer end to end ensures reliable data transmission.			
2	**a) What is IoT? Write the characteristics of IoT System.** **Solution:** "The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." 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. **b) With a neat diagram explain the inter dependency technology for IoT Planes.** **Solution:** The IoT paradigm is divided into four planes: • Services, • Local connectivity, • Global connectivity, and • Processing. The service plane is composed of two parts: 1) Things or devices and 2) low-power connectivity. • Typically, the services offered in this layer are a combination of things and low power connectivity. • For example, any IoT application requires the basic setup of sensing, followed by rudimentary processing (often), and a low-power, low-range network, which is mainly built upon the IEEE 802.15.4 protocol. • The things may be wearable's, computers, smart phones, household appliances, smart glasses. • 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. • The local connectivity is responsible for distributing Internet access to multiple local IoT deployments. • This distribution may be on the basis of the physical placement of the things, on the basis of the application domains, or even on the basis of providers of services. • Services such as address management, device management, security, sleep scheduling, and others fall within the scope of this plane. • 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.	6	CO5	L3

• 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 final plane of processing can be considered as a top-up of the basic IoT networking framework.

• The continuous rise in the usefulness and penetration of IoT in various application areas such as industries, transportation, healthcare, and others is the result of this plane.

• The members in this plane may be termed as IoT tools, simply because they wring-out useful and human-readable information from all the raw data that flows from various IoT devices and deployments.

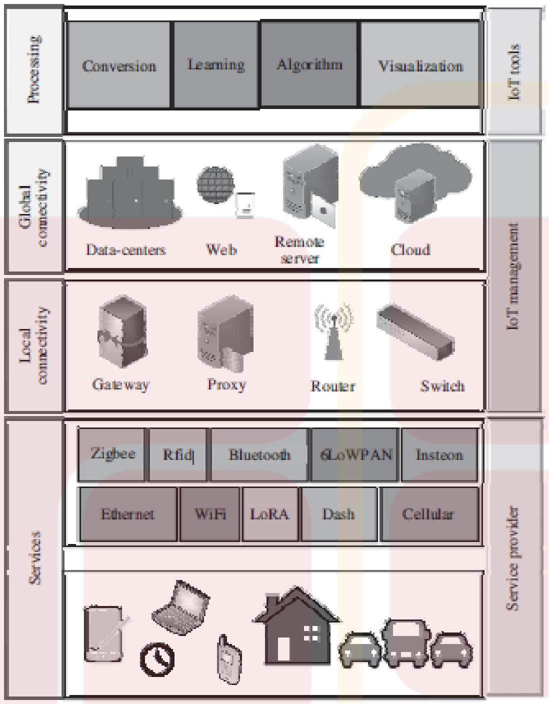
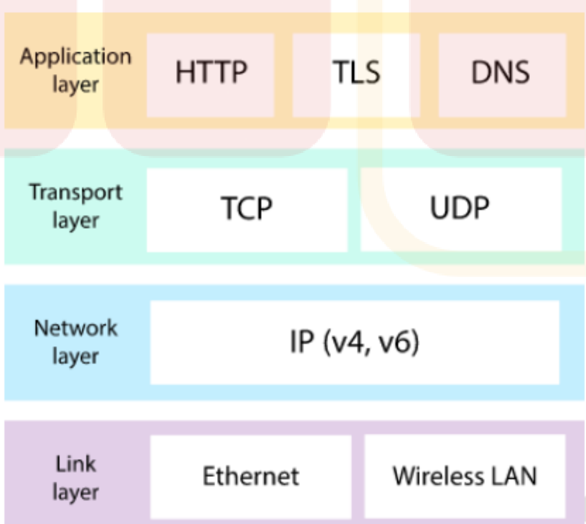


Figure 4.8 The IoT planes, various enablers of IoT, and the complex interdependencies among

c) With a neat diagram explain Internet protocol suite.



Link layer:

 The first and base layer of the TCP/IP protocol suite is also known as the network interface layer. This layer is synonymous with the collective physical and data link layer of the OSI model.

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

Internet Layer:

- Internet Layer: Layer 2 of the TCP/IP protocol suite is somewhat synonymous to the network layer of the OSI model.
- It is responsible for addressing, address translation, data packaging, data disassembly and assembly, routing, and packet delivery tracking operations.

Transport Layer:

- Transport Layer: Layer 3 of the TCP/IP protocol suite is functionally synonymous with the transport layer of the OSI model.
- This layer is tasked with the functions of error control, flow control, congestion control, segmentation, and addressing in an end-to-end manner; it is also independent of the underlying network.

Application Layer:

- Application Layer: The functionalities of the application layer, of the TCP/IP protocol suite are synonymous with the collective functionalities of the OSI model's session, presentation, and application layers.

3	**a) With a neat diagram explain the working mechanism of actuator.**	10	CO4	L2

Solution:

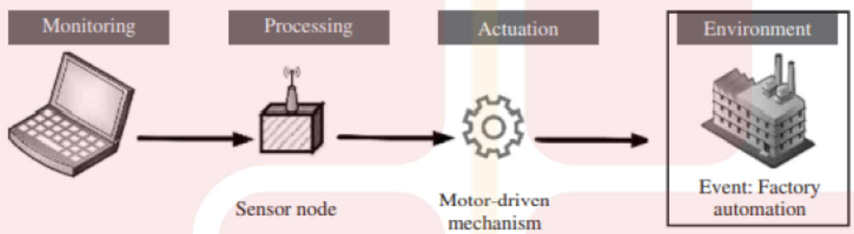


Figure 5: The outline of a simple actuation mechanism

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. Figure 5 shows the outline of a simple actuation system.
- 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.

b) Explain the types of actuators.

Solution:

Broadly, 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.

Hydraulic actuators:

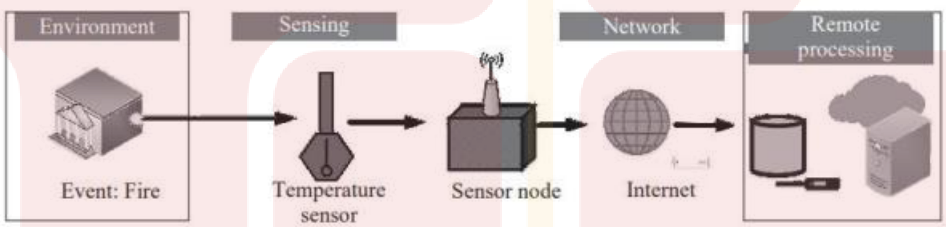
- A hydraulic actuator works on the principle of compression and decompression of fluids.

	• These actuators facilitate mechanical tasks such as lifting loads through the use of hydraulic power derived from fluids in cylinders or fluid motors. **Pneumatic actuators**: • A pneumatic actuator 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. **Electric actuators:** • 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 such as solenoid valves control the flow of water in pipes in response to electrical signals. **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. **Mechanical actuators**: • In mechanical actuation, 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. **Soft actuators:** • Soft actuators (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. **Shape memory polymers**: • Shape memory polymers (SMP) 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. **c) Define sensor and explain the characteristics of sensor.** **Solution:** 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. **Sensor Resolution:** • The smallest change in the measurable quantity that a sensor can detect is referred to as the resolution of a sensor. The more the resolution of a sensor, the more accurate is the precision. A sensor's accuracy does not depend upon its resolution. **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. We can say that this sensor is 99.98% accurate, with an error rate of ±0.02% **Sensor Precision:** • The principle of repeatability governs the precision of a sensor.			

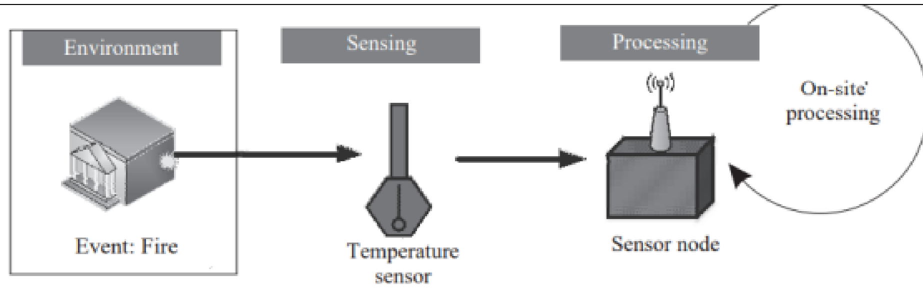
	For example, consider if the same weight sensor described earlier reports measurements of 98.28 kg, 100.34 kg, and 101.11 kg upon three repeat measurements for a mass of actual weight of 100 kg.			
4	a) List and explain the characteristics of Actuators. **Solution:** The characteristics of actuators are weight, power rating, torque to weight ratio and stiffness and compliance **Weight:** **1.** The physical weight of actuators limits its application scope. **2.** For example, the use of heavier actuators is generally preferred for industrial applications and applications requiring no mobility of the IoT deployment. **3.** In contrast, lightweight actuators typically find common usage in portable systems in vehicles, drones, and home IoT applications. **Power Rating**: **1.** The power rating defines the minimum and maximum operating power an actuator can safely withstand without damage to itself. **2.** Generally, it is indicated as the power-to-weight ratio for actuators. **3.** 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. **4.** Exceeding this limit might be detrimental to the performance of the actuator and may cause burnout of the motor. **Torque to Weight Ratio:** 1. The ratio of torque to the weight of the moving part of an instrument/device is referred to as its torque/weight ratio. 2. This indicates the sensitivity of the actuator. 3. Higher is the weight of the moving part; lower will be its torque to weight ratio for a given power **Stiffness and Compliance**: **1.** The resistance of a material against deformation is known as its stiffness, whereas compliance of a material is the opposite of stiffness. **2.** Stiffness can be directly related to the modulus of elasticity of that material. **3.** Stiff systems are considered more accurate than compliant systems as they have a faster response to the change in load applied to it. **4.** 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.** **Solution:** The following major factors influence the choice of sensors in IoT-based sensing solutions: 1) **Sensing range, 2) accuracy and precision, 3) energy, and 4) device size**. **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 k-coverage 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.	10	CO6	L2

	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 k-coverage 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. **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. **Device Size**: 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. **c) With a neat diagram explain scalar and Multimedia sensing techniques.** **Solution:** **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. The sensors used for measuring the scalar quantities like temperature, current, atmospheric pressure, rainfall, light, humidity, flux are referred to as scalar sensors, and the act is known as scalar sensing. **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 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.			
5a	a) List and explain common data types in IoT applications **Solution:** The huge data volume generated in Internet is composed of a variety of data such as e-mails, text documents (Word docs, PDFs, and others), social media posts, videos, audio files, and images, as shown in Figure 3.1. However, these data can be broadly grouped into two types based on how they	5	CO5	L2

	can be accessed and stored: 1) Structured data and 2) unstructured data. **Structured data:** These are typically text data that have a pre-defined structure. Structured data are associated with relational database management systems (RDBMS). These are primarily created by using length-limited data fields such as phone numbers, social security numbers, and other such information. Even if the data is human or machinegenerated, these data are easily searchable by querying algorithms as well as humangenerated 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 foraccessing these data in RDBMS. **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, e-mails, 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. 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.			
5b	With a neat diagram explain offsite processing topology. Off-site processing • 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 large-scale deployments typical of IoT deployments.	L1	CO3	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 large-scale 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).  Figure 3.3 Event detection using an off-site remote processing topology			
5C	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. 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	L1	CO3	5

	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 real-time 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			
6A	With a neat diagram explain onsite processing topology. On-site processing As evident from the name, 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. Figure 3.2 shows the on-site processing topology, where an event (here, fire) is detected utilizing a temperature sensor connected to a sensor node. The sensor node processes the information from the sensed event and generates an alert. The node additionally has the option of forwarding the data to a remote infrastructure for further analysis and storage.	L1	CO3	5

	 Figure 3.2: Event detection using an on-site processing topology			
6B	Explain IoT Device Design and Selection Considerations The Main focus is on the deciding factors for selecting a processor for the design of a sensor node. The main factor governing the IoT device design and selection for various applications is the processor. However, 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. 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. However, devices with higher memory tend to be costlier for obvious reasons. Processing power: As covered in earlier sections, processing power is vital	L2	CO3	8

	(comparable to memory) 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. Typically, 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. Additionally, the provision for these add-ons also decides how fast a solution can be developed, especially the hardware part of the whole IoT application. As interfacing and integration of systems at the circuit level can be daunting to the uninitiated, the prior presence of these options with the processor makes the processor or device highly lucrative to the users/ developers.			
6C	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. We distinguish the offload location into four types: Edge: Offloading processing to the edge implies that the data processing is facilitated to a	L1	CO3	7

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 resourceconstrained 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. A cloud is provisioned for processing offloading so that processing resources can be rapidly provisioned with minimal effort over the Internet, which can be accessed globally. 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.

- 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. This measure is undertaken so that the achieved QoS is collaboratively better for the full implementation rather than a select few devices enjoying very high QoS. Game theory is a common example of the bargaining based approach. This approach does not need to depend on historical data for decision making purposes. Learning based approach: Unlike the bargaining based approaches, the learning based 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.			
7A	Define Virtualization. Discuss advantages of virtualization	L1	CO4	8

- The technique of sharing a single resource among multiple end users is known as *"Virtualization"*. It is the key concept of cloud computing.
- In the virtualization process, a physical resource is logically distributed among multiple users. However, a user realizes that the resource is unlimited and is dedicatedly provided to him/her.

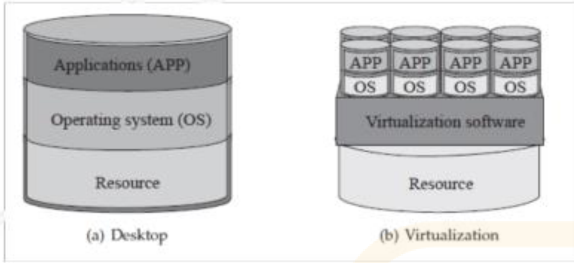


Figure 2.1 Traditional desktop versus virtualization

- Figure 2.2(a) represents a traditional desktop, where an application (App) is running on top of an OS, and resources are utilized only for that particular application.
- Figure 2.2(b) virtualization software separates the resources logically so that there is no conflict among the users during resource utilization.
- Typically, there are different software such as VMware, hypervisor, and virtual machines which enable the concept of virtualization.

2.1 Advantages of virtualization: There are TWO main entities in a cloud computing architecture: *(1) End users and (2) Cloud Service providers (CSPs).* Both are benefited in several aspects through the process of virtualization. The

(1). Advantages of virtualization for End Users: They are as follows

(a) Variety *(b) Availability*
(c) Portability *(d) Elasticity*

(a) Variety:

- It enables various types of applications based on the requirements.
- It enables end users to access applications, hardware, or software virtually from a variety of devices and networks, regardless of their operating system (OS).

<table>
<tr><td></td><td>a variety of devices and networks, regardless of their operating system (OS).

(b) Availability:
– Virtualization creates a logical separation of the resources of multiple entities without any intervention from end users.
– It makes available a considerable amount of resources as per user requirements.
– The end users feel that there are unlimited resources present dedicatedly for him/her.

(c) Portability:
– Ability to transfer applications and data between cloud computing environments.
– It enables migration between public and private clouds.
– Portability signifies the availability of cloud computing services from anywhere in the world, at any instant in time.
– It allows individuals to obtain and reuse their data for their purposes across different services.
– It allows them to move, copy or transfer personal data easily from one environment to another in a safe and secure without affecting its usability.
– This has been made possible by such as Google Drive.</td><td></td><td></td><td></td></tr>
<tr><td>7B</td><td>Summarize the case study related to Smart irrigation management system

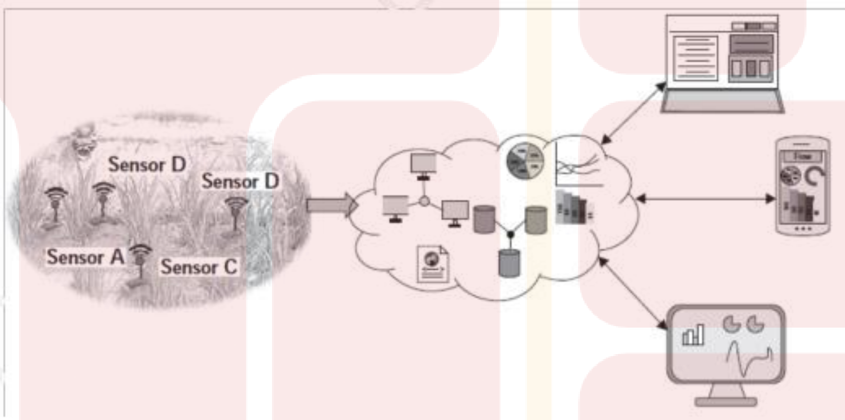


Figure 1.1 Architecture of agricultural IoT

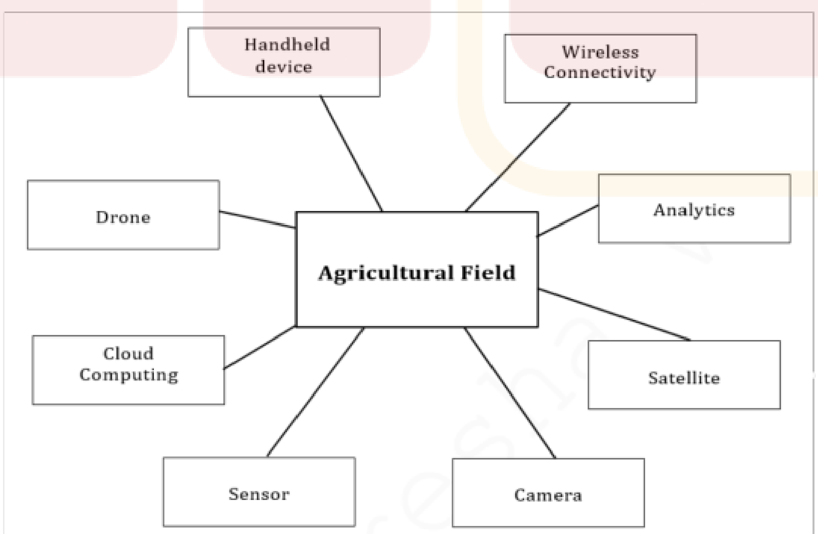
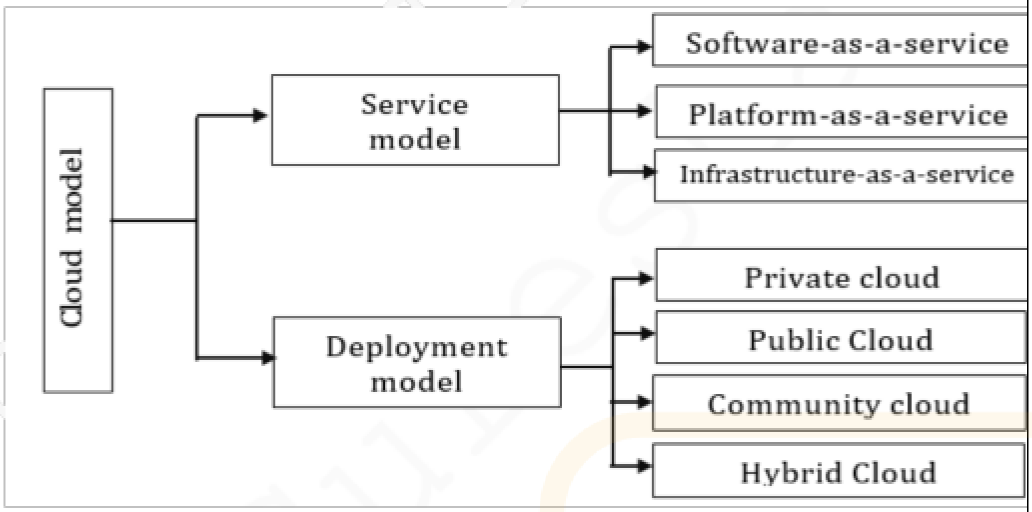
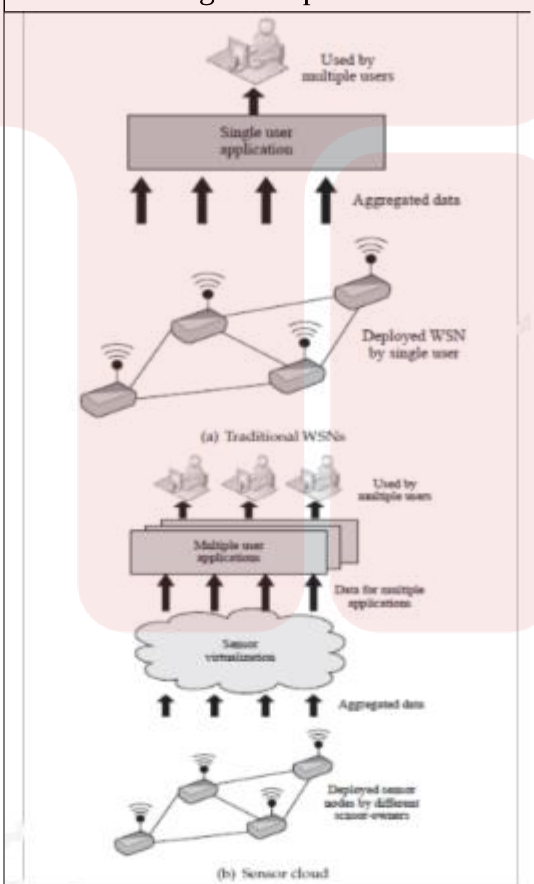


Figure 1.2 Components of agricultural IoT</td><td>L2</td><td>CO4</td><td>5</td></tr>
<tr><td>7C</td><td>With the help of neat diagrams explain the of cloud models.</td><td>L1</td><td>CO4</td><td>7</td></tr>
</table>

	 ***Figure 3.1 Cloud model***			
8a	With a neat diagram explain Architecture of a sensor-cloud platform 	L1	CO4	8

6.2 Architecture of a sensor-cloud platform: The THREE main components of a sensor-cloud architecture are (i) End-user (ii) Sensor Owner (iii) Sensor-Cloud Service Provider (SCSP). The detailed architecture of a sensor cloud is depicted in Figure 6.2

(i) End User:

- The end user is also known as a customer of the sensor-cloud services.
- An end user registers him/herself with the infrastructure through a Web portal.
- He/she chooses the template of the services that are available in the sensor-cloud architecture to which he/she is registered.
- Through the Web portal, the end user receives the services, as shown in Fig 6.2 Based on the type and usage duration of service, the end user pays the charges to the SCSP.

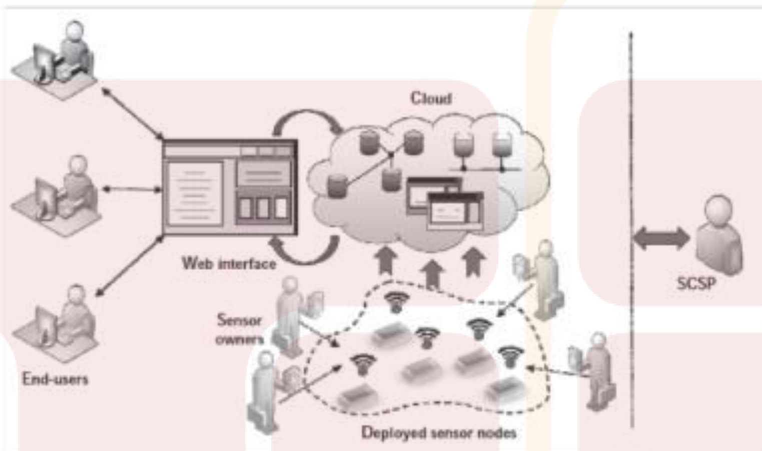


Figure 6.2 Architecture of a sensor-cloud platform

(ii) Sensor Owner:

- A particular sensor owner can own multiple homogeneous or heterogeneou sensor nodes.
- Based on the requirements of the users, these sensor nodes are virtualized an assigned to serve multiple applications at the same time.
- The sensor owner receives rent depending upon the duration and usage o his/her sensor node(s).

(iii) Sensor-Cloud Service Provider (SCSP):

- An SCSP is responsible for managing the entire sensor-cloud infrastructure.
- The SCSP receives rent from end users with the help of a pre-defined pricin model.
- The pricing scheme may include the infrastructure cost, sensor owners' ren and the revenue of the SCSP.
- The SCSP receives the rent from the end users and shares a partial amount wit the sensor owners. The remaining amount is used for maintaining th infrastructure.

8B	With a neat diagram explain Components of an agricultural IoT	L1	CO4	5

1.1 Components of an agricultural IoT*** Main components of agricultural IoT are

- *Cloud computing, Sensors, Cameras*
- *Satellites, Analytics, Wireless connectivity*
- *Handheld devices, Drones.*

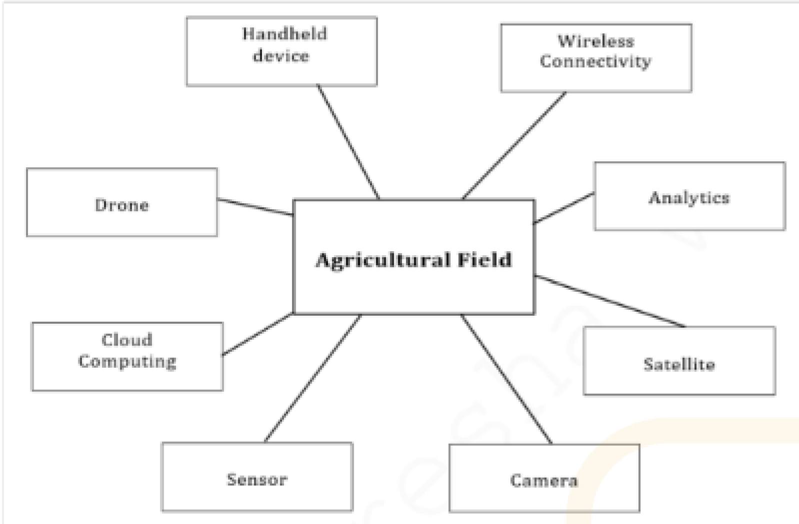


Figure 1.2 Components of agricultural IoT

Figure 1.2 Components of agricultural IoT

- The description of components is as follows

(i) Cloud computing:

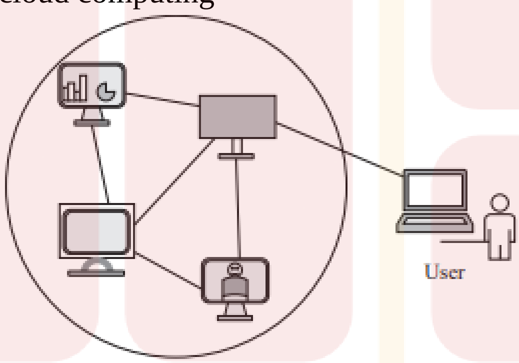
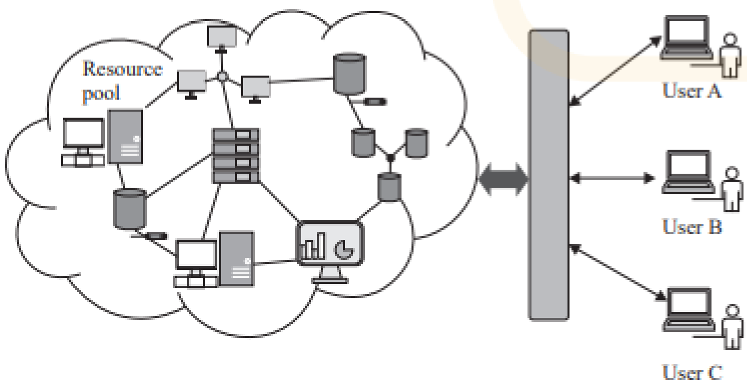
- It processes and analyzes huge amounts of agricultural data like soil moisture, humidity, soil pH level, and plant images produced by sensors. Based on the data analysis, action needs to be taken, such as switching on the water pump for irrigation.
- It stores analyzed data on a long-term basis since it may be useful for serving future applications.

(ii) Sensors:

- Sensors are the major backbone of any IoT application and these sensors are indispensable components.
- A few of the common sensors used in agriculture are sensors for soil moisture, humidity, water level, and temperature.

(iii) Cameras:

- Imaging is one of the main components of agriculture used for crop security
- Multispectral, thermal, and RGB cameras are commonly used for scientific agricultural IoT.
- These cameras are used for estimating the nitrogen status, thermal stress, water stress, and crop damage due to infestation.
- Video cameras are used for crop security.

	(iv) Satellites: – Satellite images are used in agricultural applications to monitor different aspects of the crops such as crop health monitoring and dry zone assessment over a large area. ***(v) Analytics:*** – Analytics is the systematic computational analysis of data or statistics. – It is used for the discovery, interpretation, effective decision-making, and communication of meaningful patterns in data. – Analytics contribute to modern agriculture massively. Currently, with the help of analytics, farmers can take different agricultural decisions, such as estimating the required amount of fertilizer and water in an agricultural field. – Estimating the type of crops that need to be cultivated during the upcoming season. – Data analytics can also be used for estimating crop demand in the market. ***(vi) Wireless connectivity:*** – Wireless connectivity enables the transmission of agricultural sensor data from the field to the cloud/server. – It also enables farmers to access various application services over handheld devices, which rely on wireless connectivity for communicating with the cloud/server.			
8C	With the help of neat diagrams describe the difference between Network computing and cloud computing  (a) Network computing  (b) Cloud computing Figure 1: Network Computing versus Cloud computing Cloud computing is more than traditional network computing. Unlike network computing, cloud computing comprises a pool of multiple resources such as servers, storage, and network from single/multiple organizations. These resources are allocated to the end users as per requirement, on a payment basis.	L1	CO4	7

In cloud computing architecture, an end user can request for customized resources such as storage space, RAM, operating systems, and other software to a cloud service provider (CSP) as shown in Figure 1. For example, a user can request for a Linux operating system for running an application from a CSP; another end user can request for Windows 10 operating system from the same CSP for executing some application. The cloud services are accessible from anywhere and at any time by an authorized user through Internet connectivity.

Module-5

9a	With a neat diagram explain the Architecture of vehicular IoT.	L1	CO5	7

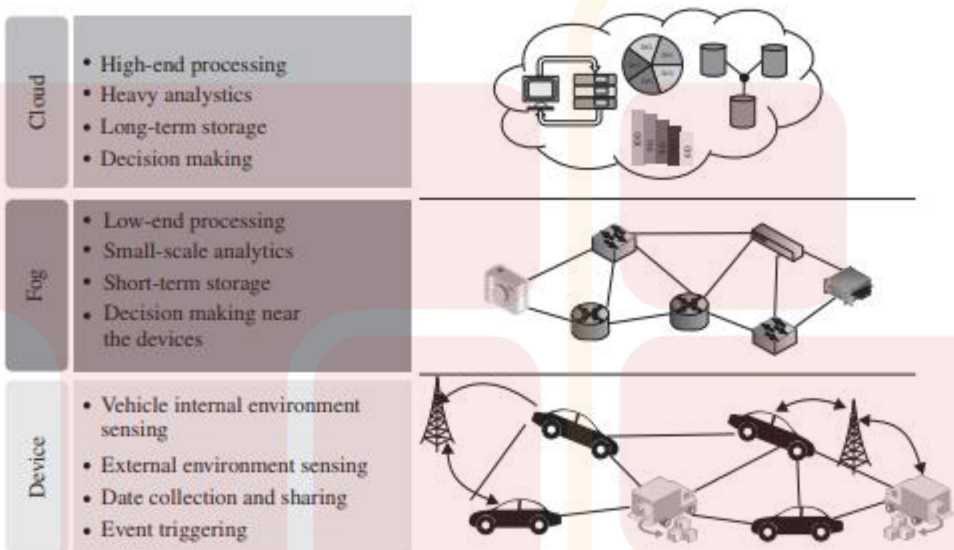
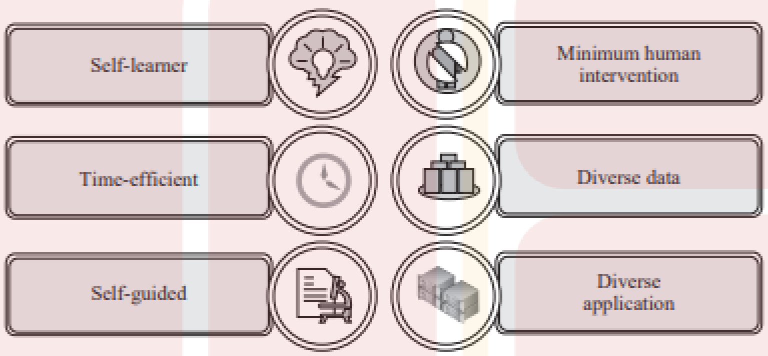


Figure 1: Architecture of vehicular IoT

Vehicular IoT systems have penetrated different aspects of the transportation ecosystem, including on-road to off-road traffic management, driver safety for heavy to small vehicles, and security in public transportation. In a connected vehicular environment, vehicles are capable of communicating and sharing their information. Moreover, IoT enables a vehicle to sense its internal and external environments to make certain autonomous decisions. With the help of modern-day IoT infrastructure, a vehicle owner residing in Earth's northern hemisphere can very easily track his vehicular asset remotely, even if it is in the southern hemisphere. Figure 1 represents a simple architecture of a vehicular IoT system. The architecture of the vehicular IoT is divided into three sub layers: device, fog, and cloud.

•Device: The device layer is the bottom-most layer, which consists of the basic infrastructure of the scenario of the connected vehicle. This layer includes the vehicles and road side units (RSU). These vehicles contain certain sensors which gather the internal information of the vehicles. On the other hand, the RSU works as a local centralized unit that manages the data from the vehicles. • Fog: In vehicular IoT systems, fast decision making is pertinent to avoid accidents and traffic mismanagement. In such situations, fog computing plays a crucial role by providing decisions in real-time, much near to the devices. Consequently, the fog layer helps to minimize data transmission time in a vehicular IoT system.

	• Cloud: Fog computing handles the data processing near the devices to take decisions instantaneously. However, for the processing of huge data, fog computing is not enough. Therefore, in such a situation, cloud computing is used. In a vehicular IoT system, cloud computing helps to handle processes that involve a huge amount of data. Further, for long-term storage, cloud computing is used as a scalable resource in vehicular IoT systems.			
9b	Define Machine learning and explain the advantages of ML. The term “machine learning” was coined by Arthur Lee Samuel, in 1959. He defined machine learning as a “field of study that gives computers the ability to learn without being explicitly programmed”. ML is a powerful tool that allows a computer to learn from past experiences and its mistakes and improve itself without user intervention. Typically, researchers envision IoT-based systems to be autonomous and self-adaptive, which enhances services and user experience. To this end, different ML models play a crucial role in designing intelligent systems in IoT by leveraging the massive amount of generated data and increasing the accuracy in their operations. The main components of ML are statistics, mathematics, and computer science for drawing inferences, constructing ML models, and implementation, respectively. Advantages of ML:  Figure 1: Advantages of ML Applications fueled by ML open a plethora of opportunities in IoT-based systems, from triggering actuators to identifying chronic diseases from images of an eye. ML also enables a system to identify changes and to take intelligent actions that relatively imitates that of a human. As ML demonstrates a myriad of advantages, its popularity in IoT applications is increasing rapidly. i) Self-learner: An ML-empowered system is capable of learning from its prior and run-time experiences, which helps in improving its performance continuously. For example, an ML-assisted weather monitoring system predicts the weather report of the next seven days with high accuracy from data collected in the last six months. The system offers even better accuracy when it analyzes weather data that extends back to three more months. ii) (ii) Time-efficient: ML tools are capable of producing faster results as compared to human interpretation. For example, the weather monitoring system generates a weather prediction report for the upcoming seven days, using data that goes back to 6–9 months. A manual analysis of such sizeable data for predicting the weather is	L1	CO5	6

	difficult and time-consuming. Moreover, the manual process of data analysis also affects accuracy. In such a situation, ML is beneficial in predicting the weather with less delay and accuracy as compared to humans. (iii) Self-guided: An ML tool uses a huge amount of data for producing its results. These tools have the capability of analyzing the huge amount of data for identifying trends autonomously. As an example, when we search for a particular item on an online e-commerce website, an ML tool analyzes our search trends. As a result, it shows a range of products similar to the original item that we searched for initially. (iv) Minimum Human Interaction Required: In an ML algorithm, the human does not need to participate in every step of its execution. The ML algorithm trains itself automatically, based on available data inputs. For instance, let us consider a healthcare system that predicts diseases. In traditional systems, humans need to determine the disease by analyzing different symptoms using standard "if– else" observations. However, the ML algorithm determines the same disease, based on the health data available in the system and matching the same with the symptoms of the patient. (v) Diverse Data Handling: Typically, IoT systems consist of different sensors and produce diverse and multi-dimensional data, which are easily analyzed by ML algorithms. For example, consider the profit of an industry in a financial year. Profits in such industries depend on the attendance of laborers, consumption of raw materials, and performance of heavy machineries. The attendance of laborers is associated with an RFID (radio frequency identification)-based system. On the other hand, industrial sensors help in the detection of machinery failures, and a scanner helps in tracking the consumption of raw materials. ML algorithms use these diverse and multi-dimensional data to determine the profit of the industry in the financial year. (vi) Diverse Applications: ML is flexible and can be applied to different application domains such as healthcare, industry, smart traffic, smart home, and many others. Two similar ML algorithms may serve two different applications.				
9c	With a neat diagram explain Architecture of healthcare IoT. Internet of Things (IoT) has resulted in the development and emergence of a variety of technologies that has had a huge impact on the medical field, especially wearable healthcare. The salient features of IoT encourage researchers and industries to develop new IoT-based technologies for healthcare. These technologies have given rise to small, power-efficient, health monitoring and diagnostic systems. Consequently, the development of numerous healthcare technologies and systems has rapidly increased over the last few years. Currently, various IoT-enabled healthcare devices are in wide use around the globe for diagnosing human diseases, monitoring human health conditions,	L1	CO5	7

caring/monitoring for elders, children, and even infants. Moreover, IoT-based healthcare systems and services help to increase the quality of life for common human beings; in fact, it has a promising scope of revolutionizing healthcare in developing nations. IoT-based healthcare devices provide access and knowledge about human physiological conditions through hand held devices. With this development, users can be aware of the Internet of Things (IoT) has resulted in the development and emergence of a variety of technologies that has had a huge impact on the medical field, especially wearable healthcare. The salient features of IoT encourage researchers and industries to develop new IoT-based technologies for healthcare. These technologies have given rise to small, power-efficient, health monitoring and diagnostic systems. Consequently, the development of numerous healthcare technologies and systems has rapidly increased over the last few years. Currently, various IoT-enabled healthcare devices are in wide use around the globe for diagnosing human diseases, monitoring human health conditions, caring/monitoring for elders, children, and even infants. Moreover, IoT-based healthcare systems and services help to increase the quality of life for common human beings; in fact, it has a promising scope of revolutionizing healthcare in developing nations. IoT-based healthcare devices provide access and knowledge about human physiological conditions risks in acquiring various diseases and take necessary precautions to avoid preventable diseases. The basic skeleton of an IoT-based healthcare system is very similar to the conventional IoT architectures. However, for IoT-based healthcare services, the sensors are specifically designed to measure and quantify different physiological conditions of its users/patients. A typical architecture for healthcare IoT is shown in Figure 1. We divide the architecture into four layers. The detailed description of these layers are as follows:

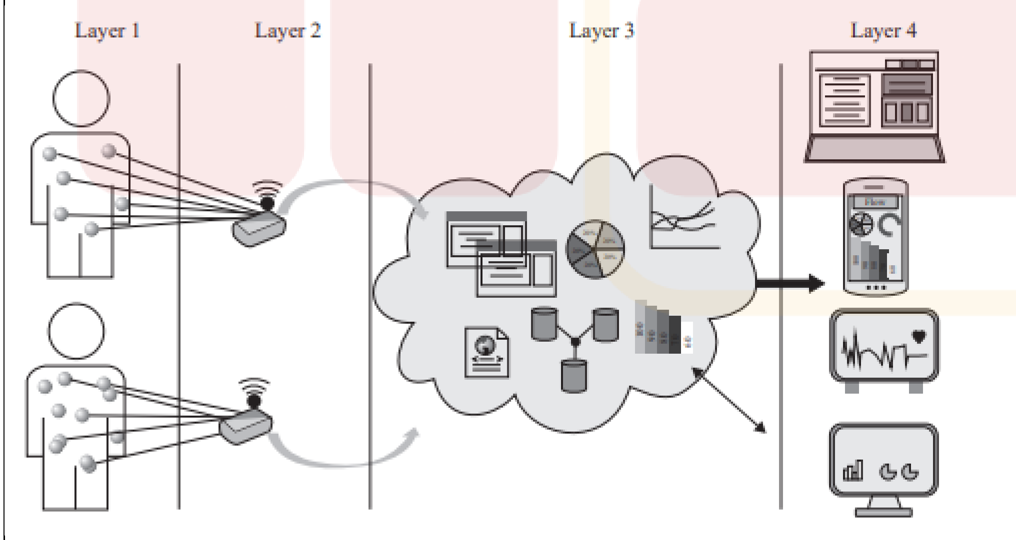
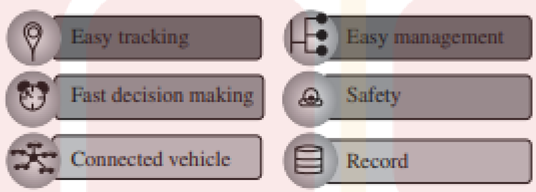
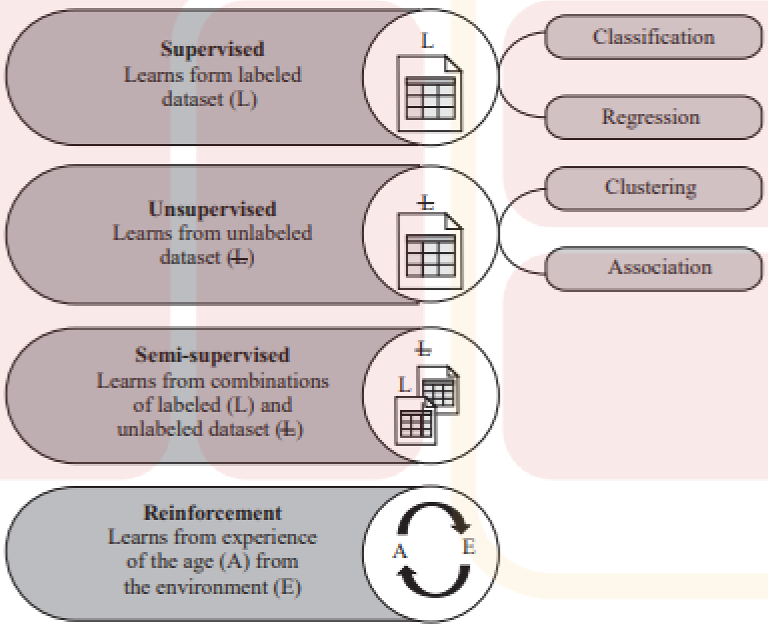


Figure 1 Architecture for healthcare IoT

Layer 1: We have already explained in previous chapters that sensors are one of the key enablers of IoT infrastructure. Layer 1 contains different physiological sensors that are placed on the human body. These sensors collect the values of various physiological parameters. The physiological data are analyzed to extract meaningful information.

(ii) Layer 2: Layer 1 delivers data to Layer 2 for short-term storage and low-level processing. The devices that belong to Layer 2 are commonly known as local

	processing units (LPU) or centralized hubs. These units collect the sensed data from the physiological sensors attached to the body and process it based on the architecture's requirement. Further, LPUs or the centralized hubs forward the data to Layer 3. (iii) Layer 3: This layer receives the data from Layer 2 and performs application specific high-level analytics. Typically, this layer consists of cloud architecture or high-end servers. The data from multiple patients, which may be from the same or different locations, are accumulated in this layer. Post analysis of data, some inferences or results are provided to the application in Layer 4 (iv) Layer 4: The end-users directly interact with Layer 4 through receiver-side applications. The modes of accessibility of these services by an end user are typically through cellphones, computers, and tablets			
	OR			
10a	List the advantages of vehicular IoT The evolution of IoT resulted in the development of a connected vehicular environment. Moreover, the typical advantages of IoT architectures directly impact the domain of connected vehicular systems. Therefore, the advantages of IoT are inherently included in vehicular IoT environments. A few selected advantages of vehicular IoT are depicted in Figure 1.  Figure 1: Advantages of vehicular IoT (i) Easy tracking: The tracking of vehicles is an essential part of vehicular IoT. Moreover, the system must know from which location and which vehicle the system is receiving the information. In a vehicular IoT system, the tracking of vehicles is straightforward; the system can collect information at a remote location. (ii) Fast decision making: Most of the decisions in the connected vehicle environment are time critical. Therefore, for such an application, fast and active decision making are pertinent for avoiding accidents. In the vehicular IoT environment, cloud and fog computing help to make fast decisions with the data received from the sensor-based devices. (iii) Connected vehicles: A vehicular IoT system provides an opportunity to remain connected and share information among different vehicles. (iv) Easy management: Since vehicular IoT systems consist of different types of sensors, a communication unit, processing devices, and GPS, the management of the vehicle becomes easy. The connectivity among different components in a vehicular IoT enables systems to track every activity in and around the vehicle. Further, the IoT infrastructure helps in managing the huge number of users located at different geographical coordinates. (v) Safety: Safety is one of the most important advantages of a vehicular IoT system. With easy management of the system, both the internal	L1	CO5	7

	and external sensors placed at different locations play an important role in providing safety to the vehicle, its occupants, as well as the people around it. (vi) Record: Storing different data related to the transportation system is an essential component of a vehicular IoT. The record may be of any form, such as video footage, still images, and documentation. By taking advantage of cloud and fog computing architecture, the vehicular IoT systems keep all the required records in its database			
10b	With a neat diagram explain the types of Machine learning. Typically, ML algorithms consist of four categories: (i) Supervised (ii) Unsupervised (iii) Semi-supervised (iv) Reinforcement Learning (Figure 1). In this section, we briefly explore different categories of ML. Before discussing further, we determine the meaning of labeled- and unlabeled-data. As the name suggests, labeled data contain certain meaningful tags, known as labels. Typically, the labels correspond to the characteristics or properties of the objects. For example, in a dataset containing the images of two birds, a particular sample is tagged as a crow or a pigeon. On the other hand, the unlabeled dataset does not have any tags associated with them. For example, a dataset containing the images of a bird without mentioning its name.  Figure 1: Types of Machine learning (i) Supervised Learning: This type of learning supervises or directs a machine to learn certain activities using labeled datasets. The labeled data are used as a supervisor to make the machine understand the relation of the labels with the properties of the corresponding input data. Consider an example of a student who tries to learn to solve equations using a set of labeled formulas. The labels indicate the formulae necessary for solving an equation. The student learns to solve the equation using suitable formulae from the set. In the case of a new equation, the student tries to identify the set of formulae necessary for solving it. Similarly, ML algorithms train themselves for selecting efficient formulae for solving equations. The selection	L1	CO5	6

of these formulae depends primarily on the nature of the equations to be solved. Supervised ML algorithms are popular in solving classification and regression problems. Typically, the classification deals with predictive models that are capable of approximating a mapping function from input data to categorical output. On the other hand, regression provides the mapping function from input data to numerical output. There are different classification algorithms in ML. However, in this chapter, we discuss three popular classification algorithms: (i) k-nearest neighbor (KNN), (ii) decision tree (DT), and (iii) random forest (RF). We use regression to estimate the relationship among a set of dependent variables with independent variables, as shown in Figure 17.3. The dependent variables are the primary factors that we want to predict. However, these dependent variables are affected by the independent variables. Let x and y be the independent and dependent variables, respectively. Mathematically, a simple regression model is represented as

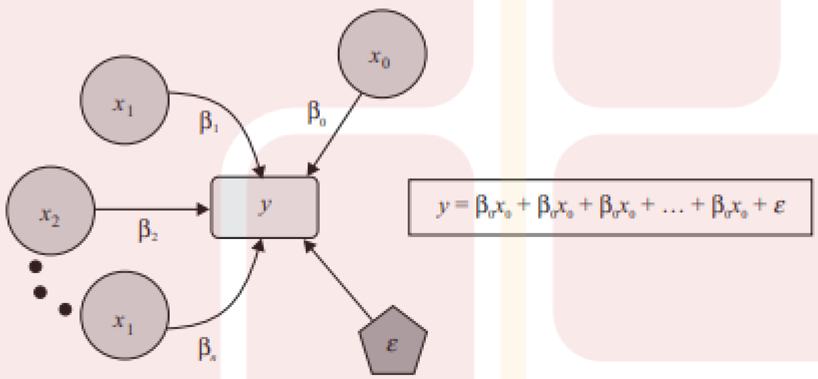


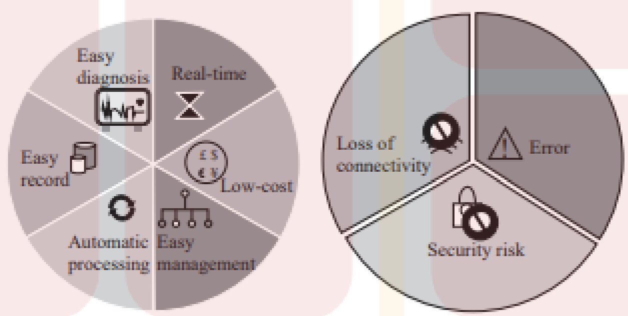
Figure 17.3 Regression model

y = β0 x0 + βx + ε (17.1)

where β represents the amount of impact of variable x on y and ε denotes an error. In the given equation, x0 creates β0 impact on y, which indicates that the value of y can never be 0. Similarly, for multiple variables, say n, the regression model is represented as: y = Xn i=0 βixi + ε (17.2)

(ii) Unsupervised Learning: Unsupervised learning algorithms use unlabeled datasets to find scientific trends. Let us consider an example of the student similar to that described in the case of supervised learning, and illustrate how it differs in case of unsupervised learning. As already mentioned, unsupervised learning does not use any labels in its operations. Instead, the ML algorithms in this category try to identify the nature and properties of the input equation and the nature of the formulae responsible for solving it. Unsupervised learning algorithms try to create different clusters based on the features of the formulae and relate it with the input equations. Unsupervised learning is usually applied to solve two types of problems: clustering and association. Clustering divides the data into multiple groups. In contrast, association discovers the relationship or association among the data in a dataset.

(iii) Semi-Supervised Learning: Semi-supervised learning belongs to a category between supervised and unsupervised learning. Algorithms under this category use a combination of both labeled and unlabeled datasets for training. Labeled

	data are typically expensive and are relatively difficult to label correctly. Unlabeled data is less expensive than labeled data. Therefore, semi-supervised learning includes both labeled and unlabeled dataset to design the learning model. Traditionally, semi-supervised learning uses mostly unlabeled data, which makes it efficient to use, and capable of overcoming samples with missing labels. (iv) Reinforcement Learning: Reinforcement learning establishes a pattern with the help of its experiences by interacting with the environment. Consequently, the agent performs a crucial role in reinforcement learning models. It aims to achieve a particular goal in an uncertain environment. Typically, the model starts with an initial state of a problem, for which different solutions are available. Based on the output, the model receives either a reward or a penalty from the environment. The output and reward act as inputs for proceeding to the next state. Thus, reinforcement learning models continue learning iteratively from their experiences while inducing correctness to the output.			
10c	Write note on advantages and risk of healthcare IoT. IoT has already started to penetrate the domain of medical science. In healthcare, IoT has become significantly popular due to its various features, which have been covered previously in this book. Healthcare IoT helps in managing different healthcare subsystems efficiently. Although it has many advantages, healthcare IoT has some risks too, which may be crucial in real-life applications. In this section, we discuss the different advantages and risks of healthcare IoT as depicted in Figure 14.3  (a) Advantages of healthcare IoT (b) Risk in healthcare IoT Figure 14.3 Advantages and risk in healthcare IoT **Advantages of healthcare IoT** The major advantages of healthcare IoT can be listed as follows: • Real-time: In healthcare sectors, different components, such as the condition of the patients, availability of doctors and beds in a hospital, medical facilities with their monetary charges, can vary dynamically with time. In such a dynamic scenario, one of the important characteristics of an IoT-based healthcare system is real-timeliness. A healthcare IoT system enables users, such as doctors, end users at the patient-side, and staff in a healthcare unit, to receive real-time updates about the healthcare IoT components, as mentioned earlier. Moreover, a healthcare IoT system can enable a doctor to observe a patient's health condition in real-time even from a remote location, and can suggest the type of care to be provided to the patient. On the other hand, users at the patient-end can easily take different decisions, such as where to take a patient during critical situations. Moreover, the staff in a healthcare unit are better aware of the current situation	L1	CO5	7

of their unit, which includes the number of patients admitted, availability of the doctors and bed, total revenue of the unit, and other such information.

• Low cost: Healthcare IoT systems facilitate users with different services at low cost. For example, an authorized user can easily find the availability of the beds in a hospital with simple Internet connectivity and a web-browser-based portal. The user need not visit the hospital physically to check the availability of beds and facilities. Moreover, multiple registered users can retrieve the same information simultaneously.

• Easy management: Healthcare IoT is an infrastructure that brings all its end users under the same umbrella to provide healthcare services. On the other hand, in such an infrastructure, the management of numerous tangible and intangible entities (such as users, medical devices, facilities, costs, and security) is a challenging task. However, healthcare IoT facilitates easy and robust management of all the entities.

• Automatic processing: A healthcare unit consists of multiple subsystems, for which manual interventions are required. For example, to register a patient with a hospital, the user may be required to enter his/her details manually. However, automatic processing features can remove such manual intervention with a fingerprint sensor/device. Healthcare IoT enables end-to-end automatic processing in different units and also consolidates the information across the whole chain: from a patient's registration to discharge.

• Easy record-keeping: When we talk about a healthcare IoT system, it includes a huge number of patients, doctors, and other staff. Different patients suffer from different types of diseases. A particular disease requires particular treatment, which requires knowledge of a patient's health history, along with other details about them. Therefore, the timely delivery of health data of the patient to the doctor is important. In such a situation, the permanent storage of the patients' health data along with their respective details is essential. Similarly, for the smooth execution of the healthcare unit, details of the staff with their daily activity in a healthcare unit are also required for storage. A healthcare unit must also track its condition and financial transactions for further development of the unit. A healthcare IoT enables the user to keep these records in a safe environment and deliver them to the authorized user as per requirement. Moreover, these recorded data are accessible from any part of the globe.

Easy diagnosis: We have already explained that a healthcare IoT system stores the data of the patient in a secure manner. Sometimes, for diagnosing a disease, a huge chunk of prior data is required. In a healthcare IoT system, the diagnosis of the disease becomes easier with the help of certain learning mechanisms along with the availability of prior datasets.

Risk in healthcare IoT

Loss of connectivity: A healthcare IoT system consists of different physiological sensors that sense and transmit the sensed data to a centralized unit. Moreover, continuous data transmission from the patient is expected in a good healthcare system. Intermittent connectivity may result in data loss, which may result in a life-threatening situation for the patient. Proper and continuous connectivity is essential in a healthcare IoT system.

• Security: A healthcare IoT system contains the health data of different patients

	associated with the system. The healthcare system must keep the data confidential. This data should not be accessible to any unauthorized person. On the other hand, different persons and devices are associated with a healthcare IoT system. In such a system, the risk of data tampering and unauthorized access is quite high. • Error: Data analytics helps a healthcare IoT system to predict the patients' condition and diagnosis of diseases. A huge amount of data needs to be fed into the system in order to perform accurate analytics. Moreover, the management of a huge amount of data is a crucial task in any IoT-based system. Particularly, in the healthcare system, errors in data may lead to misinterpretation of symptoms and lead to the wrong diagnosis of the patient. It is a challenging task to construct an error-free healthcare IoT architecture.			