UNIT-1

INTERNET OF THINGS

1.1 What is the Internet of Things? :

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy, and economic benefit.

“Thing” in the Internet of Things

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object.

These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

Examples

- Smart refrigerators
- Smart watches,
- Smart fire alarm
- Smart door lock
- Smart bicycle
- Medical sensors
- Fitness trackers
- Smart security system etc.

1.1.1 IoT – Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below −

- **AI** − IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favourite cereal run low, and to then place an order with your preferred grocer.

- **Connectivity** − New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.
- **Sensors** − IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
- **Active Engagement** − Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.
- **Small Devices** − Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

1.1.2 Evolution of Internet of Things (IoT)/ History of IoT

Let us have a look at how the evolution of IoT as a concept happened over a period of time along with the timelines:

Year 1999: Kevin Ashton, co-founder of the Auto-ID (for Automatic Identification) Center at MIT coined the term "Internet of things ". His definition of IoT was based on reinventing RFID as a networking technology by linking objects to the internet using the RFID tag.

Year 1999: Device to Device (D2D) communication as a concept was coined by Bill Joy as part of his "Six Webs" framework at the World Economic Forum.

Year 2000: LG Internet Digital DIOS, the first Internet-connected refrigerator in the world was invented. The refrigerator used a LAN port for IP connectivity.

Year 2001: David Brock, co-director at the Auto-ID Centre, MIT, proposed a new object identification scheme, the Electronic Product Code (EPC), instead of the conventional Universal Product Code (UPC or 'bar code') for unique identification and tracking of objects throughout the product life cycle using the infrastructure/internet."

Year 2003: The "Project JXTA-C: Enabling a Web of Things" is published by Bernard Traversat and team at the 36th Annual Hawaii International Conference.

According to them, the Project JXTA's aim is to specify a standard set of protocols for ad hoc, pervasive, peer-to-peer computing as a foundation of the upcoming Web of Things.

Year 2003: A special kind of network to connect many of the millions of tags that are already in the world was launched at the McCormick Place conference centre.

The launch of electronic product code (EPC) network was attended by numerous delegates from across the worlds of retail, technology and academia.

Year 2005: The faculty at the Interaction Design Institute Ivrea (IDII), Italy, invents a single-board microcontroller to be used in interactive projects being developed their students.

Year 2008: Different industry stakeholders come together to form the IPSO Alliance to promote connected devices. This was a big leap towards having the IoT implemented for large scale business in real production setups.

2016 and Beyond: We have connected home, connected cars, IoT enabled manufacturing plants, and IoT based solar trackers.

Year 2018: As of 2018, nearly half of all IoT (Internet of Things) devices were connected to WPAN (Wireless Personal Area Networks), including Zigbee, Bluetooth, and Z-wave.

Year 2019: By 2019, the global IoT market will generate a revenue of $1.7T.

Year 2020: Of the 21.7 billion active connected devices worldwide, 11.7 billion (or 54%) will be IoT device connections at the end of 2020.

"By 2025, it is expected that there will be more than 30 billion IoT connections, almost 4 IoT devices per person on average."

1.1.3 IoT − Advantages

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer −

- **Improved Customer Engagement** − Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
- **Technology Optimization** − The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

- **Reduced Waste** − IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- **Enhanced Data Collection** − Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyse our world. It allows an accurate picture of everything.
- **Efficient resource utilization:** If we know the functionality and the way that how each device work, we definitely increase the efficient resource utilization as well as monitor natural resources.
- **Minimize human effort:** As the devices of IoT interact and communicate with each other and do lot of task for us, then they minimize the human effort.
- **Save time:** As it reduces the human effort then it definitely saves out time. Time is the primary factor which can save through IoT platform.

1.1.4 IoT − Disadvantages

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues −

- **Security** − IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
- **Privacy** − The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
- **Complexity** − Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.
- **Flexibility** − Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- **Compliance** − IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

1.2 Sensors, their types and features

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules, and sensing modules. RF modules manage communications through their signal processing, WiFi, ZigBee, Bluetooth, radio transceiver, duplexer, and BAW.

The sensing module manages sensing through assorted active and passive measurement devices. Here is a list of some of the measurement devices used in IoT –

Table 1.1 Types of Sensors

S. No	Devices	Type of Sensors
1.	accelerometers	temperature sensors
2.	magnetometers	proximity sensors
3.	gyroscopes	image sensors
4.	acoustic sensors	light sensors
5.	pressure sensors	gas RFID sensors
6.	humidity sensors	micro flow sensors

1.2.1 Types of Sensors used in IoT

Temperature sensors

By definition, "A device, used to measure amount of heat energy that allows to detect a physical change in temperature from a particular source and converts the data for a device or user, is known as a Temperature Sensor."

These sensors have been deployed for a long time in a variety of devices. However, with the emergence of IoT, they have found more room to be present in an even greater number of devices. Only a couple of years ago, their uses mostly included A/C control, refrigerators and similar devices used for environmental control. However, with the advent of the IoT world, they have found their role in manufacturing processes, agriculture and health industry.

In the manufacturing process, many machines require specific environment temperature, as well as device temperature. With this kind of measurement, the manufacturing process can always remain optimal.

On the other hand, in agriculture, the temperature of soil is crucial for crop growth. This helps with the production of plants, maximizing the output.

Proximity sensor

A device that detects the presence or absence of a nearby object, or properties of that object, and converts it into signal which can be easily read by user or a simple electronic instrument without getting in contact with them.

Proximity sensors are largely used in the retail industry, as they can detect motion and the correlation between the customer and product they might be interested in. A user is immediately notified of discounts and special offers of nearby products.

Another big and quite an old use-case is vehicles. You are reversing your car and are alrmed about an obstacle while taking reverse, that's the work of proximity sensor.

They are also used for parking availability in places such as malls, stadiums or airports.

Pressure sensor

A pressure sensor is a device that senses pressure and converts it into an electric signal. Here, the amount depends upon the level of pressure applied.

Deployment of these sensors is not only very useful in manufacturing, but also in the maintenance of whole water systems and heating systems, as it is easy to detect any fluctuation or drops in pressure.

Water quality sensor

Water quality sensors are used to detect the water quality and Ion monitoring primarily in water distribution systems.

Water is practically used everywhere. These sensors play an important role as they monitor the quality of water for different purposes. They are used in a variety of industries.

Chemical sensor

Chemical sensors are applied in a number of different industries. Their goal is to indicate changes in liquid or to find out air chemical changes. They play an important role in bigger cities, where it is necessary to track changes and protect the population.

Main use cases of chemical sensors can be found in Industrial environmental monitoring and process control, intentionally or accidentally released harmful chemical detection, explosive and radioactive detection, recycling processes on Space Station, pharma industries and laboratory etc.

Gas sensor

Gas sensors are similar to the chemical ones, but are specifically used to monitor changes of the air quality and detect the presence of various gases. Like chemical sensors, they are used in numerous industries such as manufacturing, agriculture and health and used for air quality monitoring, detection of toxic or combustible gas, hazardous gas monitoring in coal mines, oil & gas industries, chemical laboratory research, manufacturing – paints, plastics, rubber, pharmaceutical & petrochemical etc.

Following are some common Gas sensors:

- Carbon dioxide sensor
- Breathalyzer
- Carbon monoxide detector
- Catalytic bead sensor
- Hydrogen sensor
- Air pollution sensor
- Nitrogen oxide sensor
- Oxygen sensor
- Ozone monitor
- Electrochemical gas sensor
- Gas detector
- Hygrometer

Smoke sensor

A smoke sensor is a device that senses smoke (airborne particulates & gases), and it's level. Smoke sensors are extensively used by manufacturing industry, HVAC, buildings and accommodation infra to detect fire and gas incidences. This serves to protect people working in dangerous environments, as the whole system is much more effective in comparison to the older ones.

Common Type of Smoke Sensors

Smoke sensors detect the presence of Smoke, Gases and Flame surrounding their field. It can be detected either optically or by the physical process or by the use of both the methods.

- Optical smoke sensor (Photoelectric): Optical smoke sensor used the light scatter principle trigger to occupants.

- Ionization smoke sensor: Ionization smoke sensor works on the principle of ionization, kind of chemistry to detect molecules causing a trigger alarm.

IR sensors

An infrared sensor is a sensor which is used to sense certain characteristics of its surroundings by either emitting or detecting infrared radiation. It is also capable of measuring the heat being emitted by the objects.

Other common use includes home appliances & remote control, breath analysis, Infrared vision (i.e. visualize heat leaks in electronics, monitor blood flow, art historians to see under layers of paint), wearable electronics, optical communication, non-contact based temperature measurements, automotive blind-angle detection.

Their usage does not end there, they are also a great tool for ensuring high-level security in your home. Also, their application includes environment checks, as they can detect a variety of chemicals and heat leaks. They are going to play an important role in the smart home industry, as they have a wide-range of applications.

Level sensors

A sensor which is used to determine the level or amount of fluids, liquids or other substances that flow in an open or closed system is called Level sensor.

Best use cases of level sensor is, fuel gauging & liquid levels in open or closed containers, sea level monitoring & Tsunami warning, water reservoirs, medical equipment, compressors, hydraulic reservoirs, machine tools, beverage and pharmaceutical processing, high or low-level detection etc.

This helps better streamline their businesses, as sensors collect all the important data at all times. With the use of these sensors, any product manager can precisely see how much liquid is ready to be distributed and whether the manufacturing should be stepped up.

Image sensors

Image sensors are instruments which are used to convert optical images into electronic signals for displaying or storing files electronically.

The major use of image sensor is found in digital camera & modules, medical imaging and night vision equipment,thermal imaging devices, radar, sonar, media house, Biometric & IRIS devices.

Motion detection sensors

A motion detector is an electronic device which is used to detect the physical movement (motion) in a given area and it transforms motion into an electric signal; motion of any object or motion of human beings

Motion detection plays an important role in the security industry. Businesses utilize these sensors in areas where no movement should be always detected, and it is easy to notice anybody's presence with these sensors installed.

These are primarily used for intrusion detection systems, automatics door control, boom barrier, smart camera (i.e motion based capture/video recording), toll plaza, automatic parking systems, automated sinks/toilet flusher, hand dryers, energy management systems(i.e. Automated Lighting, AC, Fan, Appliances Control) etc.

Accelerometer sensors

Accelerometer is a transducer that is used to measure the physical or measurable acceleration experienced by an object due to inertial forces and converts the mechanical motion into an electrical output. It is defined as rate of change of velocity with respect to time

These sensors are now present in millions of devices, such as smartphones. Their uses involve detection of vibrations, tilting and acceleration in general. This is great for monitoring your driving fleet, or using a smart pedometer.

Gyroscope sensors

A sensor or device which is used to measure the angular rate or angular velocity is known as Gyro sensors, Angular velocity is simply defined as a measurement of speed of rotation around an axis. It is a device used primarily for navigation and measurement of angular and rotational velocity in 3-axis directions. The most important application is monitoring the orientation of an object.

Their main applications are in car navigation systems, game controllers, cellular & camera devices, consumer electronics, robotics control, drone & RC control helicopter or UAV control, vehicle control/ADAS and many more.

There are several different kinds of gyro sensors which are selected by their working mechanism, output type, power, sensing range and environmental conditions.

- Rotary (classical) gyroscopes
- Vibrating Structure Gyroscope
- Optical Gyroscopes
- MEMS(micro-electro-mechanical systems) Gyroscopes

These sensors are always combined with accelerometers. The use of these two sensors simply provides more feedback to the system. With gyroscopic sensors installed, many devices can help athletes improve the efficiency of their movements, as they gain access to the athletes movement during sports activities.

This is only one example of its application, however, as the role of this sensor is to detect rotation or twist, its application is crucial for the automation of some manufacturing processes.

Humidity sensors

Humidity is defined as the amount of water vapour in an atmosphere of air or other gases. The most commonly used terms are “Relative Humidity (RH)

These sensors usually follow the use of temperature sensors, as many manufacturing processes require perfect working conditions. Through measuring humidity, you can ensure that the whole process runs smoothly, and when there is any sudden change, action can be taken immediately, as sensors detect the change almost instantaneously.

Their applications and use can be found in Industrial & residential domain for heating, ventilating, and air conditioning systems control. They can also be found in Automotive, museums, industrial spaces and greenhouses , meteorology stations,Paint and coatings industries, hospitals & pharma industries to protect medicines

Optical sensors

A sensor which measures the physical quantity of light rays and convert it into electrical signal which can be easily readable by user or an electronic instrument/device is called optical sensor.

Optical sensors are loved by IoT experts, as they are practical for measuring different things simultaneously. The technology behind this sensor allows it to monitor electromagnetic energy, which includes, electricity, light and so on.

Due to this fact, these sensors have found use in healthcare, environment monitoring, energy, aerospace and many more industries. With their presence oil companies, pharmaceutical companies and mining companies are in a much better position to track environmental changes while keeping their employees safe.T

Their main use can be found in ambient light detection, digital optical switches, optical fibres communications,due to electrical isolation best suited for oil and gas applications, civil and transportation fields, high speed network systems, elevator door control, assembly line part counters and safety systems.

1.3 IoT components: layers

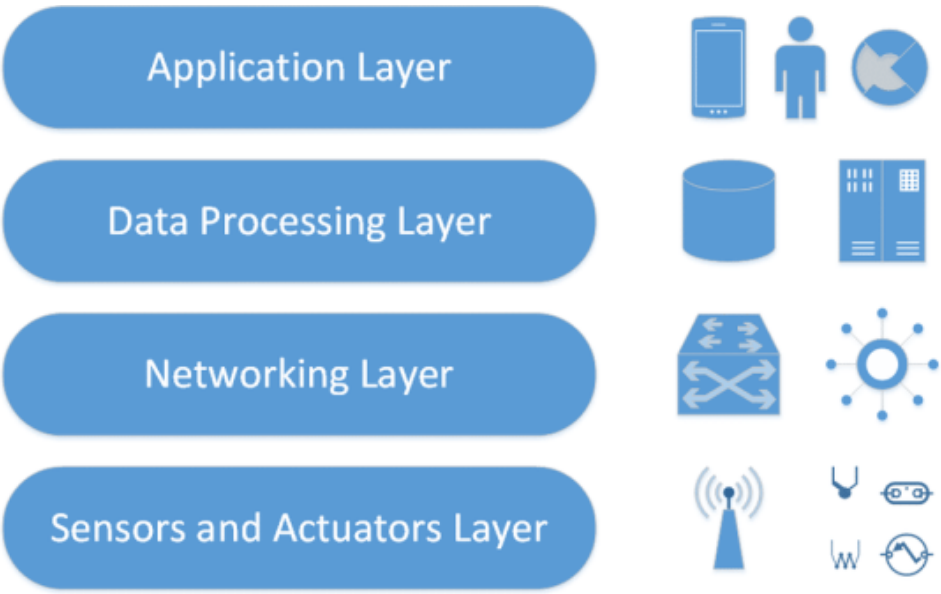

Fig 1.1 IoT Components

Application Layer

The application layer defines all applications in which IoT has deployed. It is the interface between the end IoT devices and the network. IoT Applications such as smart homes, smart health, smart cities, etc. It has the authority to provide services to the applications. The services may be different for each application because of services based on the information collected by sensors.

It is applied through a dedicated application at the device end. Such as for a computer, the application layer is applied by the browser. It is the browser that executes application layer protocols like HTTP, HTTPS, SMTP, and FTP. There are many concerns in the application layer out of which security is the key issue.

Common issues and threats of application layers are:

Cross-site scripting:

It is a type of computer security infirmities that typically found in web applications. It enables attackers to inject client-side scripts such as JavaScript into web pages viewed by other users. By doing so, an attacker can completely change the contents of the application as per his needs and use original information in an illegal way.

Malicious Code Attack:

It is a particular code in any part of the software system or script that is considered to cause undesired effects, security threats or damage to the system. It is that threat that may not be blocked or controlled by the use of anti-virus software.

Data Processing Layer

In three-layer architecture, the data were directly sent to the network layer. Due to sending data directly the chances of getting damages increase. In four-layer architecture, data is sent to this layer

that is obtained from a perception layer. Data Processing Layer has two responsibilities it confirms that data is forwarded by the authentic users and prevented from threats.

Authentication is the most commonly used method to verify the users and the data. It is applied by using pre-shared, keys and passwords to the concerned user. The second responsibility of the layer is to send information to the network layer. The medium through which data is transferred from the Data Processing Layer to the network layer can be wireless and wire-based.

Common issues and threats of the Data Processing layer are:

DoS Attack:

An attacker sends a huge amount of data to make network traffic overloaded. Thus, the huge consumption of system resources exhausts the IoT and makes the user unable to access the system.

Malicious Insider Attack:

It comes from the inside of an IoT environment to access private information. It is conducted by an authorized user to access the information of another user.

Network Layer

This layer is also known as a transmission layer. It acts like a bridge that carries and transmits data gathered from physical objects through sensors. The medium can be wireless or wire-based. It also connects the network devices and networks to each other. Hence, it is extremely sensitive to attacks from the attackers. It has important security issues regarding integrity and authentication of data that is being transmitted to the network.

Common issues and threats of the Network layer are:

Main-in-The-Middle Attack:

MiTM attack is an attack where the attacker privately intercepts and modifies the communication between the sender and receiver who assume they are directly communicating with each other. It leads to a serious threat to online security because they give the attacker the pathway to capture and control data in real-time

Storage Attack:

The crucial information of users is saved on storage devices or on the cloud. Both the storage devices and the cloud can be attacked by the attacker and the user's information may be modified to incorrect details.

By making regular backups of files, by running anti-virus software and using a system with strong passwords so that data access is restricted are the ways by which we can protect data from the attacker.

Exploit Attack:

An exploit is any unethical or illegal attack in a form of software, blocks of data or a sequence of commands. It takes benefit of security infirmities in an application, system or hardware. It usually occurs with the goal of getting control of the system and steals information stored on the network. By installing all software patches, security releases and all updates for your software are few preventive measures against attack.

Perception layer/Sensor layer

The sensor layer has the responsibility to recognize things and gather the data from them. There are many types of sensors connected to the objects to gather information such as RFID, sensors and 2-D barcode. The sensors are selected as per the requirement of applications. The data that is collected by these sensors can be about location, changes in the air, environment, etc. However, they are the main aim of attackers who wish to use them to replace the sensor with their own.

Hence, most of the threats are related to sensors are

Eavesdropping:

It is an unauthorized real-time attack where personal communications, such as phone calls, fax transmissions, text messages are intercepted by an attacker. It tries to take crucial information that is transferred over a network. Preventive measures such as Access control, continuous supervision/observation of all devices, thorough inspection by a qualified technical countermeasures specialist of all components need to be ensured.

Replay Attack:

It is also known as a playback attack. It is an attack in which an attacker intrudes on the conversation between the sender and receiver and extracts authentic information from the sender. The added risk of replay attacks is that a hacker doesn't even need improved skills to decrypt a message after seizing it from the network.

Timing Attack:

It is usually utilized in devices that have weak computing abilities. It allows an attacker to find vulnerabilities and withdraw secrets maintained in the security of a system by observing how long it takes the system to respond to various queries, input or other algorithms.

1.4 Smart City:

A **smart city** is an urban area that uses different types of electronic methods and sensors to collect data. It is a framework, predominantly composed of Information and Communication Technologies

(ICT), to develop, deploy, and promote sustainable development practices to address growing urbanization challenges. A big part of this ICT framework is essentially an intelligent network of connected objects and machines that transmit data using wireless technology and the cloud.

Cloud-based IoT applications receive, analyze, and manage data in real-time to help municipalities, enterprises, and citizens make better decisions that improve quality of life. Citizens engage with smart city ecosystems in various ways using smartphones and mobile devices and connected cars and homes. Pairing devices and data with a city's physical infrastructure and services can cut costs and improve sustainability.

The first question is what is meant by a 'smart city'. The answer is, there is no universally accepted definition of a smart city. It means different things to different people. The conceptualization of Smart City, therefore, varies from city to city and country to country, depending on the level of development, willingness to change and reform, resources and aspirations of the city residents. A smart city would have a different connotation in India than, say, Europe. Even in India, there is no one way of defining a smart city.

Some definitional boundaries are required to guide cities in the Mission. In the imagination of any city dweller in India, the picture of a smart city contains a wish list of infrastructure and services that describes his or her level of aspiration. To provide for the aspirations and needs of the citizens, urban planners ideally aim at developing the entire urban eco-system, which is represented by the four pillars of comprehensive development-institutional, physical, social and economic infrastructure. This can be a long term goal and cities can work towards developing such comprehensive infrastructure incrementally, adding on layers of 'smartness'.

In the approach of the Smart Cities Mission, the objective is to promote cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart' Solutions. The focus is on sustainable and inclusive development and the idea is to look at compact areas, create a replicable model which will act like a light house to other aspiring cities. The Smart Cities Mission of the Government is a bold, new initiative. It is meant to set examples that can be replicated both within and outside the Smart City, catalyzing the creation of similar Smart Cities in various regions and parts of the country.

The core infrastructure elements in a smart city would include:

- adequate water supply,
- assured electricity supply,
- sanitation, including solid waste management,
- efficient urban mobility and public transport,
- affordable housing, especially for the poor,

- robust IT connectivity and digitalization,
- good governance, especially e-Governance and citizen participation,
- sustainable environment,
- safety and security of citizens, particularly women, children and the elderly, and
- health and education.

As far as Smart Solutions are concerned, an illustrative list is given below. This is not, however, an exhaustive list, and cities are free to add more applications.

Fig 1.2 Smart solutions within smart cities

Accordingly, the purpose of the Smart Cities Mission is to drive economic growth and improve the quality of life of people by enabling local area development and harnessing technology, especially technology that leads to Smart outcomes. Areabased development will transform existing areas (retrofit and redevelop), including slums, into better planned ones, thereby improving liveability of the whole City. New areas (greenfield) will be developed around cities in order to accommodate the expanding population in urban areas. Application of Smart Solutions will enable cities to use technology, information and data to improve infrastructure and services. Comprehensive development in this way will improve quality of life, create employment and enhance incomes for all, especially the poor and the disadvantaged, leading to inclusive Cities.

1.5 Industrial Internet of Things (IIoT)

IIoT stands for the Industrial Internet of Things or Industrial IoT that initially mainly referred to an industrial framework whereby many devices or machines are connected and synchronized through the use of software tools and third platform technologies in a machine-to-machine and Internet of Things context, later an Industry 4.0 or Industrial Internet context.

The industrial internet of things (IIoT) is the use of smart sensors and actuators to enhance manufacturing and industrial processes. Also known as the industrial internet or Industry 4.0, IIoT leverages the power of smart machines and real-time analytics to take advantage of the data that 'dumb machines' have produced in industrial settings for years. The driving philosophy behind IIoT is that smart machines are not only better than humans at capturing and analyzing data in real time, they are better at communicating important information that can be used to drive business decisions faster and more accurately.

Connected sensors and actuators enable companies to pick up on inefficiencies and problems sooner, and save time and money in addition to supporting business intelligence (BI) efforts. In manufacturing specifically, IIoT holds great potential for quality control, sustainable and green practices, supply chain traceability and overall supply chain efficiency. In an industrial setting, IIoT is key to processes such as predictive maintenance (PdM), enhanced field service, energy management and asset tracking.

1.5.1 IIoT versus IoT

Although the internet of things and the industrial internet of things have many technologies in common, including cloud platforms, sensors, connectivity, machine-to-machine communications and data analytics, they are used for different purposes.

IoT applications connect devices across multiple verticals, including agriculture, healthcare, enterprise, consumer and utilities, as well as government and cities. IoT devices include smart appliances, fitness bands and other applications that generally don't create emergency situations if something goes amiss.

IIoT applications, on the other hand, connect machines and devices in such industries as oil and gas, utilities and manufacturing. System failures and downtime in IIoT deployments can result in high-risk situations or even life-threatening situations. IIoT applications are also more concerned with improving efficiency and improving health or safety, versus the user-centric nature of IoT applications.

1.5.2 IIoT applications and examples

In a real-world IIoT deployment of smart robotics, ABB, a power and robotics firm, is using connected sensors to monitor the maintenance needs of its robots to prompt repairs before parts break.

Likewise, commercial jetliner maker Airbus has launched what it calls the "factory of the future," a digital manufacturing initiative to streamline operations and boost production. Airbus has integrated sensors into machines and tools on the shop floor and outfitted employees with wearable tech, e.g., industrial smart glasses, aimed at cutting down on errors and enhancing workplace safety.

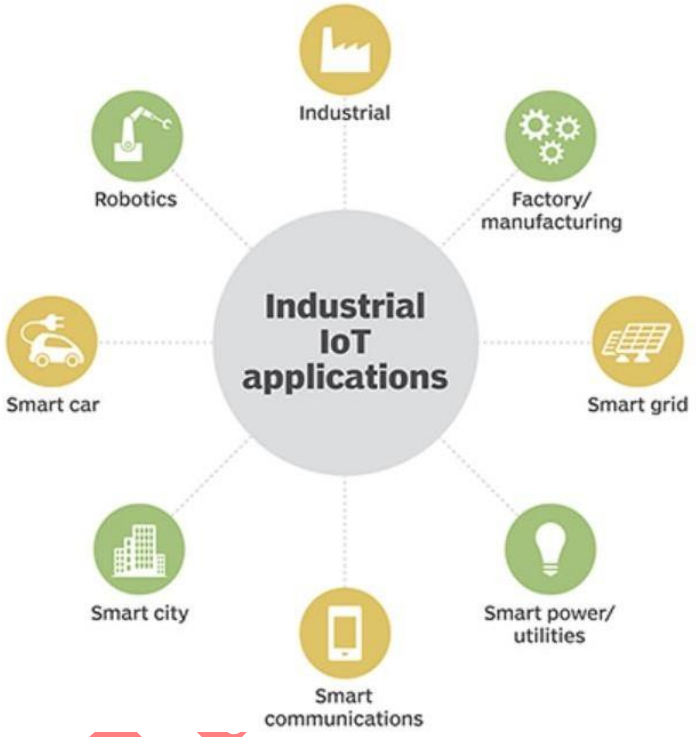

Fig 1.3 IIoT Applications and examples

Questions:

1. What is the Internet of Things (IoT)? Give some examples
2. What are the fundamental components of IoT?
3. What is the difference between IoT and IIoT?
4. List layers of IoT protocol stack
5. What are the advantages and disadvantages of IoT?
6. Define Smart City with some real-life examples.
7. What do you understand by sensors in w.r.t. IoT? Give the various types of sensors.
8. List 10 real life examples where IoT technology is being used