USN | | | | | | | | | |

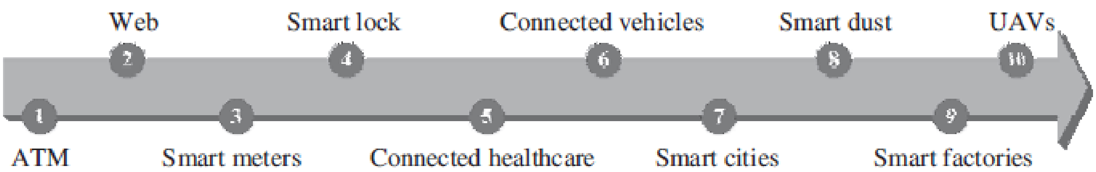
Internal Assessment Test 1 – October 2024

Sub:	**Internet of Things**					Sub Code:	**21CS735**	Branch:	**AInDS**
Date:		Duration:	**90 minutes**	Max Marks:	**50**	Sem	**VII**		**OBE**

Answer any FIVE Questions			**MARKS**	**CO**	**RBT**
Q1	a	Explain how evolution of IoT take place	[5]	1	2
	b	Differentiate between IoT and CPS.	[5]	1	2
Q 2		Differences between transducers, sensors, and actuators	[10]	2	2
Q 3		Explain different IoT networking Components	[10]	1	2
Q 4	a	How is mobility handled in IoT networks?	[5]	1	1
	b	Explain different Sensing Types	[5]	2	1
Q 5		Explain in detail different types of Sensors with example	[10]	2	1
Q 6		Discuss different interdependencies used in IoT	[10]	1	2

CI **CCI** **HOD**

Q 1 a) Explain how evolution of IoT take place



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

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

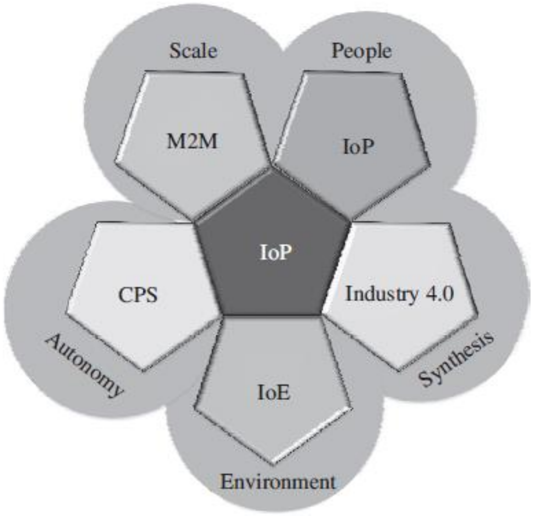
• Smart Meters: The earliest smart meter was a power meter, which became operational in early 2000. These power meters were capable of communicating remotely with the power grid. They enabled remote monitoring of subscribers' power usage and eased the process of billing and power allocation from grids.

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

- Connected Healthcare: Here, healthcare devices connect to hospitals, doctors, and relatives to alert them of medical emergencies and take preventive measures. The devices may be simple wearable appliances, monitoring just the heart rate and pulse of the wearer, as well as regular medical devices and monitors in hospitals. The connected nature of these systems makes the availability of medical records and test results much faster, cheaper, and convenient for both patients as well as hospital authorities.
- Connected Vehicles: Connected vehicles may communicate to the Internet or with other vehicles, or even with sensors and actuators contained within it. These vehicles self-diagnose themselves and alert owners about system failures.
- Smart Cities: This is a city-wide implementation of smart sensing, monitoring, and actuation systems. The city-wide infrastructure communicating amongst themselves enables unified and synchronized operations and information dissemination. Some of the facilities which may benefit are parking, transportation, and others.
- Smart Dust: These are microscopic computers. Smaller than a grain of sand each, they can be used in numerous beneficial ways, where regular computers cannot operate. For example, smart dust can be sprayed to measure chemicals in the soil or even to diagnose problems in the human body.
- Smart Factories: These factories can monitor plant processes, assembly lines, distribution lines, and manage factory floors all on their own. The reduction in mishaps due to human errors in judgment or unoptimized processes is drastically reduced.
- UAVs: UAVs or unmanned aerial vehicles have emerged as robust publicdomain solutions tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other tasks.

Q 1 b) Differentiate between IoT and CPS.

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



Q 2) Differences between transducers, sensors, and actuators

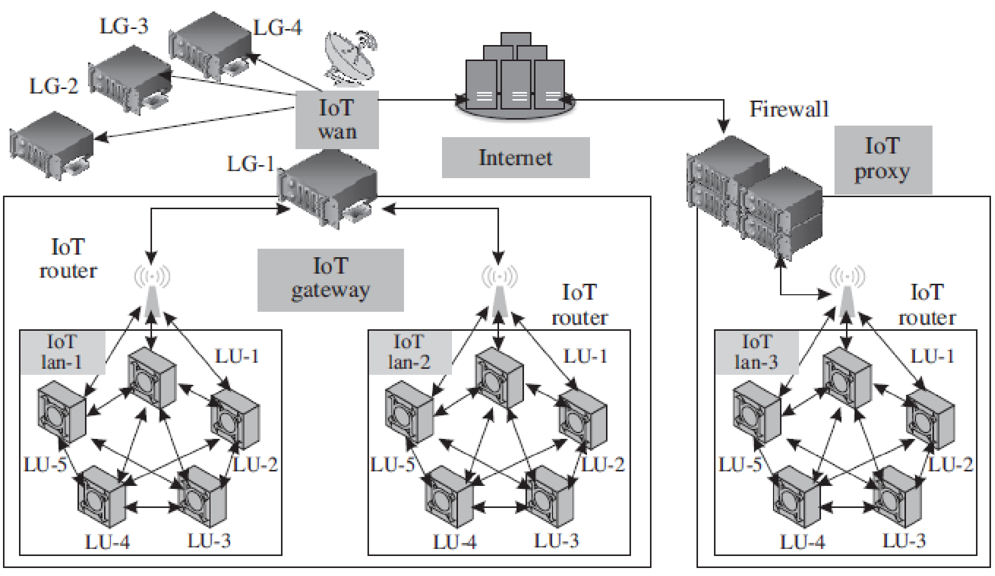
Parameters	Transducers	Sensors	Actuators
Definition	Converts energy from one form to another.	Converts various forms of energy into electrical signals.	Converts electrical signals into various forms of energy, typically mechanical energy.
Domain	Can be used to represent a sensor as well as an actuator.	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).

Q 3) Explain different IoT networking Components

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

means of a common gateway for that LAN. Connections outside the LAN are

through gateways and proxies.
(ii) **IoT Router**: An I oT router is a piece of networking equipment that is primarily tasked with the routing of packets between various entities in the IoT network; it keeps the traffic flowing correctly within the network. A router can be repurposed as a gateway by enhancing its functionalities.
(iii) **IoT LAN**: The local area network (LAN) enables local connectivity within the purview of a single gateway. Typically, they consist of short-range connectivity technologies. IoT LANs may or may not be connected to the Internet. Generally, they are localized within a building or an organization.
(iv) **IoT WAN**: The wide area network (WAN) connects various network segments such as LANs. They are typically organizationally and geographically wide, with their operational range lying between a few kilometers to hundreds of kilometers. IoT WANs connect to the Internet and enable Internet access to the segments they are connecting.
(v) **IoT Gateway**: An IoT gateway is simply a router connecting the IoT LAN to a WAN or the Internet. Gateways can implement several LANs and WANs. Their primary task is to forward packets between LANs and WANs, and the IP layer using only layer 3.
(vi) **IoT Proxy**: Proxies actively lie on the application layer and performs application layer functions between IoT nodes and other entities. Typically, application layer proxies are a means of providing security to the network entities under it ; it helps to extend the addressing range of its network.



Q 4 a) How is mobility handled in IoT networks?

One of the following three strategies may be to for ensure portability of addresses in the event of node mobility in IoT deployments [2] as shown in Figure 4.12:
(i) **Global Prefix Changes**: Figure 4.12(a) abstracts the addressing strategy using global prefix changes. A node from the left LAN moves to the LAN on the right. The node undergoing movement is highlighted in the figure. The nodes in the first LAN have the prefix **A**, which changes to **B** under the domain of the new gateway overseeing the operation of nodes in the new LAN. However, it may happen that due to movement, the device identifier may face clashes. Recall the structure of the IPv6 address (Figure 4.10). The device identifier, if allotted randomly, might face an address clash upon the node's arrival into the new LAN as there may already be a similar node identifier present in it. Typically, addresses are assigned using DHCPv6/ SLAAC; however, in this scenario, it is always prudent to have static node IP addresses to avoid a clash of addresses. This strategy is, in most cases, beneficial as the IoT nodes may be resourceconstrained

and have low-processing resources due to which it may not be able
to handle protocols such as DHCPv6 or SLAAC.

(ii) **Prefix Changes within WANs**: Figure 4.12(b) abstracts the addressing strategy for prefix changes within WANs. In case the WAN changes its global prefix, the network entities underneath it must be resilient to change and function normally. The address allocation is hence delegated to entities such as gateways and proxies, which make use of ULAs to manage the network within the WAN.

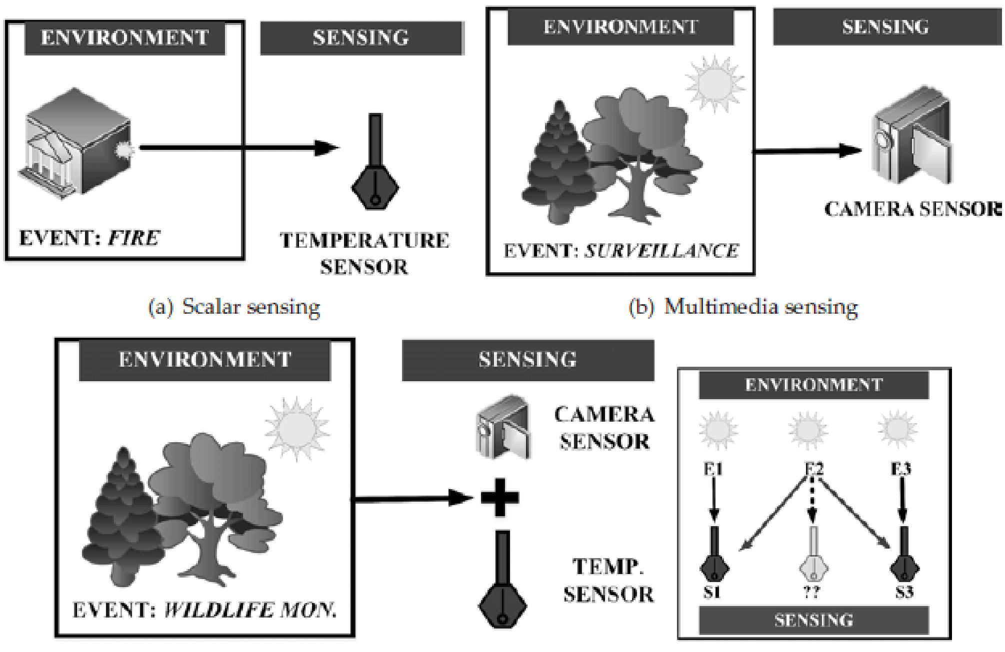
(iii) **Remote Anchoring**: Figure 4.12(c) abstracts the addressing strategy using a remote anchoring point. This is applicable in certain cases which require that the IoT node's global addresses are maintained and not affected by its mobility or even the change in network prefixes. Although a bit expensive to implement, this strategy of having a remote anchoring point from which the IoT nodes obtain their global addresses through tunneling ensures that the nodes are resilient to changes and are quite stable. Even if the node's original network's (LAN) prefix changes from **A** to **B**, the node's global address remains immune to this change.

Q 4 b) Explain different Sensing Types

Sensing can be broadly divided into four different categories based on the nature of the environment being sensed and the physical sensors being used to do so (Figure 5.4): 1) scalar sensing, 2) multimedia sensing, 3) hybrid sensing, and 4) virtual sensing—[2].

5.5.1 Scalar sensing

Scalar sensing encompasses the sensing of features that can be quantified simply by measuring changes in the amplitude of the measured values with respect to time [3]. Quantities such as ambient temperature, current, atmospheric pressure, rainfall, light, humidity, flux, and others are considered as scalar values as they normally do not have a directional or spatial property assigned with them. Simply measuring the changes in their values with passing time provides enough information about these quantities. The sensors used for measuring these scalar quantities are referred to as scalar sensors, and the act is known as scalar sensing. Figures 5.3(b), 5.3(d), 5.3(e), 5.3(f), 5.3(g), 5.3(h), 5.3(i), and 5.3(j) show scalar sensors. A simple scalar temperature sensing of a fire detection event is shown in Figure 5.4(a).



(a) Scalar sensing (b) Multimedia sensing

(c) Hybrid sensing (d) Virtual sensing

5.5.2 Multimedia sensing

Multimedia sensing encompasses the sensing of features that have a spatial variance property associated with the property of temporal variance [4]. 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. Additionally, these quantities follow the vector law of addition and hence are designated as vector quantities. They might have different values in different directions for the same working condition at the same time. The sensors used for measuring these quantities are known as vector sensors. Figures 5.3(a) and 5.3(c) are vector sensors. A simple camera-based multimedia sensing using surveillance as an example is shown in Figure 5.4(b).

5.5.3 Hybrid sensing

The act of using scalar as well as multimedia sensing at the same time is referred to as hybrid sensing. Many a time, there is a need to measure certain vector as well as scalar properties of an environment at the same time. Under these conditions, a range of various sensors are employed (from the collection of scalar as well as multimedia sensors) to measure the various properties of that environment at any instant of time, and temporally map the collected information to generate new information.

For example, in an agricultural field, it is required to measure the soil conditions at regular intervals of time to determine plant health. Sensors such as soil moisture and soil temperature are deployed underground to estimate the soil's water retention capacity and the moisture being held by the soil at any instant of time. However, this setup only determines whether the plant is getting enough water or not. There may be a host of other factors besides water availability, which may affect a plant's health. The additional inclusion of a camera sensor with the plant may be able to determine the actual condition of a plant by additionally determining the color of leaves. The aggregate information from soil moisture, soil temperature, and the camera sensor will be able to collectively determine a plant's health at any instant of time. Other common examples of hybrid sensing include smart parking systems, traffic management systems, and others. Figure 5.4(c) shows an example of hybrid sensing, where a camera and a temperature sensor are collectively used to detect and confirm forest fires during wildlife monitoring.

5.5.4 Virtual sensing

Many a time, there is a need for very dense and large-scale deployment of sensor nodes spread over a large area for monitoring of parameters. One such domain is agriculture [5]. Here, often, the parameters being measured, such as soil moisture, soil temperature, and water level, do not show significant spatial variations. Hence, if sensors are deployed in the fields of farmer **A**, it is highly likely that the measurements from his sensors will be able to provide almost concise measurements of his neighbor **B**'s fields; this is especially true of fields which are immediately surrounding **A**'s fields. Exploiting this property, if the data from **A**'s field is digitized using an IoT infrastructure and this system advises him regarding the appropriate watering, fertilizer, and pesticide regimen for his crops, this advisory can also be used by **B** for maintaining his crops. In short, **A** 's sensors are being used for actual measurement of parameters; whereas virtual data (which does not have actual physical sensors but uses extrapolation-based measurements) is being used for advising **B**. This is the virtual sensing paradigm. Figure 5.4(d) shows an example of virtual sensing. Two temperature sensors S1 and S3 monitor three nearby events E1, E2, and E3 (fires). The event E2 does not have a dedicated sensor for monitoring it; however, through the superposition of readings from sensors S1 and S3, the presence of fire in E2 is inferred.

Q 5) Explain in detail different types of Sensors with example

The various sensors can be classified based on: 1) power requirements, 2) sensor output, and 3) property to be measured.

• **Power Requirements**: The way sensors operate decides the power requirements that must be provided for an IoT implementation. Some sensors need to be provided with separate power sources for them to function, whereas some sensors do not require any power sources. Depending on the requirements of power, sensors can be of two types.

(i) Active: Active sensors do not require an external circuitry or mechanism to provide it with power. It directly responds to the external stimuli from its ambient environment and converts it into an output signal. For example, a photodiode converts light into electrical impulses.

(ii) Passive: Passive sensors require an external mechanism to power them up. The sensed properties are modulated with the sensor's inherent characteristics to generate patterns in the output of the sensor. For example, a thermistor's resistance can be detected by applying voltage difference across it or passing a current through it.

• **Output**: The output of a sensor helps in deciding the additional components to be integrated with an IoT node or system. Typically, almost all modern-day processors are digital; digital sensors can be directly integrated to the processors. However, the integration of analog sensors to these digital processors or IoT nodes requires additional interfacing mechanisms such as analog to digital converters (ADC), voltage level converters, and others. Sensors are broadly divided into two types, depending on the type of output generated from these sensors, as follows.

(i) Analog: Analog sensors generate an output signal or voltage, which is proportional (linearly or non-linearly) to the quantity being measured and is continuous in time and amplitude. Physical quantities such as temperature, speed, pressure, displacement, strain, and others are all continuous and categorized as analog quantities. For example, a thermometer or a thermocouple can be used for measuring the temperature of a liquid (e.g., in household water heaters). These sensors continuously respond to changes in the temperature of the liquid.

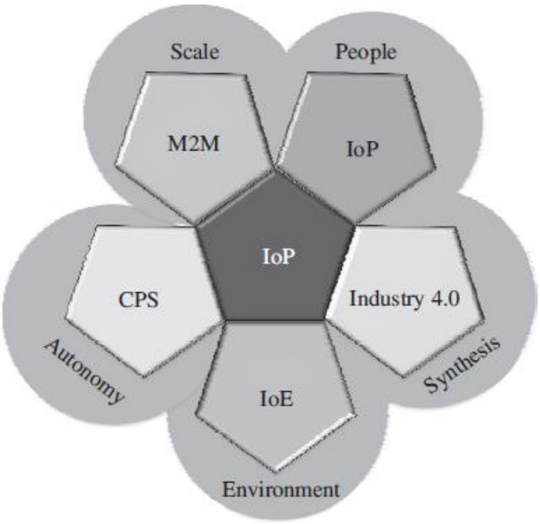
(ii) Digital: These sensors generate the output of discrete time digital representation (time, or amplitude, or both) of a quantity being measured, in the form of output signals or voltages. Typically, binary output signals in the form of a logic **1** or a logic **0** for **ON** or **OFF**, respectively are associated with digital sensors. The generated discrete (non-continuous) values may be output as a single "bit" (serial transmission), eight of which combine to produce a single "byte" output (parallel transmission) in digital sensors.

• **Measured Property**: The property of the environment being measured by the sensors can be crucial in deciding the number of sensors in an IoT implementation. Some properties to be measured do not show high spatial variations and can be quantified only based on temporal variations in the measured property, such as ambient temperature, atmospheric pressure, and others. Whereas some properties to be measured show high spatial as well as temporal variations such as sound, image, and others. Depending on the properties to be measured, sensors can be of two types.

(i) Scalar: Scalar sensors produce an output proportional to the magnitude of the quantity being measured. The output is in the form of a signal or voltage. Scalar physical quantities are those where only the magnitude of the signal is sufficient for describing or characterizing the phenomenon and information generation. Examples of such measurable physical quantities include color, pressure, temperature, strain, and others. A thermometer or thermocouple is an example of a scalar sensor that has the ability to detect changes in ambient or object temperatures (depending on the sensor's configuration). Factors such as changes in sensor orientation or direction do not affect these sensors (typically).

(ii) Vector: Vector sensors are affected by the magnitude as well as the direction and/or orientation of the property they are measuring. Physical quantities such as velocity and images that require additional information besides their magnitude for completely categorizing a physical phenomenon are categorized as vector quantities. Measuring such quantities are undertaken using vector sensors. For example, an electronic gyroscope, which is commonly found in all modern aircraft, is used for detecting the changes in orientation of the gyroscope with respect to the Earth's orientation along all three axes

Q 6) Discuss different interdependencies used in IoT



M2M: The M2M or the machine-to-machine paradigm signifies a system of connected machines and devices, which can talk amongst themselves without human intervention. The communication between the machines can be for updates on machine status (stocks, health, power status, and others), collaborative task completion, overall knowledge of the systems and the environment, and others.

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

IoE: The IoE paradigm is mainly concerned with minimizing and even reversing the ill-effects of the permeation of Internet-based technologies on the environment [3]. The major focus areas of this paradigm include smart and sustainable farming, sustainable and energy-efficient habitats, enhancing the energy efficiency of systems and processes, and others. In brief, we can safely assume that any aspect of IoT that concerns and affects the environment, falls under the purview of IoE.

(iv) **Industry 4.0**: Industry 4.0 is commonly referred to as the fourth industrial revolution pertaining to digitization in the manufacturing industry. The previous revolutions chronologically dealt with mechanization, mass production, and the industrial revolution, respectively. This paradigm strongly puts forward the concept of smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT. The digitization and connectedness in Industry 4.0 translate to better resource and workforce management, optimization of production time and resources, and better upkeep and lifetimes of industrial systems.

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