1 INTRODUCTION TO INTERNET OF THINGS

1.1 Introduction

Internet of Things (IoT) is presently a hot technology worldwide. Government, academia and industry are involved in different aspects of research, implementation and business with IoT. IoT cuts across different application domain verticals ranging from civilian to defense sectors. These domains include agriculture, space, healthcare, manufacturing, construction, water and mining, which are presently transitioning their legacy to support IoT. Today it is possible to envision pervasive connectivity, storage and computation, which in turn gives rise to build different IoT solutions. IoT-based applications such as Innovative Shopping System, Infrastructure Management in both urban and rural areas, Remote Health Monitoring & Emergency Notification Systems and Transportation Systems are gradually relying on IoT based systems. Therefore, it is very important to learn the fundamentals of this emerging technology.

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and network connectivity which enables these objects to get connected and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. *Internet of Things can also be defined as an Internet technology connecting devices, machines and tools to the Internet by means of wireless technologies like Bluetooth, WiFi, ZigBee etc.*

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. IoT also results in unification of technologies such as low power embedded systems, cloud computing, big data, machine learning and networking. The two solutions for the networking technologies in IoT are either to expand the existing network or to build a separate network from the scratch. Following Figure 1.1 gives an overview of objects connected to Internet of Things.

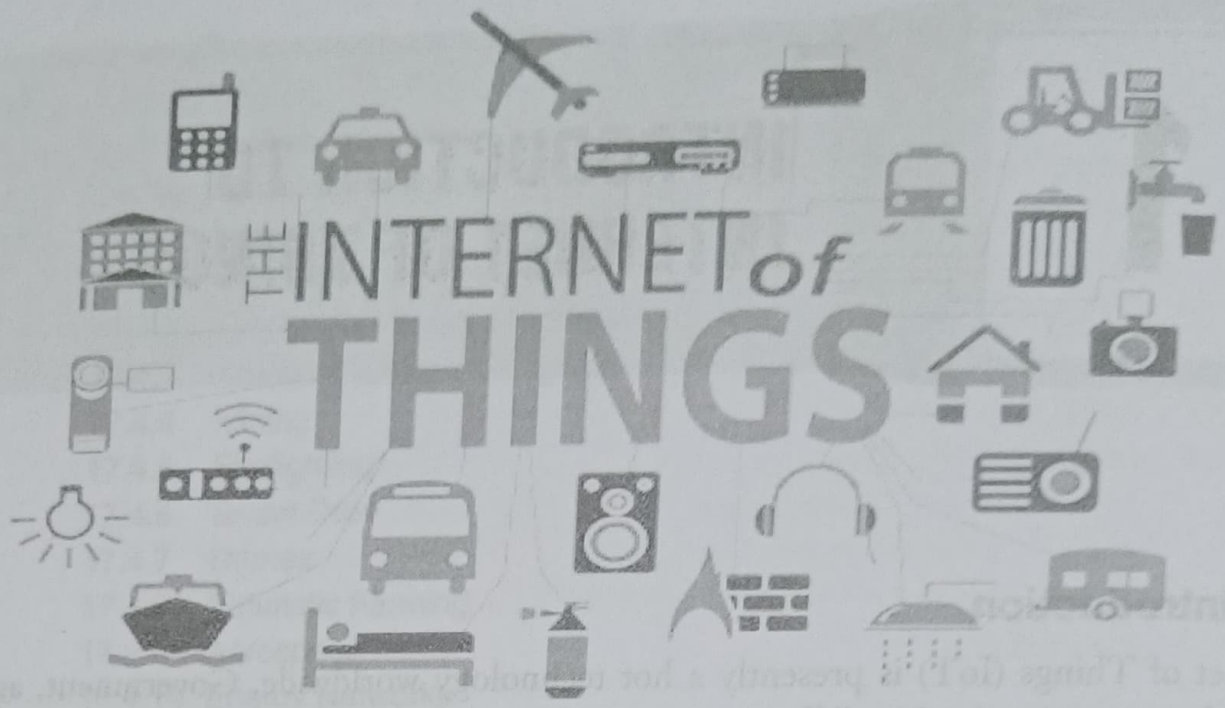

Fig.1.1: Overview of Internet of Things

The concept of the **Internet of Things** became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the Internet of Things at that point. If all objects and people in daily life were equipped with identifiers, computers could manage and store them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking. Other IoT enabling technologies are nanotechnology, sensors and smart networks. Presently we are heading into a new era of ubiquity where the "users" of the Internet will be counted in billions. Humans may become the minority as generators and receivers of traffic. Instead most of the traffic will flow between among devices and all kinds of "things" thereby creating a much wider and more complex Internet of Things.

1.2 Characteristics of IoT

The fundamental characteristics of IoT are as follows.

Interconnectivity: With regards to IoT, anything can be interconnected with the global information and communication infrastructure.

Things related services: IoT is capable of providing "thing" related services within the constraints of things, such as privacy protection and semantic consistency among physical things and their associated virtual things. In order to provide "thing" related services within the constraints of things, both the technologies in physical world and information world will be changed.

Heterogeneity: The devices in the IoT are heterogeneous based on different hardware platforms, applications and networks. They can interact with other devices or service platforms through different networks. IoT may comprise of sleeping nodes, mobile devices and non-IP devices.

Dynamic changes: The state of device change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can be changed dynamically.

Enormous scale: The number of devices that need to be managed and that communicate with one another will be at least in an order of magnitude larger than the devices connected to the current Internet. The management of generated data and their interpretation for application purposes will be more critical. This relates to semantics of data, as well as efficient data handling.

Safety: We gain benefits from IoT, but we must not forget about safety. IoT must be designed with safety in mind. This includes the safety of our personal data and the safety of our physical devices. Securing the endpoints, the networks and the data moving across all of it means creating a security paradigm in IoT.

Connectivity: Connectivity enables network accessibility and compatibility. Accessibility is found on a network while compatibility provides the common ability to consume and produce data. The intermittent connectivity is desirable in IoT as when the device is no longer in use, the connection can be detached whereas the device needs to be connected when it wants to generate, transfer or receive data.

Naming and Addressing: The names and addresses of devices connected to Internet of Things should be unique. Efficient and unambiguous addressing mechanisms should be deployed for devices connected in IoT. Moreover the conversion and translation of addresses from one network to the other should take place efficiently.

1.3 Applications of IoT

The applications of IoT are found in almost all domains of life. It includes business, manufacturing, healthcare, retail, security, transport and other domains. The applications of IoT in key areas are explained in the following description.

Smart Home: In this concept, it is possible to switch on air conditioning before reaching home or switch off lights even after we have left home. Similarly we can unlock the doors to friends for temporary access even when we are not at home. Thus IoT is building products to make our life simpler and convenient. Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart Homes will become as common as smart phones. The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money. With Smart Home companies like Nest, Ecobee, Ring and August, to name a few, will become household brands and are planning to deliver a unique experience.

Wearables: Wearables have experienced an explosive demand in markets all over the world. Companies like Google, Samsung, etc. have invested heavily in building such devices. Wearable devices are installed with sensors and software which collect data and information about the users. This data is later pre-processed to extract essential insights about user. These devices broadly cover fitness, health and entertainment requirements. The pre-requisite for Internet of Things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized.

Connected Cars/Smart Cars: The automotive digital technology has focused on optimizing vehicle's internal functions. But now, this attention is growing towards enhancing the in-car experience. A connected car is a vehicle which is able to optimize it's own operation, maintenance as well as comfort of passengers using onboard sensors and Internet connectivity is ensured. Similarly a smart car can identify the behavior of another car coming in its opposite direction. For example, if a car coming in opposite direction switches on the indicator to the left, our car understands it and takes action accordingly. Most of the large automobile manufacturers as well as some brave startups are working on connected car and smart car solutions. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.

Smart Industry: Smart Industry is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and big data analytic to create brilliant machines. The driving philosophy behind IIoT is that, smart machines are more accurate and consistent than humans in communicating through data. This data can help companies in picking up inefficiencies and problems sooner. IIoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency.

Smart Cities: Smart City is another powerful application of IoT generating curiosity among world's population. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring are examples of Internet of Things applications for Smart Cities. IoT will solve major problems faced by the people living in cities of pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart Belly trash will send alerts to municipal services when a bin needs to be emptied. By installing sensors and using web applications, citizens can find free available parking slots across the city. Also, the sensors can detect meter tampering issues, general malfunctions and any installation issues in the electricity system.

Smart Agriculture: With the continuous increment in world's population, demand for food supply is extremely raised. Governments are helping farmers to use advanced techniques and researches to increase food production. Smart farming is one of the fastest growing fields in IoT. Farmers are using meaningful insights from the data to yield better return on

investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple usages of IoT.

Smart Retail: The potential of IoT in the retail sector is enormous. IoT provides an opportunity to retailers to get connected with the customers to enhance the in-store experience. Smart phones will be the way for retailers to remain connected with their consumers even out of store. Interacting through Smart phones and using beacon technology can help retailers serve their consumers in a better manner. They can also track consumer's path through a store and improve store layout and place premium products in high traffic areas.

Energy Management: Power grids of the future will not only be smart enough but also highly reliable. Smart Grid concept is becoming very popular all over the world. The basic idea behind the smart grids is to collect data in an automated fashion and analyze the behavior of electricity consumers and suppliers for improving efficiency as well as economics of electricity usage. Smart Grids will also be able to detect sources of power outages more quickly and at individual household levels like nearby solar panel, making possible distributed energy system.

Smart Healthcare: Connected healthcare yet remains the sleeping giant of the Internet of Things applications. The concept of connected healthcare system and smart medical devices bear enormous potential not just for companies, but also for the well-being of people in general.

Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness. In smart healthcare, devices are connected to hospitals, doctors and relatives to alert them of medical emergencies and take preventive or necessary measures.

Smart Poultry and Farming: Livestock monitoring is about animal husbandry and cost saving. Using IoT applications to gather data about the health and well being of the cattle, ranchers know early about the sick animal which can be pulled out and help prevent large number of sick cattle. With the help of collected data, ranchers can increase the poultry production.

Smart Dust: This consists of sensors at the nanotechnology level that can be deployed in the millions to billions, with a myriad of applications. They are computers smaller than a grain of sand and can be sprayed or injected almost anywhere to measure chemicals in the soil or to diagnose problems in human body. These devices are the wave of the future for anything from global weather management and smart city monitoring to war theater mapping and internal medicine. They are a single package with sensing, computation, communication and power to collect data and report it back to home base.

Other applications of IoT include smart parking for vehicles, detecting and regulating traffic congestion, smart lighting of cities, waste management, detection of river floods, landslides and earthquakes in advance, monitoring of snow level, measuring and control air and water pollution, forest fire detection, detection of leakages in a water transmission system, identification of radiation levels, explosives and hazardous gases and smart rescue systems. Figure 1.2 shows the IoT market share in various domains.

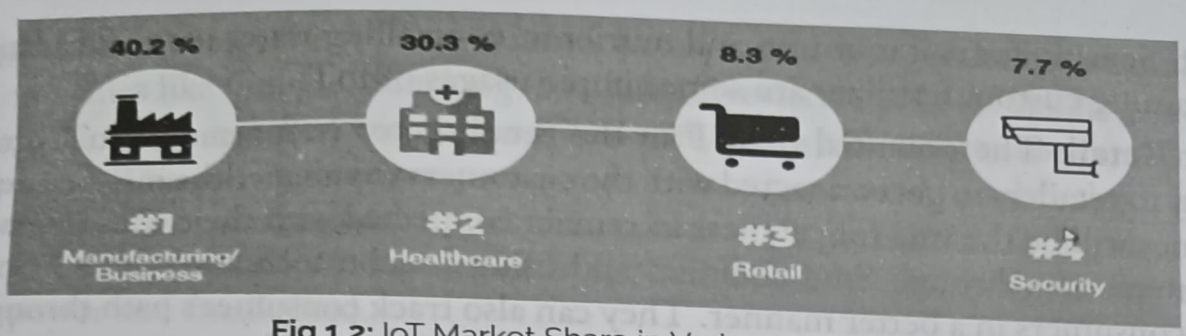

Fig.1.2: IoT Market Share in Various Domains

1.4 IoT Categories

Internet of Things can be classified into two categories: Industrial IoT and Consumer IoT. Figure 1.3 shows the components in Industrial IoT and Consumer IoT.

Fig.1.3: Components in Industrial IoT and Consumer IoT

Industrial IoT: If our factory equipment has sensors connected to Internet, then it is part of Industrial IoT (IIoT). In an Industrial IoT, a device connects to both an IP network and the global Internet. Connectivity between the nodes is done using regular as well as industry specific technologies. The IoT is important but not critical, while the IIoT failure often results in life-threatening or other emergency situations. IIoT provides an unprecedented level of visibility throughout the supply chain. Individual items, cases, pallets, containers and vehicles can be equipped with auto-identification tags and tied to GPS-enabled connections to continuously update location and movement. The IoT generates medium or high volume of data, while IIoT generates massive amount of data (a single turbine compressor blade can generate more than 500GB of data per day) so includes Big Data, Cloud Computing, Machine

Learning as necessary computing requirements. In future, the IoT will continue to enhance our lives as consumers while IIoT will enable efficient management of entire supply chain.

Consumer IoT: If our thermostat or refrigerator is connected to the Internet, then it is part of the consumer IoT. IoT devices communicate within the locally networked devices and communication to outside Internet is done through a gateway. Local communication is done mostly via Bluetooth, ZigBee or WiFi. The consumer IoT has an impact on end consumers. Consumer IoT refers to the use of 'smart' objects, which are everyday things from cars and home appliances to athletic shoes and light switches that can connect to the Internet, transmitting and receiving data and connecting the physical world to the digital world. It is mostly about human interaction with objects. Devices can alert users when certain events or situations occur or monitor activities. Google Nest sends an alert when temperature in the house is dropped below 68 degrees is an example of Consumer IoT. Similarly a garage door sensors alert the user with sound when opened, turn up the air conditioner and turn on the driveway lights half an hour before you arrive at your home, a meeting room that turns off lights when no one is using it and an air conditioner switches off when windows are open are all examples of Consumer IoT.

1.5 IoT Enablers and Connectivity Layers

IoT enablers can be looked upon based on three factors namely (a) Implementation Perspective (b) Connectivity Methods (c) Enabling Technologies. Figure 1.4 shows various IoT enablers.

Fig.1.4: IoT Enablers

The implementation perspective includes smart industries, smart homes, smart factories, smart vehicles, smart healthcare etc. Connectivity methods in Internet of Things include ZigBee, RFID, Bluetooth, WiFi, 6LoWPAN, LoRa etc. Enabling technologies include cloud computing, artificial intelligence, big data, machine learning, deep learning, fog computing etc. The connectivity methods and enabling technology will be explained in the forthcoming Chapters. Figure 1.5 shows the connectivity layers in IoT.

Fig.1.5: Connectivity Layers in IoT

The top level is the services layer comprises of various implementation entities like smart industries, smart homes, smart factories, smart vehicles, smart healthcare etc. The layer below the services layer is the local connectivity layer consisting of various technologies like RFID, Bluetooth, WiFi, 6LoWPAN, LoRa etc. Below the local connectivity layer comes the global connectivity layer which comprises of gateways to connect to the Internet and the bottom layer forms the Internet. The local connectivity is offered by various service providers and IoT management takes place at the bottom layer.

1.6 Baseline Technologies

There are various baseline technologies that are very closely related to IoT. They include

(a) Machine-to-Machine Communication

(b) Cyber-Physical Systems

(c) Web of Things

(a) Machine-to-Machine Communication (M2M) — M2M refers to communications and interactions between machines and devices. (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. M2M is a term introduced by telecommunication providers and pays emphasis on machine interactions via one or more telecom or communication networks like 3G, 4G, 5G, satellite or other public networks. This technology forms the basis for IoT. However IoT has a broader scope than M2M, since it comprises of a broader range of interactions including interactions between devices/things, things and people, things with applications and people with applications. It also enables the composition of workflows comprising all of the above interactions.

In product restocking, for example, a vending machine can message the distributor when a particular item is running low. M2M communication is an important aspect

of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and tele-medicines. Key components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link and autonomic computing software programmed to help a networked device interpret data and make decisions. The most well-known type of M2M communication is telemetry, which has been used since the early part of the last century to transmit operational data. Pioneers in telemetries first used telephone lines and later used radio waves to transmit performance measurements gathered from monitoring instruments in remote locations. The Internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday used products like home heating units, electric meters and Internet-connected appliances. Products built with M2M communication capabilities are often marketed to end users as being "smart."

Currently, M2M does not have a standardized connected device platform and many M2M systems are built to be task or device specific. It is expected that M2M becomes more pervasive, vendors will need to agree upon standards for device-to-device communications.

(b) **Cyber-Physical Systems** — Cyber-Physical Systems (CPS) represent the next generation embedded intelligent ICT systems that are interconnected, interdependent, collaborative, autonomous and provide computing and communication, monitoring/control of physical components/processes in various applications. Future CPS needs to be scalable, distributed, decentralized allowing interaction with humans, environment and machines while being connected to Internet or to other networks. Adaptability, reactivity, optimality and security are features to be embedded in such systems, as the CPS is now forming an invisible 'neural network' of the society.

Cyber-Physical systems are systems that integrate computing elements with the physical components and processes. The computing elements coordinate and communicate with sensors, which monitor cyber and physical indicators and actuators, which modify the cyber and physical environment. Cyber-Physical systems use sensors to connect all distributed intelligence in the environment to gain a deeper knowledge of the environment, which enables more accurate actions and tasks. Common applications of CPS typically fall under sensor-based communication-enabled autonomous systems. For example, many wireless sensor networks monitor some aspects of the environment and relay the processed information to a central node. Other types of CPS include smart grid, autonomous automotive systems, medical monitoring, process control systems, distributed robotics, and automatic pilot avionics.

(c) **Web of Things** — The Web of Things (WoT) is a term used to describe approaches, software architectural styles and programming patterns that allow real-world objects to be part of the World Wide Web. Similarly to what the Web (Application Layer) is to the Internet (Network Layer), the Web of Things provides an Application Layer

that simplifies the creation of Internet of Things applications. Rather than re-inventing completely new standards, the Web of Things reuses existing and well-known Web standards used in the programmable Web (e.g., REST, HTTP, JSON), semantic Web (e.g., JSON-LD, Microdata, etc.), the real-time Web (e.g., WebSockets) and the social Web (e.g., OAuth or social networks).

From a developer's perspective, the WoT enables access and control over IoT resources and applications using mainstream Web technologies like HTML 5.0, Javascript, Ajax, PHP etc. The approach to build WoT is therefore based on Representational State Transfer (REST) principles and REST APIs, which enable both developers and deployers to benefit from the popularity and maturity of Web Technologies. Building the WoT has various security and scalability issues which are needed to be addressed for achieving an efficient WoT. One of the early prototypes of the Web of Things is the "Energie Visible" project in which sensors are capable of monitoring and controlling the energy consumption of household appliances. They offered their functionality through a RESTful API. This API is then used to create a physical Mashup. Nimbits is an open source data historian server built on cloud computing architecture that provides connectivity among devices using data points.

ThingSpeak is an open source Internet of Things platform created by Hans Scharler to collect, analyze and to act on data generated by sensors and actuators. EVRYTHING is a platform for making unconnected products and connected devices as part of the Web based on Web of Things architecture. Figure 1.6 shows the terminological interdependence among various technologies.

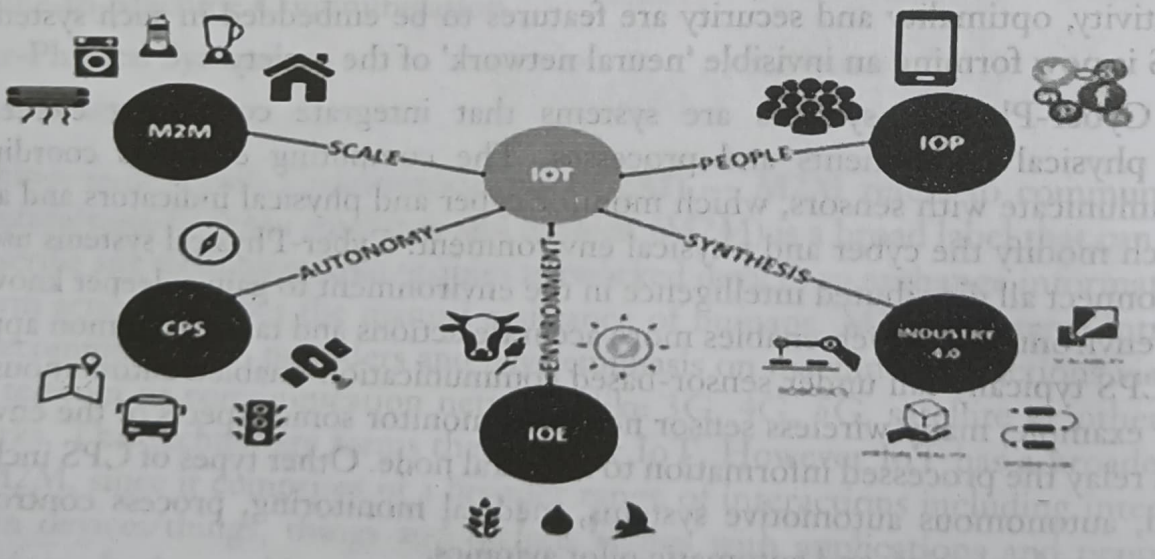

Fig.1.6: Terminological Interdependence among Technologies

1.7 Sensors

A sensor is a device that detects and responds to some type of input from the physical

environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing. Examples of sensors include infrared sensor, ultrasonic sensor, camera sensor, smoke detection sensor, temperature sensor, humidity sensor etc. Real world examples for sensing include the conversion of heat into electrical signals in a temperature sensor or atmospheric pressure converted to electrical signals in a barometer. Figure 1.7 shows a temperature sensor with three pins for sensing the temperature.

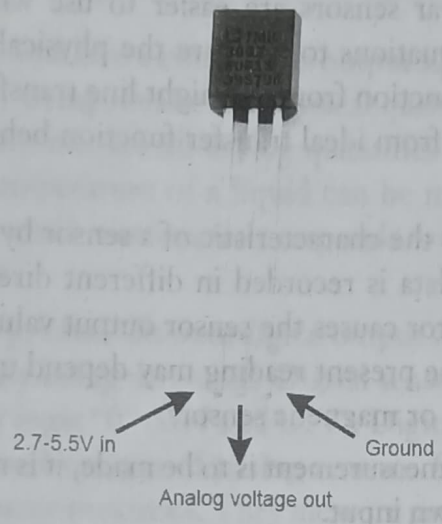

Fig.1.7: Temperature Sensor

1.7.1 Characteristics of a Sensor

Range: Every sensor has a range in which they work with an acceptable error. If the input is not in range, then the output is unpredictable.

Drift: If the output signal slowly changes or varies for the same input over a long period, this is called as drift. The drift will cause an error in the measured value. The drift may result from ageing of the sensor, temperature variance or physical changes in the sensor.

Sensitivity: Sensitivity is defined as the change in output per unit change in input of the property being measured. The sensitivity of the sensor may be constant or linear for the entire range of sensor or vary exponentially if the sensor is a non-linear sensor. The sensitivity of a sensor under real conditions may differ from the value specified. This is known as sensitivity error. If the output signal differs from the correct value by a constant, the sensor is said to have an offset error or bias.

Selectivity: Selectivity is the ability of the sensor to measure a target property in the presence of other properties. The sensor should only be sensitive to the measured property and should be insensitive to any other property likely to be encountered in its application. For example, if an oxygen sensor does not react to other gasses like CO_2 then it has good selectivity.

Resolution: The resolution of a sensor is the smallest change it can detect in the quantity that it is measuring. The resolution of a sensor with a digital output is usually the smallest resolution the digital output it is capable of processing. The more the resolution of a sensor, the more accurate is its precision. A sensor's accuracy does not depend upon its resolution.

Response and Recovery Time: The response time is the time taken by the sensor for its output to reach 95% of its final value when it is exposed to a target material. The Recovery Time is defined conversely.

Linearity: If the sensitivity of the sensor is constant for the range, then it is called as linearity of the sensor. The linear sensors are easier to use while the non-linear sensors require complex mathematical equations to measure the physical property. Non-linearity is the deviation a sensor's transfer function from a straight line transfer function. This is defined by the amount the output differs from ideal transfer function behavior over the full range of the sensor.

Hysteresis: The hysteresis is the characteristic of a sensor by which the sensor produces a different set of outputs if the data is recorded in different directions (increasing input or decreasing input). A hysteresis error causes the sensor output value to vary depending on the sensor's previous input values. The present reading may depend upon past input values. This usually happens in analog sensors or magnetic sensors.

Calibration: If a meaningful measurement is to be made, it is necessary to tune the output of the sensor with accurately known input.

Full-Scale Output: The full-scale output is the difference between the output for maximum input and the output for minimum input. The full scale range of a sensor defines the maximum and minimum values of the measured property. Since the range of the output signal is always limited, the output signal will eventually reach a minimum or maximum value, when the measured property exceeds the limits.

Precision: The precision of a sensor is its ability to produce same output when repeatedly measured for the same input. The precision is determined using statistical analysis like standard deviation.

Accuracy: The accuracy of a sensor defines how close the output is to the real value. The accuracy defines the maximum error the sensor may produce.

If the sensor has a digital output, the output is essentially an approximation of the measured property. Such an error is called quantization error. If the signal is monitored digitally, the sampling frequency can cause a dynamic error, or if the input variable or added noise changes periodically at a frequency proportional to the multiple of the sampling rate, aliasing errors may also occur.

1.7.2 Classification of Sensors

Sensors can be classified into two broad categories based on output and based on the type of data measured. Figure 1.8 shows the classification of sensors.

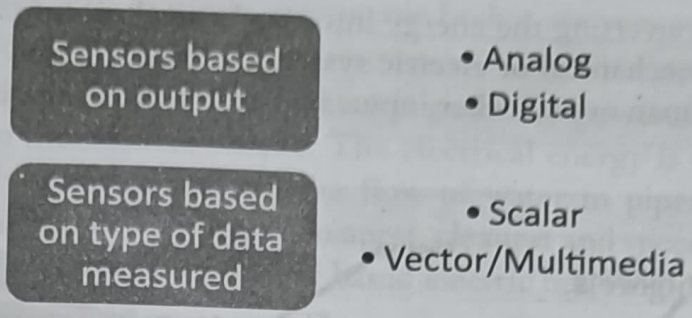

Fig.1.8: Classification of Sensors

Analog Sensors: They produce a continuous output signal or voltage which is generally proportional to the quantity being measured. Physical quantities such as temperature, speed, pressure, displacement, strain etc. are all analog quantities as they tend to be continuous in nature. For example, the temperature of a liquid can be measured using a thermometer or thermocouple (eg: geysers) which continuously responds to temperature changes as the liquid is heated up or cooled down.

Digital Sensors: They produce discrete digital output signals or voltages that are a digital representation of the quantity being measured. Digital sensors produce a binary output signal in the form of a logic "1" or logic "0" (ON and OFF). Digital sensors have been developed to overcome the traditional disadvantages of analog sensors. Digital sensors are mainly used in water, waste water and industrial processes. They measure parameters such as pH, conductivity, dissolved oxygen, ammonium, nitrate, Strong Acidic Citiation and turbidity. A digital sensor system also consists of the sensor itself, a cable and a transmitter.

Scalar sensors: These are the sensors that produce output signal or voltage which is generally proportional to the magnitude of the quantity being measured. Physical quantities such as temperature, color, pressure, strain etc. are all scalar quantities as only their magnitude is sufficient to convey the information. For example, the temperature of a room can be measured using a thermometer or thermocouple which responds to temperature changes irrespective of the orientation of the sensor or its direction.

Vector Sensors: Vector sensors produce output signal or voltage which is generally proportional to the magnitude, direction as well as the orientation of the quantity being measured. Physical quantities such as sound, image, velocity, acceleration, orientation etc. are all vector quantities as only their magnitude is not sufficient to convey the complete information. For example, the acceleration of a body can be measured using an accelerometer, which gives the component of acceleration of the body with respect to x, y, z co-ordinate axes.

1.8 Actuators

An actuator is a component of a machine or system that moves or controls the mechanism or the system. It is the mechanism by which a control system acts upon an environment. An actuator requires a control signal and a source of energy. Upon receiving the control signal,

the actuator responds by converting the energy into mechanical motion. The control system can be simple (*eg.* a fixed mechanical or electric system), software-based (*eg.* a printer driver, robot control system), a human or any other input. Figure 1.9 shows the image of an oil based hydraulic actuator.

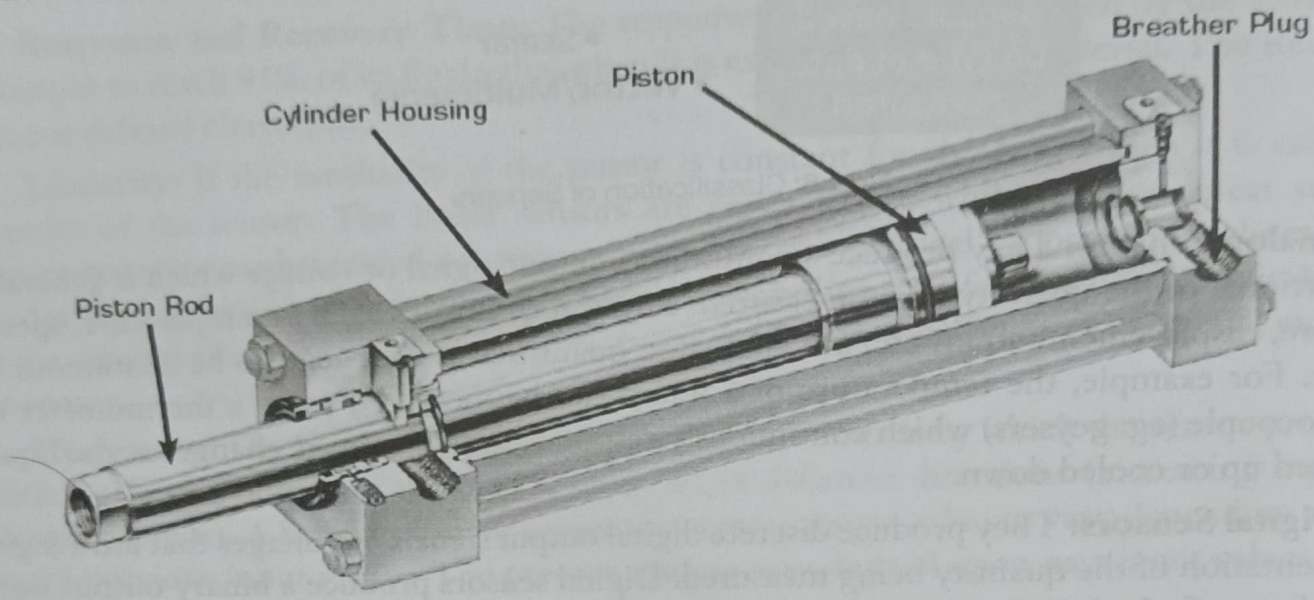

Fig.1.9: Oil based Hydraulic Actuator

1.8.1 Types of Actuators

Based on the technology used, actuators are classified into several categories as follows.

- Hydraulic Actuators
- Pneumatic Actuators
- Electrical Actuators
- Thermal/Magnetic Actuators
- Mechanical Actuators
- Soft Actuators

Hydraulic Actuators: A hydraulic actuator consists of a cylinder or fluid motor that uses hydraulic power to facilitate mechanical operation. The mechanical motion is converted to linear, rotary or oscillatory motion. Since liquids are nearly impossible to compress, a hydraulic actuator exerts considerable force. The actuator's limited acceleration restricts its usage. Examples for hydraulic actuator is the hydraulic brake in a vehicle.

Pneumatic Actuators: A pneumatic actuator converts energy formed by vacuum or compressed air at high pressure into either linear or rotary motion. Examples for pneumatic actuators are rack and pinion actuators which are used for valve controls of pipes. They are responsible for converting pressure into force. The advantage is pneumatic energy quickly responds to starting and stopping signals. The power source does not need to be stored in reserve for operation. Pneumatic actuators enable large forces to be produced from relatively

small pressure changes. For example, pneumatic brakes are very responsive to small changes in pressure applied by the driver.

Electric Actuators: An electric actuator is generally powered by a motor that converts electrical energy into mechanical torque. The electrical energy is used to actuate equipment such as solenoid valves which control the flow of water in pipes in response to electrical signals. This is considered as one of the cheapest, cleanest and speedy actuator types available. Examples of electric actuator is a solenoid based electric bell ringing mechanism.

Thermal or Magnetic Actuators: These types of actuators can be actuated by applying thermal or magnetic energy. They tend to be compact, lightweight, economical and with high power density. These actuators use shape memory materials such as shape memory alloys. Example of a thermal actuator is a thermostat and that of a magnetic actuator is an electro magnet.

Mechanical Actuators: A mechanical actuator converts rotary motion into linear motion to execute some movement. It involves gears, rails, pulleys, chains and other devices to operate. Examples of mechanical actuators are the rack & pinion mechanism and crank shaft acting as mechanical actuator.

Soft Actuators: Soft actuators are polymer based which are designed to handle fragile objects like fruit harvesting in agriculture or manipulating the internal organs in biomedicine. Soft actuators produce flexible motion due to the integration of microscopic changes at the molecular levels into a macroscopic deformation of the actuator materials. They typically address the challenging tasks in robotics. The functions of Shape Memory Polymer Actuator are similar to our muscles. Even they provide a response to a range of stimuli such as light, electrical, magnetic, heat, pH, and moisture changes. Shape memory polymers exhibit surprising features such as low density, high strain recovery, biocompatibility and biodegradability. Photo polymers or light activated polymers are a special type of shape memory polymers that are activated by light stimuli. These actuators have instant response and can be controlled remotely using the variation of light frequency or intensity without any physical contact.

1.9 IoT Components and Implementation

Before Internet of Things is implemented we need to know the functional components of IoT. They can be classified as shown in Figure 1.10. The functional components include the following.

- Devices (Things): Various devices connected to IoT forms the components for interaction and communication with other IoT devices. It may include various mobile, non-mobile devices fitted with sensors.
- Local Network: This is the component for processing and analysis of local operations
- Internet: This is the outside network through which the data is transferred for remote processing and analytics.

- Back-end services: Components for handling Web services of applications comprising of processors, servers etc. Based on the data received some actuators may be activated
- Applications: This includes various applications for communications, processing, analytics and storage.
- User Interface: This is the interface between humans and machines to access IoT.

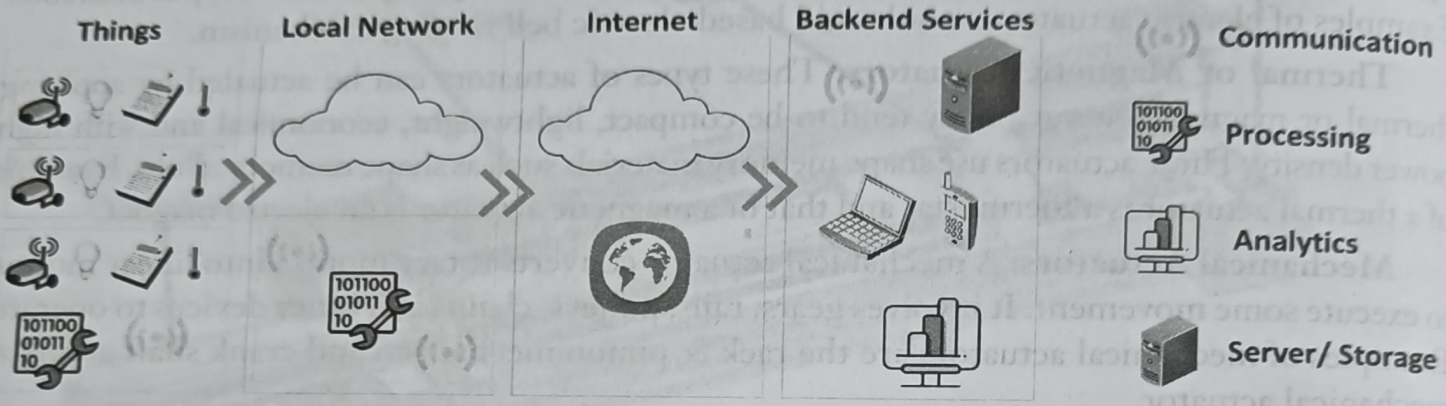

Fig.1.10: Functional Components of IoT

Now we will see the implementation of Internet of Things. Figure 1.11 shows an example for IoT implementation. On one end, we have various devices which include processors, sensor fitted equipments, radios etc which senses the data. They can also be called IoT nodes. These devices can talk to each other but they are under the jurisdiction of a gateway.

This gateway takes care of the addressing of the devices in that particular local area network. From the gateway, the sensor data passes through a proxy server to reach the Internet. Then the data passes through a Web socket. From the Web socket, the data moves on to the cloud server. It is in this cloud server back-end processing and analytics take place. Based on the analytics and inferences, the actuation takes place on the sensed data. Actuation for example may be lighting a lamp or turning off a motor or fan etc.

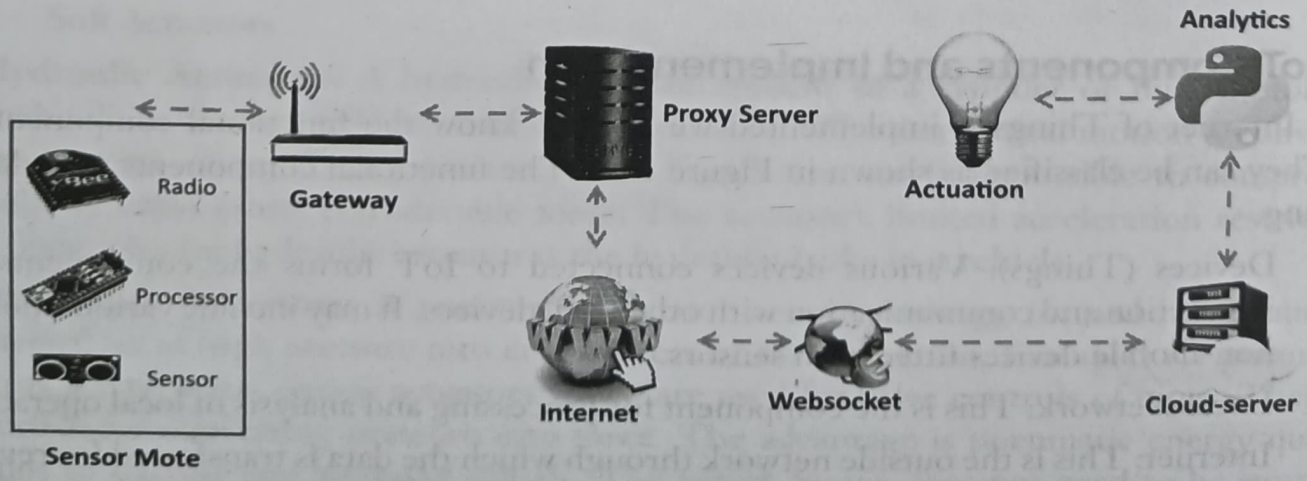

Fig.1.11: Implementation of IoT

1.9.1 Service Oriented Architecture

The service oriented architecture has four layers namely sensing layer, network layer, service layer and interface layer. Figure 1.12 shows the diagrammatic representation of service oriented architecture in IoT.

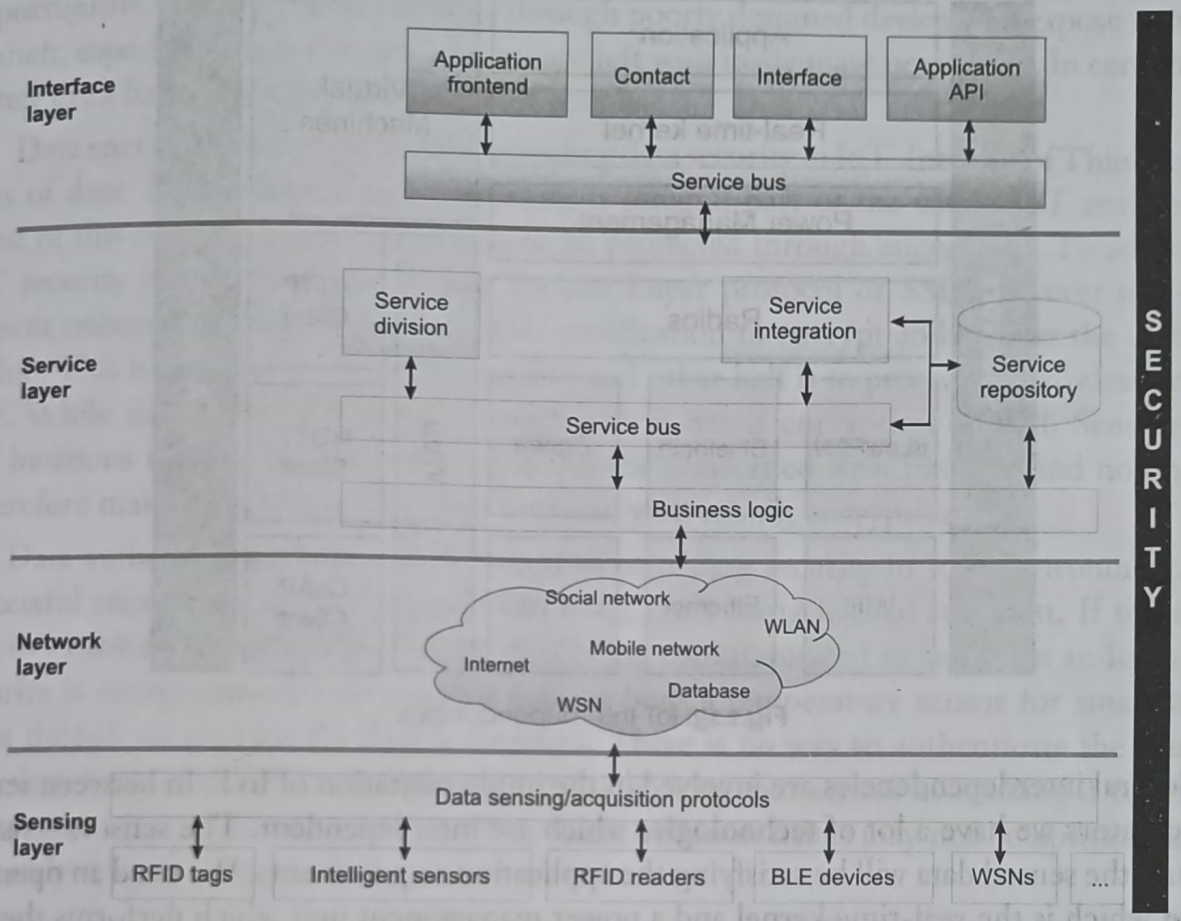

Fig.1.12: Service Oriented Architecture

The bottom most layer is the sensing layer whose prime responsibility is data sensing or taking care of the acquisition protocols. Various sensing devices like RFID tags, intelligent sensors, RFID readers, Bluetooth Low Energy (BLE) devices, wireless sensor networks etc constitute the sensing layer. The network layer above the sensing layer comprises of wireless sensor networks, Internet, mobile networks, databases, social networks and wireless LANs. The service layer comprises of the business logic, service repository, service division and service integration. The application front end, contract, API and interface forms the top most layer called the interface layer. Security is a matter of concern in all layers from top to bottom.

1.9.2 IoT Interdependencies

IoT comprises of a large number of entities like embedded devices, sensors, actuators, power management, real-time kernel, virtual machines, WWW, various clients like HTTP client, MQTT client, CoAP client etc., connectivity technologies like 6LowPan, Bluetooth, Zigbee,

WiFi, Ethernet and Low Range WiFi (LoRWiFi). Figure 1.13 shows the interdependencies between various components in IoT.

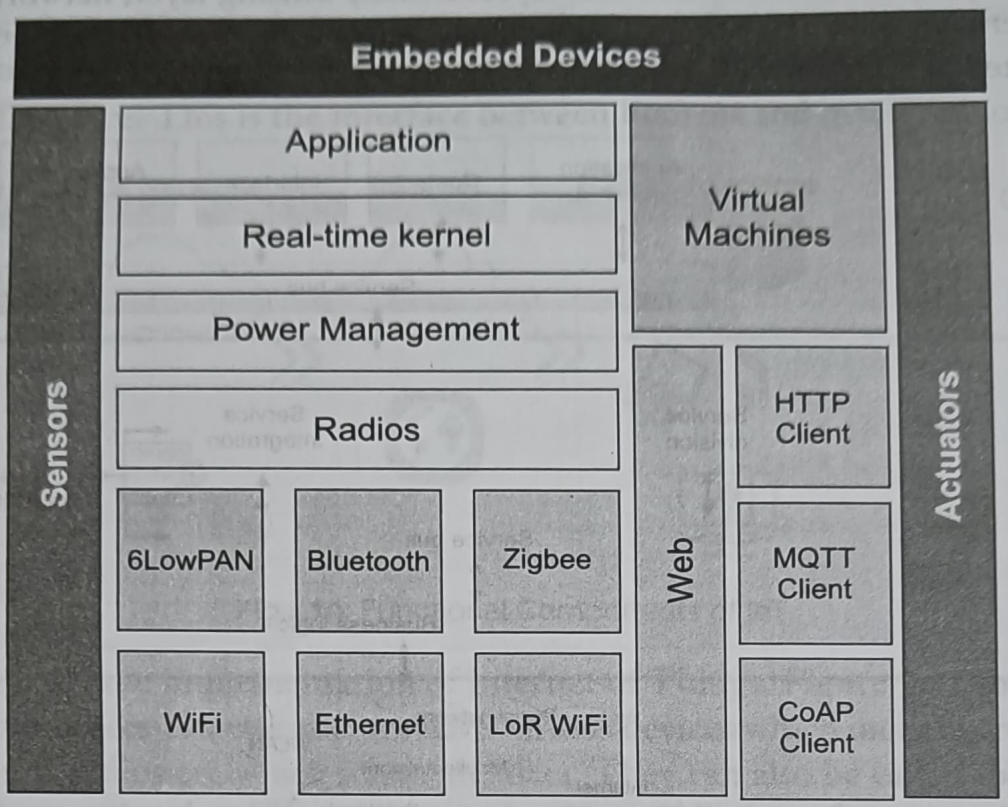

Fig.1.13: IoT Interdependencies

Several interdependencies are involved in the implementation of IoT. In between sensors and actuators we have a lot of technologies which are interdependent. The sensors sense the data and the sensed data will be satisfying the application requirements. We need an operating system which is the real-time kernel and a power management unit which performs the duty cycling of sensors. This determines how much time the sensors will be in active state, how much time will be in sleep state, how to power the sensors, how much power will be consumed, whether it can be optimized and so on. Various radios like 6LowPAN, Bluetooth, Zigbee, WiFi, Ethernet and LoR WiFi are the connectivity technologies that help to communicate the sensed data to other nodes. Virtual machines take care of the virtualization of the nodes. Different application level protocols like HTTP client, MQTT client and CoAP client help for the functioning of IoT. All these together constitute the horizontal embedded devices.

1.10 Challenges for IoT

When it comes to developing Internet of Things devices inside a laboratory, network connectivity is not a major issue. With only a few devices backed up by a server, connectivity has a very low latency and is seamless. But deploying the same IoT application on a global scale, with thousands or maybe even millions of users accessing it simultaneously, it is completely different. The Internet isn't only one network, and there are many considerations like cell

towers, connectivity, firewalls, and proxy servers that can cause problems with connectivity. Following are the most discussed challenges in IoT.

Security: Security is a crucial issue on the Internet, and it is probably the most significant challenge for the IoT. When we increase the number of connected devices, the number of opportunities to exploit vulnerabilities through poorly designed devices can expose user's data to theft, especially when the data streams are left with inadequate protection. In certain cases, it may even harm the safety and health of people.

Data encryption is one method of providing data security in IoT. Internet of Things collects tons of data. Data retrieval and processing is integral part of the whole IoT environment. Most of this data is personal and needs to be protected through encryption. To address this IoT security issue we can use Secure Sockets Layer protocol or SSL wherever our data is present online. Websites already use SSL certification to encrypt and protect the user's data online. This is only half part of the equation and other half is to protect the wireless protocol side. While data is being transferred wirelessly it needs encryption as well. Sensitive data like locations need to be available and it is to be concerned with the user and no one else. Therefore make sure we use a wireless protocol with inbuilt encryption.

Data authentication is another method of providing security in IoT environment. After successful encryption of data, chances of device itself being hacked still exist. If there is no way to establish the authenticity of the data being communicated to and from an IoT device, security is compromised. For instance, say we built a temperature sensor for smart homes. Even though we encrypt the data it transfers. There is no way to authenticate the source of data then anyone can make up fake data and send it to your sensor instructing it to cool the room even when its freezing or vice versa. Authentication issues may not be upfront but they definitely pose a security risk.

Side-channel attack is yet another security issue in IoT. Encryption and authentication both are in place. Still it leaves scope for side channel attacks. Such attacks focus less on the information and more on how that information is being presented. For instance if someone can access data like timing information, power consumption or electromagnetic leak, all of this information can be used for side channel attacks.

Hardware security issues are another problem faced by IoT. With all the hype and sudden interest in IoT devices chipmakers like ARM and Intel are reinforcing their processors for more security with every new generation but the realistic scenario doesn't seem to ever close that security gap. The problem is with modern architecture of the chips made specifically for the IoT devices, the prices will go up making them expensive. Also the complex design will require more battery power which is definitely a challenge for IoT applications. Affordable wearable IoT devices won't use such chips meaning there is need for better approach.

Privacy: The Internet of Things presents some unique challenges when it comes to privacy and a lot of that goes far beyond the data privacy issues that exist currently. Much of this is due to the trouble of integrating devices into the environments without people using

them consciously. This is becoming even more prevalent when it comes to consumer devices, such as tracking devices for cars and phones and also smart TVs. Vision features and voice recognition are now being integrated into smart TVs. These features can listen continuously to conversations or look for activity and transmit data selectively to cloud services for processing. These cloud services may sometimes even include third parties. The collection of all this information faces a number of regulatory and legal challenges.

Apart from this, there are a number of IoT scenarios that involve the data collection and the deployment of devices with a global or multinational scope that crosses cultural and social boundaries. If we are to realize the opportunities of the Internet of Things, strategies are going to have to be developed that respect the individual privacy choices while fostering innovation for new services and technologies.

Scalability: With exponential growth, the ability to manage efficiently those devices becomes paramount. Our business needs to be able to monitor the operation of its devices and add to its system as device functionality matures and networks evolve.

When deploying an IoT system, we have to keep in mind both current and future needs. If our system is not scalable, then it will not be able to accommodate future expansion when shifts in technology occur. This leaves businesses with unusable systems and devices that must either be replaced or augmented, and both are expensive prospects. The network can adapt when failures occur and remain mostly operational until the issue is repaired. For example, 2G technology is still being used in more than half of the world's mobile connections, and unless the companies still utilizing this technology are prepared for the network's impending sunset, they will likely find themselves with millions of useless devices on their hands in the not-so-distant future. Make sure our plans incorporate long-term support for devices based on technology projections in IoT.

Bandwidth Management: The number of devices connected to IoT network is skyrocketing. This is going to be a massive change to Internet. If we have more IoT devices trying to report data over a low bandwidth link than it is capable of carrying, then to ensure that the most important data gets through, we are going to filter out the less important data and compress the remaining data down. Hopefully the data will then fit within the available bandwidth. The obvious pitfall of this approach is the possibility of filtering out the important data if you have many IoT devices. The problem going forward with the IoT is every solution is going to be different and require different approaches to solve the network latency and bandwidth problems and therefore, it is difficult to make sweeping solution statements.

Interoperability: At the most basic level, the Internet of Things (IoT) is connectivity among people, processes and things. While this is as vast when spanning all industries, the enterprise and consumers, one of the central-most challenges in IoT is the enablement of seamless interoperability between each connection. These issues include the following.

- Different devices or equipments that are not made by the same manufacturer cannot be integrated.

- Different operating systems: inability to run on the same operating systems
- Different versions or times of purchase: devices that weren't made or purchased at the same time.
- Different/incommunicable types of connectors or connectivity frameworks (e.g. devices)
- Different/inconsistent communication protocol standards (i.e. rules)
- Lack of programs needed to connect the devices

Data Storage: The Internet of Things will have a huge impact on storage – the sheer volume of data, the radically different types of data created and the storage needed. Machine-generated data comes in two distinct types, creating two entirely different challenges. First, there is large-file data, such as images and videos captured from smart phones and other devices. This data type is typically accessed sequentially. The second data type is very small, for example, log-file data captured from sensors. These sensors, while they are small in size, can create billions of files that must be accessed randomly. There can be no single method to deal with the data generated by things, not least because there is such a wide variety of data generators and data types. For those planning storage for an IoT project, the first task is to determine the types of data the project will generate. It is also clear that data volumes are large and growing, that the data centre needs to adapt to deal with them and cloud-based storage may be one solution – but not the only one.

Data Analytics: The analysis of Internet of Things (IoT) data is quickly becoming a mainstream activity. With many data sources, it is often quite an effort to gather the source data required for analysis. It is necessary to identify what information is available, how it is formatted, and also to reconcile data from different sources that often contained similar information, but have inconsistencies in how it is provided.

Another challenge is to determine the proper frequency of sensor readings. For example, a temperature sensor may spit out a reading every millisecond. However, in most cases, receiving data at that cadence is overkill. That overkill has a price due to the cost of storing the extra data and the cost and complexity of analyzing masses of data that aren't valuable. As a result, it is necessary to determine what cadence actually has value for the problem you're tackling. If we're monitoring a car engine, readings once per second might be more than enough. The point is that we have to assess each metric and determine what you need through some experiments. Then, filter the data down to the proper level. Otherwise, we'll be overwhelmed with data and meaningful patterns will be that much harder to identify.

Another challenge is to identify complex patterns over time. The heart of many IoT analytics need to identify complex patterns or trends that occur over time. Classic time series and forecasting models are oriented towards identifying a trend and then extending it to forward. When analyzing IoT data, in contrast, we are often interested in deviations from normal rather than projecting the expected. After identifying what is normal we must work to find abnormal patterns that are of importance. However, there are multiple ways that abnormal

patterns might evolve. Sudden increases in temperature would naturally draw interest. But, the impacts of a very small rise in temperature that either persists for an extended period or that comes and goes with increasing frequency is different. There is much complexity in the identification of these time-based patterns.

Next challenge is how to handle interactions between terms in a model. With sensor data, this process is much more difficult. The problem is that there can be lags between impacts. For example, temperature may start rising in advance of pressure rising. To identify the interactions between various sensor readings require complicated analysis to determine not just what metrics might interact, but also over what time frame and with what lag. This makes the analysis difficult.

Finally there exist challenges in accounting for errors and missing readings. Sensors aren't always reliable. Any analytics process must build in checks and balances to account for missing data or data that is in error. For example, if an engine sensor says temperature spiked from 300 to 1,000 degrees in one second, there is a good chance that the reading was an error. If the next reading is back to normal, it is easy to flag and correct the error. But, what about if a sensor gets moved into an improper position or breaks and bad readings continue? What if a sensor fails to transmit at all for a period of time? Our analytics processes must include logic to identify suspected errors or transmission gaps and to handle those scenarios. We don't want a multitude of warning lights or messages alerting to a problem if it is really a data issue.

Standards: A lack of documented or standard best practices has had a much larger impact on Internet of Things devices that goes well beyond simply limiting their development and potential. An absence of standards may well enable inappropriate behavior by IoT devices. Without the right standards to guide and regulate manufacturers, developers may design products that operate in any number of disruptive ways online without regard for their impact. If they are configured or designed poorly, these devices may have negative consequences for networking resources they connect to and, in the broader picture, the Internet itself. A lot of this is caused by cost constraints as well as the need to develop products and get them to market before their competitors. When we add the difficulties of configuring and managing a large number of IoT devices, the need for standardization of methods, interfaces, configuration tools, and thoughtful design, along with IPv6 adoption, which is essential for the future.

Regulation: Just like privacy, there are a number of legal and regulatory questions that surround the Internet of Things. This also needs some thoughtful consideration. Legal issues concerning Internet of Things devices aren't limited to potential violations of civil rights because of law-enforcement surveillance. Other issues that must be considered are cross-border data flow, legal liability when it comes to unintended use, privacy lapses and security breaches. Also, technology is advancing at a much faster pace than regulatory policies and the agencies charged with setting and supervising IoT guidelines cannot keep up with the pace of technology.

1.11 Conclusion

This Chapter gives an introduction to Internet of Things. The characteristics of IoT, applications of IoT, various categories of IoT including consumer IoT and industrial IoT is explained. Further the different IoT enablers - implementation perspective, connectivity methods & enabling technologies and connectivity layers – services layer, local connectivity and global connectivity are illustrated with diagrams. Important baseline technologies closely related to Internet of Things like Machine-to-Machine communication, Cyber-Physical systems and Web of Things are explained in this Chapter. Sensors which provide data or input to IoT network with its characteristics are described. The different types of sensors – analog, digital, scalar and vector sensors are illustrated with examples. Another important component of IoT network is the actuator that needs to take actions according to the sensed data. Various types of actuators based on the technology used – hydraulic, pneumatic, electrical, thermal/ magnetic, mechanical and soft actuators are illustrated. The components of IoT and how IoT is implemented is explained with necessary diagrams. The service oriented architecture and dependencies between various components in IoT are described. Finally, the challenges faced in IoT implementation and how it could be mitigated is discussed in detail. After reading this Chapter, the reader will get a clear idea about the basic concepts in IoT. In the forthcoming Chapters, we will have a detailed study of all the components discussed in this Chapter.