3.1 Introduction to the Concept of IoT Devices:

IoT stands for Internet of Things. It refers to the interconnectedness of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the categorical examples where IoT is strongly established.

IOT is a system of interrelated things, computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers. And the ability to transfer the data over a network requiring human-to-human or human-to-computer interaction.

History of IOT

- 1982- Vending machine
- 1990-Toaster
- 1999-IOT(Kevin Ashton)
- 2000-LG Smart Fridge
- 2004-Smart Watch
- 2007-Smart i phone
- 2009-Car Testing
- 2011-Smart TV
- 2013-Google Lens
- 2014-Echo
- 2015-Tesla autopilot

Four Key Components of IOT

- Device or sensor
- Connectivity
- Data processing
- Interface

IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.

Over 9 billion ‘Things’ (physical objects) are currently connected to the Internet, as of now. In the near future, this number is expected to rise to a whopping 20 billion.

Main Components Used in IoT

- **Low-power embedded systems:** Less battery consumption, high performance are the inverse factors that play a significant role during the design of electronic systems.
- **Sensors:** Sensors are the major part of any IoT application. It is a physical device that measures and detects certain physical quantities and converts it into signal which can be provided as an input to processing or control unit for analysis purpose.

Different types of Sensors

- Temperature Sensors
- Image Sensors
- Gyro Sensors
- Obstacle Sensors
- RF Sensor
- IR Sensor
- MQ-02/05 Gas Sensor
- LDR Sensor
- Ultrasonic Distance Sensor

- **Control Units:** It is a unit of small computer on a single integrated circuit containing microprocessor or processing core, memory and programmable input/output devices/peripherals. It is responsible for major processing work of IoT devices and all logical operations are carried out here.
- **Cloud computing:** Data collected through IoT devices is massive, and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
- **Availability of big data:** We know that IoT relies heavily on sensors, especially in real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
- **Networking connection:** In order to communicate, internet connectivity is a must, where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

Ways of Building IOT

There are two ways of building IoT:

- Form a separate internet work including only physical objects.
- Make the Internet ever more expansive, but this requires hard-core technologies such as rigorous cloud computing and rapid big data storage (expensive).

In the near future, IoT will become broader and more complex in terms of scope. It will change the world in terms of *"anytime, anyplace, anything in connectivity."*

IoT Enablers

- **RFIDs:** uses radio waves in order to electronically track the tags attached to each physical object.
- **Sensors:** devices that are able to detect changes in an environment (ex: motion detectors).
- **Nanotechnology:** as the name suggests, these are tiny devices with dimensions usually less than a hundred nanometers.
- **Smart networks:** (ex: mesh topology).

Working with IoT Devices

- **Collect and Transmit Data :** For this purpose sensors are widely used they are used as per requirements in different application areas.
- **Actuate device based on triggers produced by sensors or processing devices:** If certain conditions are satisfied or according to user's requirements if certain trigger is activated then which action to perform that is shown by Actuator devices.
- **Receive Information:** From network devices, users or devices can take certain information also for their analysis and processing purposes.
- **Communication Assistance:** Communication assistance is the phenomenon of communication between 2 networks or communication between 2 or more IoT devices of same or different networks. This can be achieved by different communication protocols like: MQTT, Constrained Application Protocol, ZigBee, FTP, HTTP etc.

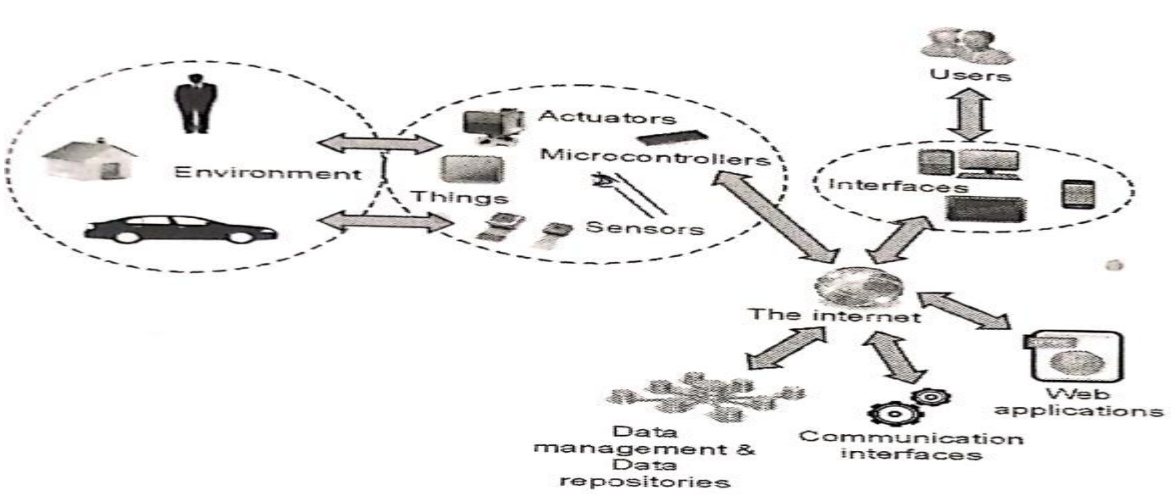

Fig: Working with IOT devices

Characteristics of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that do not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.

- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

Desired Quality of any IoT Application

Interconnectivity
It is the basic first requirement in any IoT infrastructure. Connectivity should be guaranteed from any devices on any network then only devices in a network can communicate with each other.
Heterogeneity
There can be diversity in IoT enabled devices like different hardware and software configuration or different network topologies or connections, but they should connect and interact with each other despite so much heterogeneity.
Dynamic in Nature
IoT devices should dynamically adapt themselves to the changing surroundings like different situations and different prefaces.
Self-adapting and self-configuring technology
For example, surveillance camera. It should be flexible to work in different weather conditions and different light situations (morning, afternoon, or night).
Intelligence
Just data collection is not enough in IoT, extraction of knowledge from the generated data is very important. For example, sensors generate data, but that data will only be useful if it is interpreted properly. So intelligence is one of the key characteristics in IoT. Because data interpretation is the major part in any IoT application because without data processing we can't make any insights from data. Hence, big data is also one of the most enabling technologies in IoT field.
Scalability
The number of elements (devices) connected to IoT zones is increasing day by day. Therefore, an IoT setup should be capable of handling the expansion. It can be either expand capability in terms of processing power, storage, etc. as vertical scaling or horizontal scaling by multiplying with easy cloning.
Identity
Each IoT device has a unique identity (e.g., an IP address). This identity is helpful in communication, tracking and to know status of the things. If there is no identification then it will directly affect security and safety of any system because without discrimination we can't identify with whom one network is connected or with whom we have to communicate. So there should be clear and appropriate discrimination technology available between IoT networks and devices.

Safety

Sensitive personal details of a user might be compromised when the devices are connected to the Internet. So data security is a major challenge. This could cause a loss to the user. Equipment in the huge IoT network may also be at risk. Therefore, equipment safety is also critical.

Architecture

It should be hybrid, supporting different manufacturer's products to function in the IoT network.

As a quick note, IoT incorporates trillions of sensors, billions of smart systems, and millions of applications.

Application Domains

IoT is currently found in four different popular domains:

1) Industrial business - 40.2%
2) Healthcare - 30.3%
3) Security-7.7%
4) Retail - 8.3%

Modern Applications

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection
- Water flow monitoring
- Traffic monitoring
- Wearables
- Smart door lock protection system
- Robots and Drones
- Healthcare and Hospitals, Telemedicine applications
- Security
- Biochip Transponders (For animals in farms)
- Heart monitoring implants (Example Pacemaker, ECG real time tracking)
- Agriculture
- Industry

Advantages of IoT

- Improved efficiency and automation of tasks.
- Increased convenience and accessibility of information.
- Better monitoring and control of devices and systems.
- Greater ability to gather and analyze data.
- Improved decision-making.
- Cost savings.

Disadvantages of IoT

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- Dependence on technology and potential for system failures.
- Limited standardization and interoperability among devices.
- Complexity and increased maintenance requirements.
- High initial investment costs.
- Limited battery life on some devices.
- Concerns about job displacement due to automation.
- Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.