CBCS SCHEME

USN | | | | | | | | | |

BETCK205H/BETCKH205

Second Semester B.E./B.Tech. Degree Examination, June/July 2024
Introduction to Internet of Things (IOT)

Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	M	L	C
Q.1	a.	Classify the network types based on physical topologies and connection types with schematic diagram.	10	L2	CO1
	b.	With a neat diagram, explain the interdependency technology for IOT planes.	10	L2	CO1
		OR			
Q.2	a.	With neat diagram, explain the network communication between two hosts following OSI model.	10	L2	CO1
	b.	Explain the interdependencies and reach of IoT over various application domains and networking paradigms.	10	L2	CO1
		Module – 2			
Q.3	a.	Outline the basic differences between transducers, sensors and actuators.	6	L2	CO2
	b.	Explain the major factors influence the choice of sensors in IoT based sensing applications.	8	L2	CO2
	c.	Define Sensor and explain the characteristics of sensor.	6	L1	CO1
		OR			
Q.4	a.	Classify the sensor based on : i) Power requirements ii) Sensor output iii) Power to be measured.	10	L2	CO2
	b.	Classify Sensing types on the nature of the environment and the physical sensors.	10	L2	CO2
		Module – 3			
Q.5	a.	Explain IoT device design and selection considerations.	10	L2	CO2
	b.	What are the parameters considered for off loading the data and identify typical data offload locations available in context of IoT.	10	L2	CO2
		OR			
Q.6	a.	Explain event detection using onsite , offsite remote processing topology and collaborative processing technology.	10	L2	CO2
	b.	Classify the data based on how they can be accessed and stored and the importance of processing of IoT	10	L2	CO2

		Module – 4			
Q.7	a.	Explain the classification of virtualization based on the requirements of the user.	6	L2	CO2
	b.	Explain different types of cloud model.	10	L2	CO1
	c.	What is SLA and mention its metrics.	4	L2	CO2
		OR			
Q.8	a.	What are the advantages of virtualization?	10	L2	CO1
	b.	Explain different types of cloud simulators with its features.	10	L2	CO1
		Module – 5			
Q.9	a.	Explain the different components of health care IoT.	10	L2	CO1
	b.	Explain the architecture and advantages of vehicular IoT.	10	L2	CO2
		OR			
Q.10	a.	What is Machine Learning? What are the advantages and challenges of Machine Learning?	10	L2	CO2
	b.	What are the advantages and risk of health care IoT?	10	L2	CO2

*****

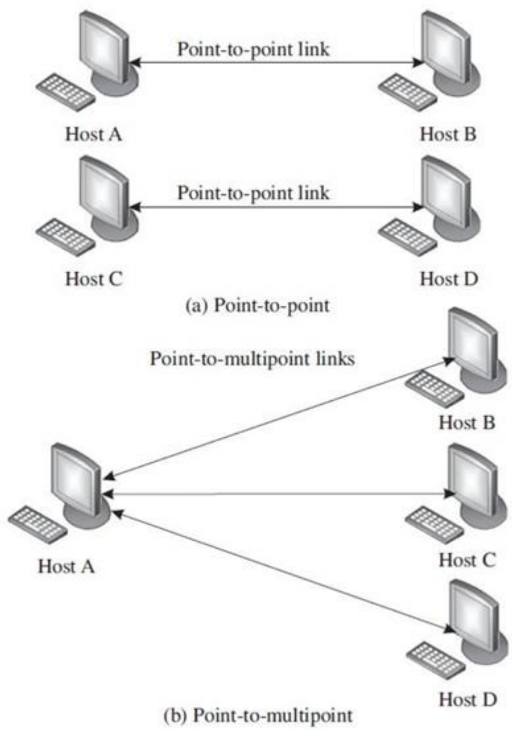
Solution QP – July 2024

Sub:	Introduction to Internet of Things (IOT)	Sub Code:	**BETCK205H**	Branch:	ECE, CSE, CSDS

Date:	Feb 2024	Duration:	3 hours	Max Marks:	100	Sec:	II	OBE

		MARKS	CO	RBT
1a	**a. Classify the network types based on Physical topologies and connection types with schematic diagram.**	[10]	CO1	L2

Depending on the way a host communicates with other hosts, computer networks are of two types: Point-to-point and Point-to-multipoint.
I. Point-to -point: Point-to-point connections are used to establish direct connections between two hosts. Day-to-day systems such as a remote control for an air conditioner or television is a point to point connection, where the connection has the whole channel dedicated to it only. These networks were designed to work over duplex links and are functional for both synchronous as well as asynchronous systems. II. Point-to-multipoint: In a point-to-multipoint connection, more than two hosts share the same link. This type of configuration is similar to the one-to-many connection type. Point-to-multipoint connections find popular use in wireless networks and IP telephony. The channel is shared between the various hosts, either spatially or temporally. One common scheme of spatial sharing of the channel is frequency division multiple access (FDMA). Temporal sharing of channels include approaches such as time division multiple access (TDMA). Point to-multipoint connections find popular use in present-day networks, especially while enabling communication between a massive number of connected devices.



(a) Point-to-point
(b) Point-to-multipoint

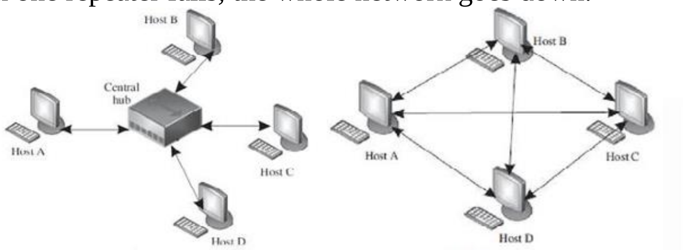
Depending on the physical manner in which communication paths between the hosts are connected, computer networks can have the following four broad topologies: Star, Mesh, Bus, and Ring.
Star: In a star topology, every host has a point-to-point link to a central controller or hub. The hosts cannot communicate with one another directly; they can only do so through the central hub. The hub acts as the network traffic exchange. The main advantages of the star topology are easy installation and the ease of fault identification

within the network. However, the main disadvantage of this topology is the danger of a single point of failure. If the hub fails, the whole network fails.

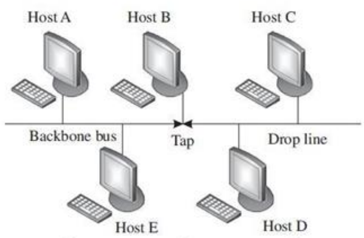
Mesh: In a mesh topology, every host is connected to every other host using a dedicated link (in a point-to-point manner). This implies that for n hosts in a mesh, there are a total of n(n-1)/2 dedicated full duplex links between the hosts. This massive number of links makes the mesh topology expensive.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

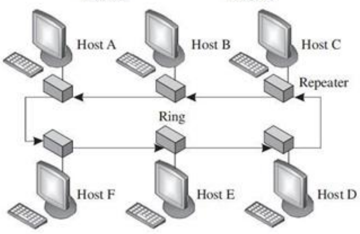
Bus: A bus topology follows the point-to-multipoint connection. A backbone cable or bus serves as the primary traffic pathway between the hosts. The hosts are connected to the main bus employing drop lines or taps. The main advantage of this topology is the ease of installation. However, there is a restriction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

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



(a) Star topology (b) Mesh topology

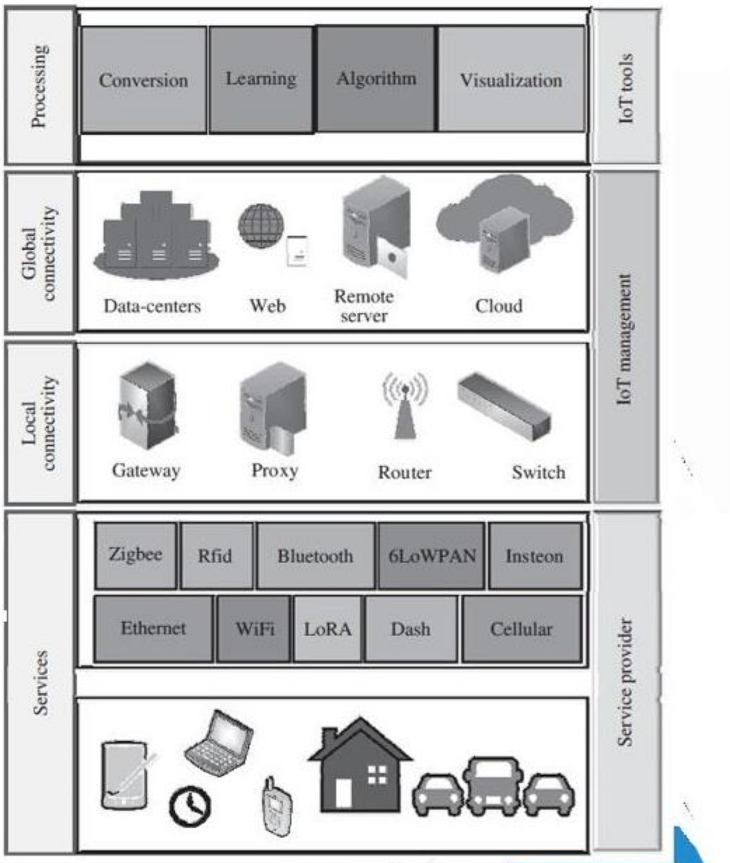




(c) Bus topology

1b	**With a neat diagram explain the interdependency technology for IoT planes.**	[10]	CO1	L2

Ans: IoT is a paradigm built upon complex interdependencies of technologies (both legacy and modern), which occur at various planes. we can divide the IoT paradigm into four planes: services, local connectivity, global connectivity, and processing. If we consider a bottom-up view, the services offered fall under the control and purview of service providers. The service plane is composed of two parts: 1) things or devices and 2) low-power connectivity. Typically, the services offered in this layer are a combination of things and low-power connectivity. The things may be wearables, computers, smartphones, household appliances, smart glasses, factory machinery, vending machines, vehicles, UAVs, robots, and other such contraptions (which may even be just a sensor). The immediate low-power connectivity, which is responsible for connecting the things in local implementation, may be legacy protocols such as 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. 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 plan.



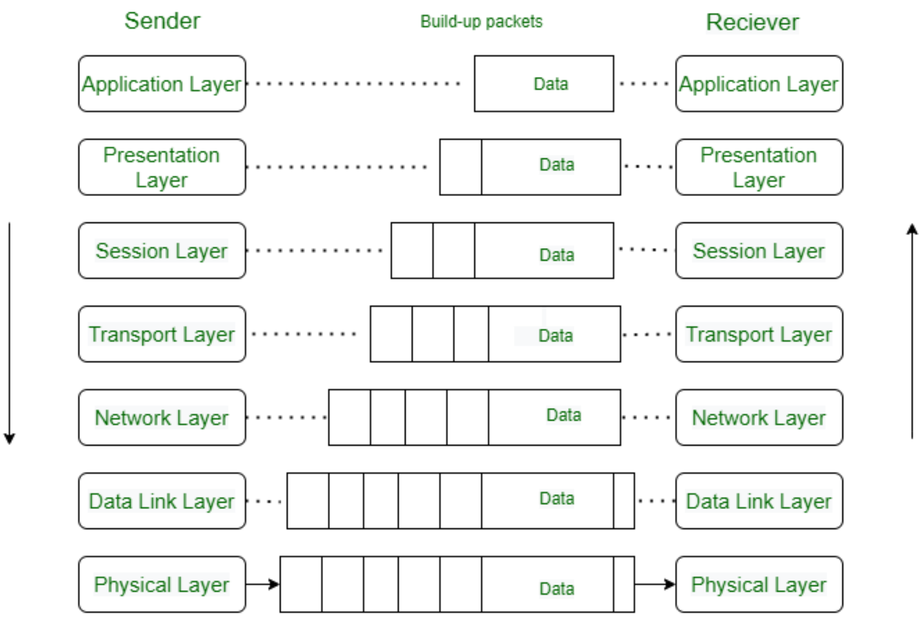
ure 9: The IoT planes, various enablers of IoT, and the complex interdependencies among

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. In continuation, the penultimate plane of global connectivity plays a significant role in enabling IoT in the real sense by allowing for worldwide implementations and connectivity between things, users, controllers, and applications. This plane also falls under the purview of IoT management as it decides how and when to store data, when to process it, when to forward it, and in which form to forward it. The Web, data-centers, remote servers, Cloud, and others make up this plane. The paradigm of "fog computing" lies between the planes of local connectivity and global connectivity. The final plane of processing can be considered as a top-up of the basic IoT networking framework. The members in this plane may be termed as IoT tools, simply because they wring-out useful and human-readable information from all the raw data that flows from various IoT devices and deployments. The various sub-domains of this plane include intelligence, conversion (data and format conversion, and data cleaning), learning (making sense of temporal and spatial data patterns), cognition (recognizing patterns and mapping it to already known patterns), algorithms (various control and monitoring algorithms), visualization (rendering numbers and strings in the form of collective trends, graphs, charts, and projections), and analysis (estimating the usefulness of the generated information, making sense of the information with respect to the application and place of data generation, and estimating future trends based on past and present patterns of information obtained). Various computing paradigms such as "big data", "machine Learning", and others, fall within the scope of this domain.

2a	**With a neat diagram explain the network communication between two hosts following the OSI model.**	[10]	CO1	L2

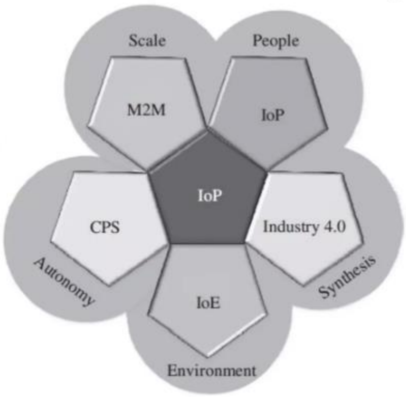
Ans:
The Open System Interconnection (OSI) model is a standard "reference model" created by an International Organization for Standardization (ISO) to describe how software and hardware components involved in network communication divide efforts and interact with each other.

The communication process in the OSI/ISO 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, 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), excep**t 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

<table>
<tr>
<td></td>
<td>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.
5. Each layer is assumed to handle messages or data from the layers that are above or below it.
6. Thus, each layer takes data from the adjacent layer, Handles it according to these rules, and then sends the processed data to the next layer on the other side.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2b</td>
<td>Explain the interdependencies and reach of IoT over various application domains and networking paradigms.

Ans:
• Technological interdependencies of IoT with other domains and networking paradigms
• M2M: Machine-to-Machine Paradigm
Talk Amongst Themselves without Human Interventic
• CPS: Cyber Physical System Paradigm
Sensing, Processing & Actuation - Feedback Mechanis
• IoE: Internet of Environment Paradigm
minimizing & reversing the ill-effects of Internet-based technologies
• Industry 4.0: 4th industrial revolution
digitization of manufacturing industry
• IoP: Internet of People
Decentralize Online Social Interactions, Payments, Transactions


IOT vs M2M
• M2M refers to communications and interactions between machines and devices.
• These interactions occurs in cloud computing infrastructure
• M2M collects data from machinery and sensors, also enabling device management and device interaction.
• Telecommunication services providers introduced the term M2M and technically emphasized on machine interactions via one or more communication networks (e.g., 3G, 4G, 5G, satellite, public networks).
• M2M is part of the IoT and is considered as one of its sub-domains
• 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.

IOT vs CPS
• Cyber physical systems (CPS) encompasses sensing, control, actuation and feedback as a package.
• A digital twin is attached to a CPS-based system.
• A digital twin is a virtual system–model relation, in which the system signifies a physical system or equipment or a piece of machinery, while the model represents the mathematical model or representation of the physical system’s behavior or operation.
• A digital twin is used parallel to a physical system, especially in CPS as it allows for the comparison of the physical system’s output, performance and health.
• Based on feedback from the digital twin, a physical system can be easily given corrective directions/commands to obtain desirable outputs.
• The IoT paradigm does not compulsorily need feedback or a digital twin system.
• IoT is more focused on networking than controls.
• A sub-systems in an IoT environment may include feedback and controls too
• CPS is also one of the sub-domains of IoT.

IOT vs WoT</td>
<td>[10]</td>
<td>CO1</td>
<td>L2</td>
</tr>
</table>

	• The Web of Things (WoT) paradigm enables access and control over IoT resources and applications. • These resources and applications are built using technologies such as HTML 5.0, JavaScript, Ajax, PHP and others. • REST (Representational State Transfer) is one of the key enablers of WoT. • The use of RESTful principles and RESTful APIs enables both developers and deployers to benefit from the recognition, acceptance and maturity of existing web technologies without redesign and redeploy solutions. • Still, designing and building the WoT paradigm has various adaptability and security challenges, when trying to build a globally uniform WoT. • As IoT is focused on creating networks comprising objects, things, people, systems and applications, which do not consider the unification aspect and the limitations of the Internet, the need for WoT, which aims to integrate the various areas of IoT into the existing Web. • Technically, WoT can be thought of as an application layer-based hat added over the network layer. • However, the scope of IoT applications is much broader; IoT also which includes non-IP-based systems that are not accessible through the web.			
3a	**Outline the basic differences between Sensors, Actuators and TRansducers.**			

Table 1: Basic outline of the differences between transducers, sensors, and actuators

Parameters	Transducers	Sensors	Actuators
Definition	Converts energy from one form to another.	Converts various forms of energy into electrical signals.	Converts electrical signals into various forms of energy, typically mechanical energy.
Domain	Can be used to represent a sensor as well as an actuator.	It is an input transducer.	It is an output transducer.
Function	Can work as a sensor or an actuator but not simultaneously.	Used for quantifying environmental stimuli into signals.	Used for converting signals into proportional mechanical or electrical outputs.
Examples	Any sensor or actuator	Humidity sensors, Temperature sensors, Anemometers (measures flow velocity), Manometers (measures fluid pressure), Accelerometers (measures the acceleration of a body), Gas sensors (measures concentration of specific gas or gases), and others	Motors (convert electrical energy to rotary motion), Force heads (which impose a force), Pumps (which convert rotary motion of shafts into either a pressure or a fluid velocity).

3b	Explain the Major factors that influence the choice of sensors in IoT based sensing applications The choice of sensors in an IoT sensor node is critical and can either make or break the feasibility of an IoT deployment. 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. ● 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.			

	● Additionally, 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. Accuracy and Precision: ● The accuracy and precision of measurements provided by a sensor are critical in deciding the operations of specific functional processes. ● For example, a standard temperature sensor can be easily integrated with 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. 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. 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. ● The wearable sensors are highly energy-efficient, small in size, and almost part of the wearer's regular wardrobe.			
4 a	Classify sensors based on: 1) Power requirement ii) Sensor output iii) Power to be measured. Ans: 1) Based upon the power requirement sensors may be of two kinds: Passive sensor: it does not need any additional energy source and directly generates an electric signal in response to an external stimulus. That is, the input stimulus energy is converted by the sensor into the output signal. Most of passive sensors are direct sensors as we defined them earlier. Example: a thermocouple, a photodiode, and a piezoelectric sensor. Active Sensor: it requires external power for its operation, which is called an excitation signal. That signal is modified by the sensor to produce the output signal. Example: a			

	thermistor is a temperature sensitive resistor. It does not generate any electric signal, but by passing an electric current through it (excitation signal) its resistance can be measured by detecting variations in current and/or voltage across the thermistor. 2) Based upon the sensor output, sensors may be of two kinds: Analog Sensors: It produce an output signal which is usually in the form of voltage, current, or resistance, proportional to the measured quantity. Digital Sensors: It provide discrete or digital data as output. 3) Based upon the power to be measured sensors may classified as: (i) Physical sensors: Physical sensors measure a physical quantity and convert it into a signal, which can be identified by the user. These sensors can detect environmental changes, such as force, acceleration, rate of flow, mass, volume, density, and pressure. (ii) Chemical sensors: A chemical sensor is defined as, "a device that converts chemical information into an analytically useful signal ranging from the concentration of a particular sample component to total composition analysis." Chemical sensor is employed to monitor the activity or concentration of the respective chemical species in the gas or liquid phase. (iii) Thermal sensors: A thermal sensor is a device that is used to measure the temperature of an environment and transforms the input data into electronic data to record or monitor signal of temperature changes. Examples of temperature sensors include thermocouples, thermistors, and RTDs. (iv) Biological sensors: Biological sensors monitor biomolecular processes, such as antibody/antigen interactions, DNA interactions, enzymatic interactions, or cellular communication processes.			
4 b	**Classify sensing types on the nature of the environment and the physical sensors.** **Ans:** The final classification of the sensors are Analog and Digital, these produce an analog output i.e., a continuous output signal (usually voltage but sometimes other quantities like Resistance etc.) with respect to the quantity being measured. Digital, in contrast to Analog, work with discrete or digital data. The data in digital sensors, which is used for conversion and transmission, is digital in nature. The following is a list of different types of sensors that are commonly used in various applications with examples. All these types are used for measuring one of the physical properties like Temperature, Resistance, Capacitance, Conduction, Heat Transfer etc.			

	Type of Sensor / **Used For** Temperature Sensor — Controlling HVAC systems in homes and offices Proximity Sensor — Detecting objects in automatic doors Accelerometer Sensor — Screen orientation in smartphones IR Sensor (Infrared Sensor) — Remote controls for TVs and other devices Pressure Sensor — Monitoring tire pressure in vehicles Light Sensor — Adjusting screen brightness on smartphones Ultrasonic Sensor — Parking assistance in cars Flow and Level Sensor — Managing water levels in tanks Smoke, Gas and Alcohol Sensor — Detecting smoke and gas leaks in homes Microphone (Sound Sensor) — Voice recognition in smart speakers Touch Sensor — Touchscreens on smartphones and tablets Color Sensor — Color detection in industrial sorting machines Humidity Sensor — Controlling humidity levels in greenhouses Magnetic Sensor (Hall Effect Sensor) — Detecting the position of a rotating object Position Sensor — Tracking the position of machine parts Tilt Sensor — Detecting the tilt of gaming controllers PIR Sensor — Motion detection in security systems			
1. 5a	**a.**Explain IOT device design and selection considerations IoT Device Design and Selection Considerations Size: ➢ This decides the form factor and the energy consumption of a sensor node. ➢ The larger the form factor, the larger the energy consumption of the hardware. Energy ➢ The energy requirements of a processor are the most important consideration. ➢ The higher the energy requirements, the higher the energy source (battery) replacement frequency. Cost ➢ The cost is the driving force in deciding the density of deployment of sensor nodes for IoT-based solutions. ➢ The 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. IoT Device Design and Selection Considerations Memory: ➢ Features such as local data processing, data storage, data filtering, data formatting and other features rely heavily on the memory capabilities of devices. ➢ The memory requirements (both volatile and non-volatile memory) of IoT devices determine the capabilities of the device. ➢ However, devices with higher memory tend to be costlier for obvious reasons. Processing power: • Processing power decides what type of sensors and the type of application	[10]	CO2	L2

	that is accommodated with the IoT device/node, and what processing features can integrate on-site with the IoT device. • 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 an IoT device 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 meagre I/O voltage rating of 3.3 V, as compared to 5 V for the somewhat older processors. Add-ons • The support of various add-ons to a processor like analogue to digital conversion (ADC) units, in-built clock circuits, connections to USB and ethernet, inbuilt wireless access capabilities and others help in defining the robustness and usability of a processor or IoT device in various application scenarios. • Additionally, these add-ons also decide how fast a solution can be developed, especially the hardware part of the whole IoT application. • The presence of these options with the processor makes the processor ordevice highly lucrative to the users/ developers.			

	b. What are the parameters considered for offloading the data and identify typical data offload locations available in the context of IOT. 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 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 volume.	[10]	CO2	L2

6.	**a.Explain event detection using onsite, ofsite remote processing topology and collaborative processing technology.**	10	L2	CO2

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.
The fire detection event using an off-site remote processing topology is shown in Fig 5b.

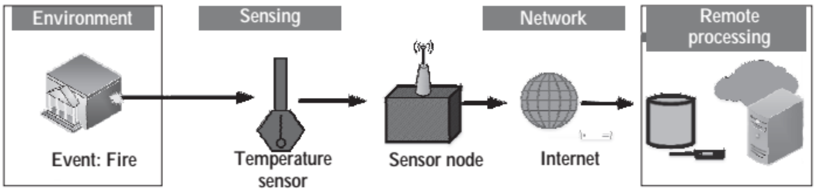


Figure 5a: Event detection using an off-site remote processing topology

Here the sensing of an event is performed locally, and the decision making is outsourced to a remote processor (here, cloud). However, this paradigm tends to use up a lot of network bandwidth and relies heavily on the presence of network connectivity between the sensor nodes and the remote processing infrastructure.

✓ **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.**

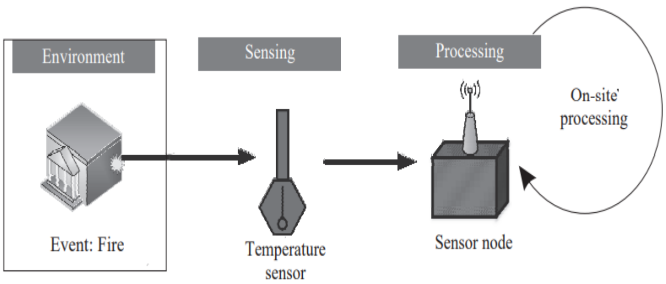


Figure 3.2: Event detection using an on-site processing topology

Collaborative processing

- **This processing topology typically finds use in scenarios with limited or no network connectivity, especially systems lacking a backbone network.**
- **Additionally, this topology can be quite economical for large-scale deployments spread over vast areas, where providing networked access to a remote infrastructure is not viable.**
- **In such scenarios, the simplest solution is to club together the processing power of nearby processing nodes and collaboratively process the data in the vicinity of the data source itself.**

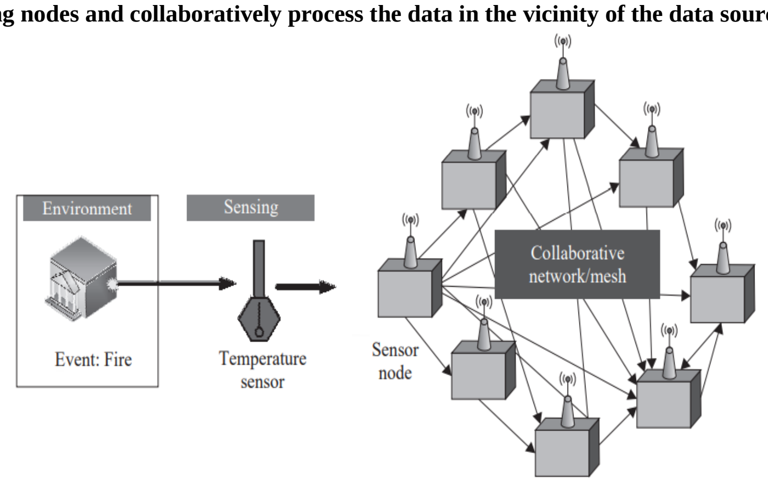


Figure 3.4: Event detection using a collaborative processing topology

6.	**b.Classify the data based on how they can be accessed and stored and hte importance of processing of Iot .**	10	L2	CO2

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 can be accessed and stored: 1) Structured data and 2) unstructured data.

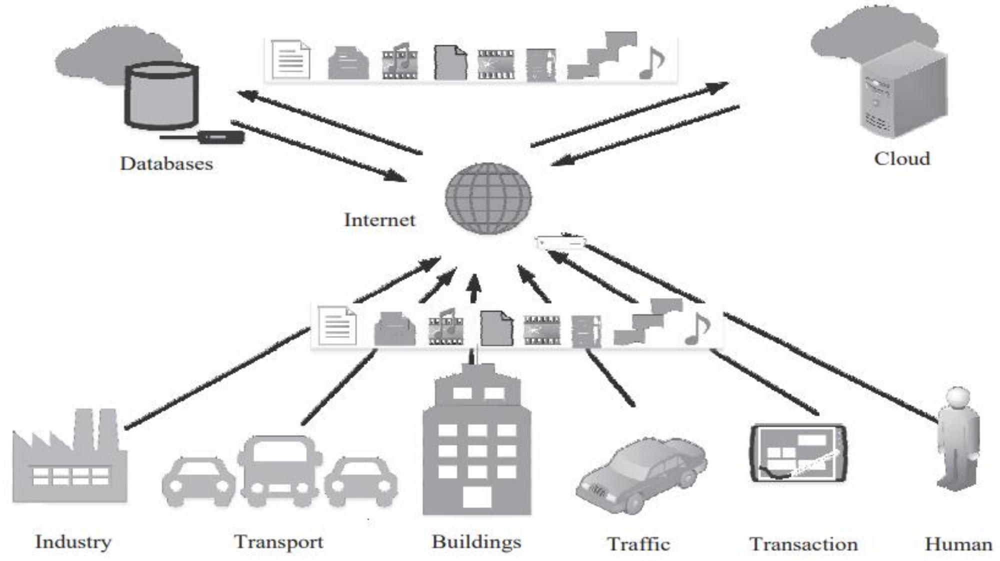


Figure 3.1: The various data generating and storage sources connected to the Internet and the plethora of data types contained within it

- **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 for accessing 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.**

3.2 Importance of Processing in IoT

- ✓ **The necessity of intelligent and resourceful data processing techniques has become even more crucial with the rapid advancements in IoT, which is laying enormous pressure on the existing network infrastructure globally.**
- ✓ **we first divide the data to be processed into three types based on the urgency of processing:**
  1) Very time critical,

	2) Time critical, and 3) Normal. ✓ Data from sources such as flight control systems, healthcare, and other such sources, which need immediate decision support, are deemed as very critical. These data have a very low threshold of processing latency, typically in the range of a few milliseconds. ✓ Data from sources that can tolerate normal processing latency are deemed as timecritical data. These data, generally associated with sources such as vehicles, traffic, machine systems, smart home systems, surveillance systems, and others, which can tolerate a latency of a few seconds fall in this category. ✓ Finally, the last category of data, normal data, can tolerate a processing latency of a few minutes to a few hours and are typically associated with less data-sensitive domains such as agriculture, environmental monitoring, and others.	10	L2	CO1

Q. No.	Question	Marks	RBT	CO
7a	**Explain the classification of virtualization based on the requirements of the user.**	6	L2	CO2

- **Hardware Virtualization:** This type of virtualization indicates the sharing of hardware resources among multiple users. For example, a single processor appears as many different processors in a cloud computing architecture.
- **Storage Virtualization:** In storage virtualization, the storage space from different entities are accumulated virtually, and seem like a single storage location.
- **Application Virtualization:** A single application is stored at the cloud end. However, as per requirement, a user can use the application in his/her local computer without ever actually installing the application.
- **Desktop Virtualization:** This type of virtualization allows a user to access and utilize the services of a desktop that resides at the cloud. The users can use the desktop from their local desktop.

Q. No.	Question	Marks	RBT	CO
7b	**Explain different types of cloud model.**	10	L2	CO1

- As per the National Institute of Standards and Technology (NIST) [1] and Cloud Computing Standards Roadmap Working Group, the cloud model can be divided into two parts:
- Service model and
- Deployment model

Further the service model is categorized as:

- Software-as-a-Service (SaaS),
- Platform-as-a-Service (PaaS), and
- Infrastructure-as-a-Service (IaaS).

On the other hand, the deployment model is further categorized as:

- Private cloud,
- Community cloud,
- Public cloud, and
- Hybrid cloud.
- Software-as-a-Service (SaaS): This service provides access to different software applications to an end user through Internet connectivity. Ex : Google Workspace, Dropbox, Salesforce
- Platform-as-a-Service (PaaS): PaaS provides a computing platform, by which a user can develop and run different applications. Ex: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine
- Infrastructure-as-a-Service (IaaS): IaaS provides infrastructure such as storage, networks, and computing resources. A user uses the infrastructure without purchasing the software and other network components. Google Compute Engine (GCE)

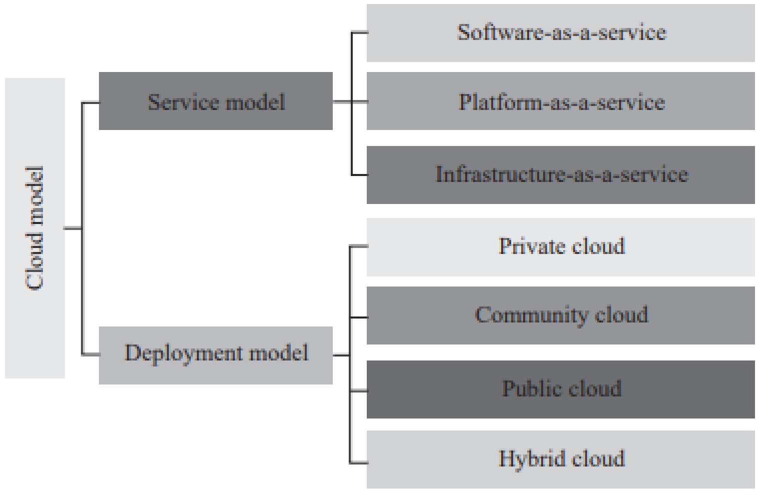


Figure 10.4 Cloud model

Deployment Model

- **Private Cloud:** This type of cloud is owned explicitly by an end user organization. The internal resources of the organization maintain the private cloud.
- **Community Cloud:** This cloud forms with the collaboration of a set of organizations for a specific community. For a community cloud, each organization has some shared interests.
- **Public Cloud:** The public cloud is owned by a third party organization, which provides services to the common public. The service of this cloud is available for any user, on a payment basis.
- **Hybrid Cloud:** This type of cloud comprises two or more clouds (private, public, or community)

7C **What is SLA and mention its metrics.**

4 | L2 | CO2

- The most important actors in cloud computing are the end user/customer and CSP.
- Cloud computing architecture aims to provide optimal and efficient services to the end users and generate revenue from them as per their usage.
- Therefore, for a clear understanding between CSP and the customer about the services, an agreement is required to be made, which is known as service-level agreement (SLA).
- An SLA provides a detailed description of the services that will be received by the customer.
- **Customer Point of View:** Each CSP has its SLA, which contains a detailed description of the services. If a customer wants to use a cloud service, he/she can compare the SLAs of different organizations. Therefore, a customer can choose a preferred CSP based on the SLAs.
- **CSP Point of View:** In many cases, certain performance issues may occur for a particular service, because of which a CSP may not be able to provide

the services efficiently. Thus, in such a situation, a CSP can explicitly mention in the SLA that they are not responsible for inefficient service.

- **Availability:** This metric signifies the amount of time the service will be accessible for the customer.
- **Response Time:** The maximum time that will be taken for responding to a customer request is measured by response time.
- **Portability:** This metric indicates the flexibility of transferring the data to another service.
- **Problem Reporting:** How to report a problem, whom and how to be contacted, is explained in this metric.

Penalty: The penalty for not meeting the promises mentioned in the SLA.

8a.	What are advantages off virtualization?	10	L2	CO1

Advantages for End Users

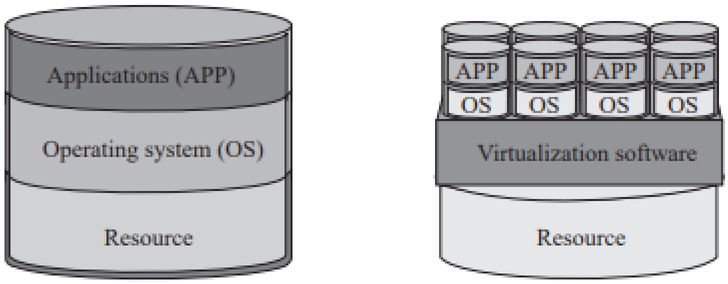
Variety: The process of virtualization in cloud computing enables an end user organization to use various types of applications based on the requirements.

Availability: Virtualization creates a logical separation of the resources of multiple entities without any intervention of end users.

Portability: Portability signifies the availability of cloud computing services from anywhere in the world, at any instant of time.

Elasticity: Through the concept of virtualization, an end user can scale-up or scale-down resource utilization as per requirements.

- **Resource Utilization**: Typically, a CSP in a cloud computing architecture procures resources on their own or get them from third parties. These resources are distributed among different users dynamically as per their requirements.
- **Effective Revenue Generation:** A CSP generates revenue from the end users based on resource utilization.



(a) Desktop (b) Virtualization

Figure 10.2 Traditional desktop versus virtualization

8b **Explain different types of cloud simulation with its features.**

Cloud simulation

Real deployment of the cloud is a complex and costly procedure.

Thus, there is a requirement for simulating the system through a cloud simulator before real implementation.

There are many cloud simulators that provide pre-deployment test services for repeatable performance evaluation of a system.

Typically, a cloud simulator provides the following advantages to a customer:

- Pre-deployment test before real implementation
- System testing at no cost
- Repeatable evaluation of the system
- Pre-detection of issues that may affect the system performance
- Flexibility to control the environment

CloudSim:

- Description: CloudSim is a popular cloud simulator that was developed at the University of Melbourne. This simulator is written in a Java-based environment.
- In CloudSim, a user is allowed to add or remove resources dynamically during the simulation and evaluate the performance of the scenario.

Features: CloudSim has different features, which are listed as follows:

(1) The CloudSim simulator provides various cloud computing data centers along with different data center network topologies in a simulation environment.

(2) Using CloudSim, virtualization of server hosts can be done in a simulation.

(3) A user is able to allocate virtual machines (VMs) dynamically.

(4) It allows users to define their own policies for the allocation of host resources to VMs.

(5) It provides flexibility to add or remove simulation components dynamically.

(6) A user can stop and resume the simulation at any instant of time.

CloudAnalyst:

1. Description: CloudAnalyst [4] is based on CloudSim. This simulator provides a graphical user interface (GUI) for simulating a cloud environment, easily. The CloudAnalyst is used for simulating large-scale cloud applications.

(b) Features:

(1) The CloudAnalyst simulator is easy to use due to the presence of the GUI.

(2) It allows a user to add components and provides a flexible and high level of configuration.

(3) A user can perform repeated experiments, considering different parameter values.

- (4) It can provide a graphical output, including a chart and table.

GreenCloud:

(a) Description: GreenCloud [2] is developed as an extension of a packet- level network simulator, NS2. This simulator can monitor the energy consumption of different network components such as servers and switches.

(b) Features:

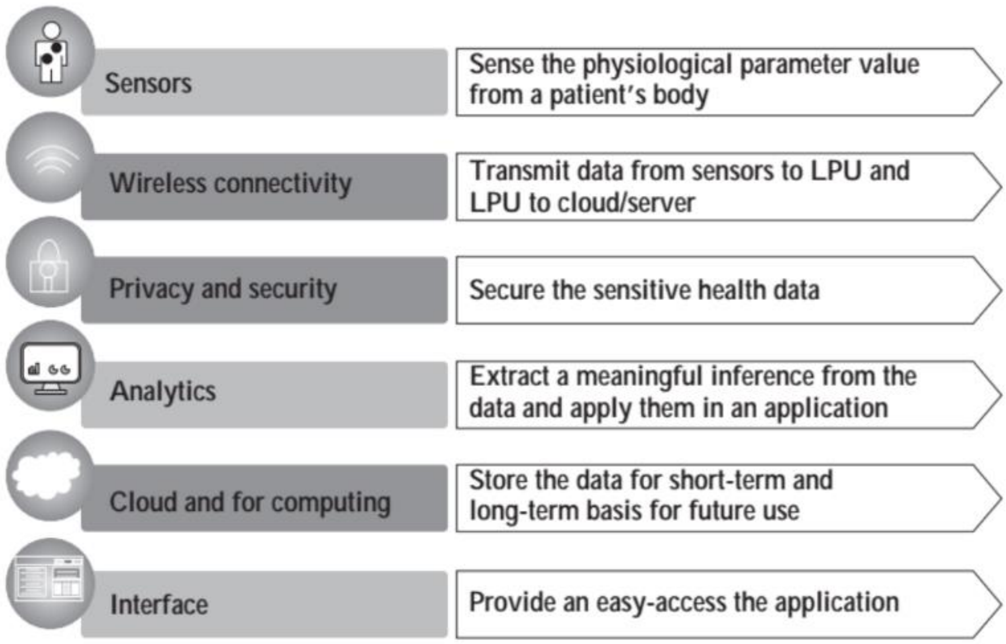
(1) GreenCloud is an open-source simulator with user-friendly GUI.

(2) It provides the facility for monitoring the energy consumption of the network and its various components.

(3) It supports the simulations of cloud network components.

(4) It enables improved power management schemes.

(5) It allows a user to manage and configure devices, dynamically, in simulation.

9	**9a. Healthcare IoT (Internet of Things) consists of various interconnected components that work together to provide efficient, real-time healthcare services** **1. Sensors: Layer 1 mainly consists of physiological sensors that collect the physiological** **parameters of the patient. Few commonly used physiological sensors and their uses are** **depicted in Table 1.** **2. Wireless Connectivity:** **• The communication between the wearable sensors and the LPU is through either wired or** **wireless connectivity. .** **• The wireless communication between the physiological sensors and LPU occurs with the** **help of Bluetooth and ZigBee.** **• The communication between the LPU and the cloud or server takes place with Internet** **connectivity such as WiFi and WLAN.**  **For example, when a service is received by a cellphone, it uses GSM (global system for** **mobile communications). On the other hand, if the same service is received on a desktop,** **it can be through Ethernet or Wi-Fi.** **3. Privacy and Security:** **• Moreover, between LPU and the server/cloud, different networking devices work via** **network hops (from one networked device to another) to transmit the data.** **• If any of these devices are compromised, it may result in the theft of health data of a** **patient, leading to serious security breaches and ensuing lawsuits.** **• In order to increase the security of the healthcare data, different healthcare service** **providers and organizations are implementing healthcare data encryption and protection** **schemes.** **4. Analytics:**	10	L2	CO1

• For converting the raw data into information, analytics plays an important role in healthcare IoT.
• Several actors, such as doctors, nurses, and patients, access the healthcare information in a different customized format.
• Analytics plays a vital role in providing different actors in the system access to meaningful information extracted from the raw healthcare data.
• Analytics is also used for diagnosing a disease from the raw physiological data available.

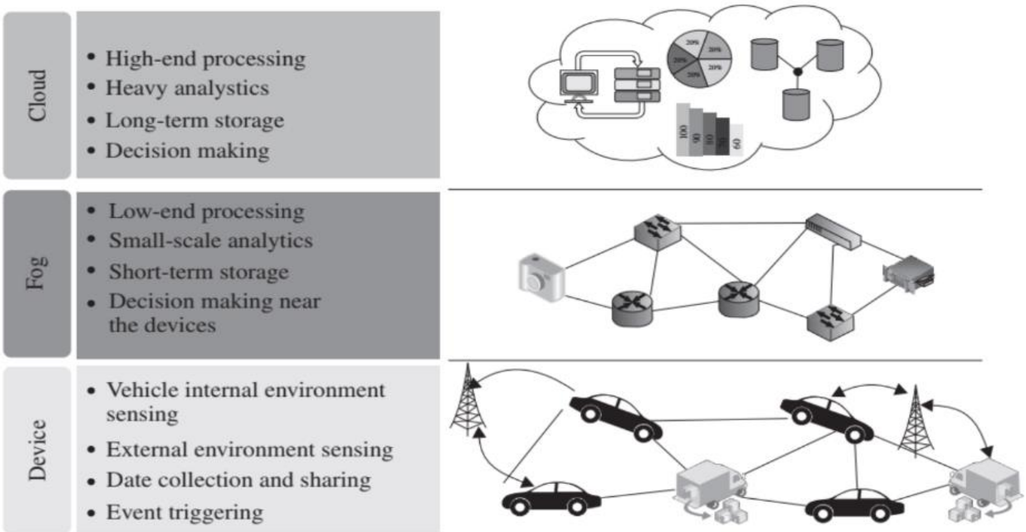
5. Cloud and Fog Computing:

• For storing these huge amounts of heterogeneous health data, efficient storage space is essential.
• These data are used for checking the patient's history, current health status, and future for diagnosing different diseases and the symptoms of the patient.
• To store health data in a healthcare IoT system, cloud storage space is used.
• The major challenges in storage are security and delay in accessing the data.

6. Interface:

• Healthcare IoT is a very crucial and sensitive application.
• Thus, the user interface must be designed in such a way that it can depict all the required information clearly and, if necessary, reformat or represent it such that it is easy to understand.
• To store health data in a healthcare IoT system, cloud storage space is used.
• An interface must also contain all the useful information related to the services.

9b.



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.
• IoT enables a vehicle to sense its internal and external environments to make certain

10	L2	CO2

autonomous decisions.

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.
- RSU works as a local centralized unit that manages the data from the vehicles.

Fog:

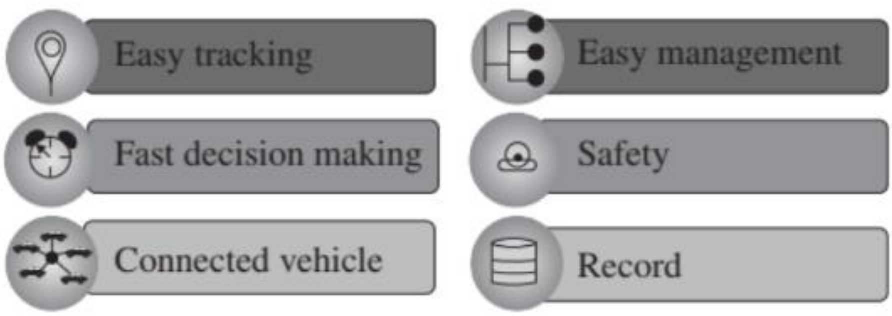
- Fast decision making is pertinent to avoid accidents and traffic mismanagement.
- Fog computing plays a crucial role by providing decisions in real-time, much near to the devices.
- The fog layer helps to minimize data transmission time in a vehicular IoT system.

Cloud:

- For the processing of huge data, fog computing is not enough. 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.
- For long-term storage, cloud computing is used as a scalable resource in vehicular IoT systems.

Advantages of vehicular IoT

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.



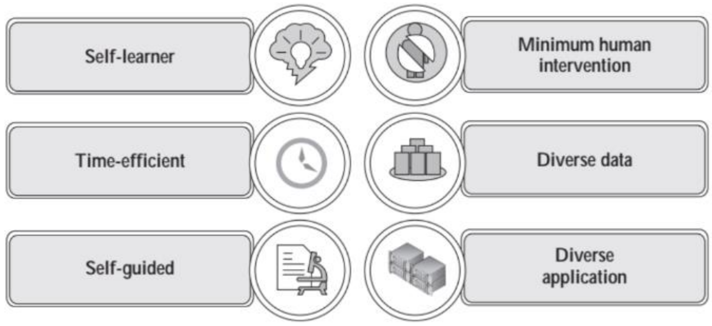
Easy tracking: In a vehicular IoT system, the tracking of vehicles is straightforward; the system can collect information at a remote location.

2. Fast Decision Making:

- Most of the decisions in the connected vehicle environment are time critical.
- 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.

3. Connected vehicle:

	• A vehicular IoT system provides an opportunity to remain connected and share information among different vehicles. 4. Easy management: • 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. • IoT infrastructure helps in managing the huge number of users located at different geographical coordinates. 5. Safety: • With easy management of the system, both the internal 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. 6. 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.			
10	10 a. Machine Learning: • The term “machine learning” was coined by Arthur Lee Samuel, in 1959. • 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. • 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 Machine Learning (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.	10	L2	CO2



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.
1. Self Learner:

• ML tools are capable of producing faster results as compared to human interpretation.
• 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.
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.
5. Diverse Data Handling:

• On the other hand, industrial sensors help in the detection of machiney 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.

Challenges in Machine Learning (ML):
An ML algorithm utilizes a model and its corresponding input data to produce an
output. A few major challenges in ML are listed as follows:
• Data Description: The data acquired from different sensors are required to be informative
and meaningful. Description of data is a challenging part of ML.
• Amount of Data: In order to provide an accurate output, a model must have sufficient
amount of data. The availability of a huge amount of data is a challenge in ML.

• Selection of Model: Multiple models may be suitable for serving a particular purpose.
However, one model may perform better than others. In such cases, the proper selection of
the model is pertinent for ML.
• Erroneous Data: A dataset may contain noisy or erroneous data. On the other hand, the
learning of a model is heavily dependent on the quality of data. Since erroneous data
misleads the ML model, its identification is crucial.

• Quality of Model: After the selection of a model, it is difficult to determine the quality of
the selected model. However, the quality of the model is essential in an ML-based system.

10 b. Risk in Healthcare IoT
In a healthcare IoT system, there are multiple risks as well.
1. Loss of Connectivity:
• Intermittent connectivity may result in data loss, which may result in a life-threatening
situations for the patient.

• Proper and continuous connectivity is essential in a healthcare IoT system.
2. Security:
• The healthcare system must keep the data confidential.
• 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.
3. Error:
• 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.

10	L2	CO2

COURSE INSTRUCTOR	CCI	HOD