Internet of Things
Assignment - 1

MANOJ. L
4AL16CS125

1. Memorize the goals of IOT? List out different challenges of IOT.

→ Goals of IOT:-

* The basic premise and goal of IOT is to "Connect the unconnected". This means that objects that are not currently joined to a computer network, namely the Internet, will be connected so that they can communicate and interact with people and other objects
* When objects and machine can be sensed and controlled remotely across a network, a tighter integration between the physical world and computer is enabled.
* This allows for improvements in the areas of efficiency, accuracy, automation and the enablement of advanced applications.

Challenges of IOT:

* Scale:- While the scale of IT networks can be large, the scale of IOT can be several order of magnitude larger. The scale of the network the utility is managing has increased by more than 1000 fold.
* Security:- With more "things" becoming connected with other "things" and people. security is an increasingly complex issue for IOT. Threat surface is now greatly expanded, and if a device gets hacked its connectivity is a major concern. IOT security is also pervasive across just about every fact of IOT
* Privacy:- As sensors become more prolific in our everyday lives, much of the data gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment.

For business, this data has monetary value.

* Bigdata and data Analytics:- IOT and its large number of sensors is going to trigger a deluge of data that must be handled. This data will provide critical information and insights if it can be processed in an efficient manner. The challenge, however is evaluating massive amounts of data arriving from different sources in various form and doing so in a timely manner.

* Interoperability:- Various protocols and architectures are jockeying for market share and standardization within IOT. Some of these protocols and architectures are based on propietary elements, and others are open. Recent IOT standards are helping minimize this problem, but there are often various protocols and implementation available for IOT networks

2. Define Information Technology and operational Technology. Distinguish Various differences between IT and OT network

Infomation technology support connection to the internet along with related data and technology systems and is focused on the secure flow of data across an agarication.

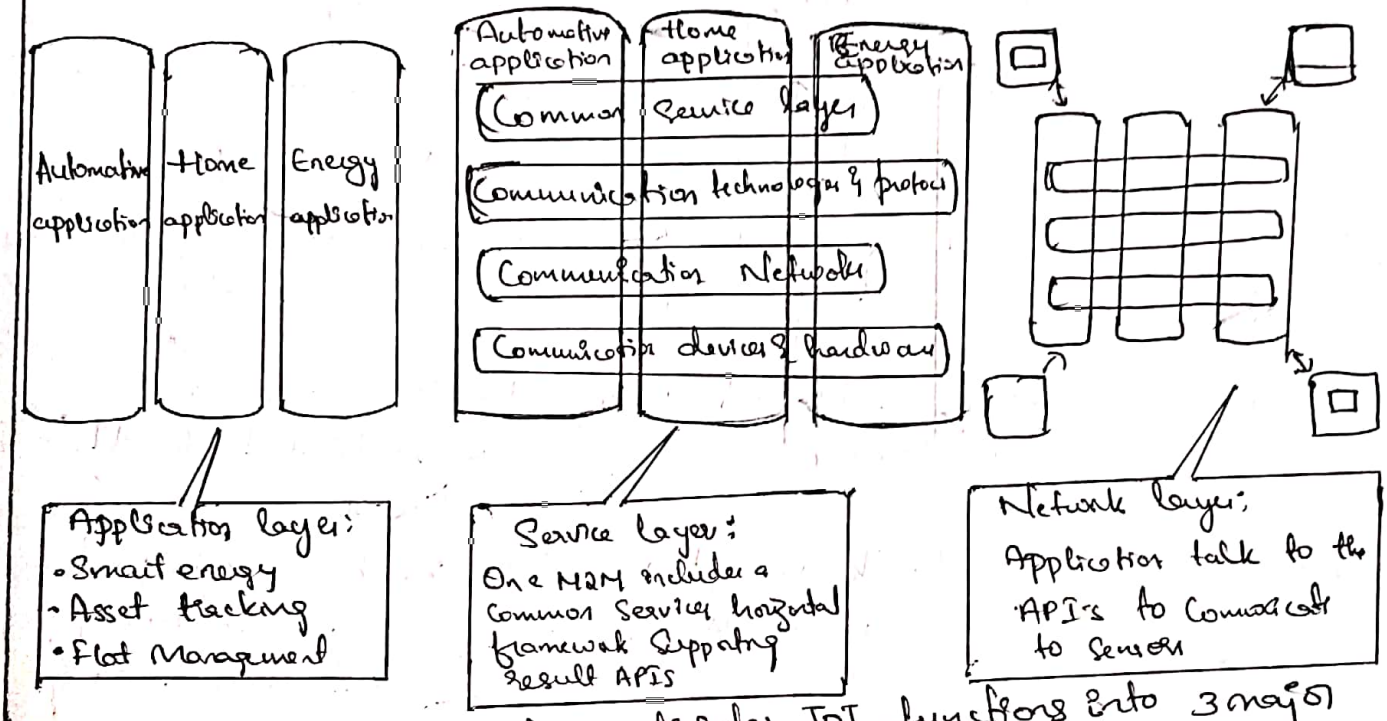
Operational technology monitors and controls devices and processes on physical operational systems.

Some of the differences between IT and OT networks and their various challenges.

Criterion	OT Network	IT Network
1. Operational focus	Keep the business operating 24x7	Manage the Computer, data & employee Communication System in a secure way.
2. Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability.
3. Type of data	Monitoring, Control, and Supervisory data	voice, video, transactional and bulk data.
4. Security	Controlled physical access to devices	Devices and user authenticated to the network.
5. Implication of failure	OT network disruption directly impacts business	Can be business impacting depending on industry, but work around may be possible.
6. Network upgrades	Only during operational maintenance windows	Often requires an outage window when workers are not on site, impact can be mitigated.
7. Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: Continual patching of hosts is required and the network is Connected to internet and requires vigilant protection.

3. Illustrate the one-machine to machine IOT architecture with diagram and also examine how the application, Service and Network layer providing functions to one M2M architecture.

One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software and access methods. By developing a horizontal platform architecture, one M2M is developing standards that allow interoperability at all levels of the IoT stack.



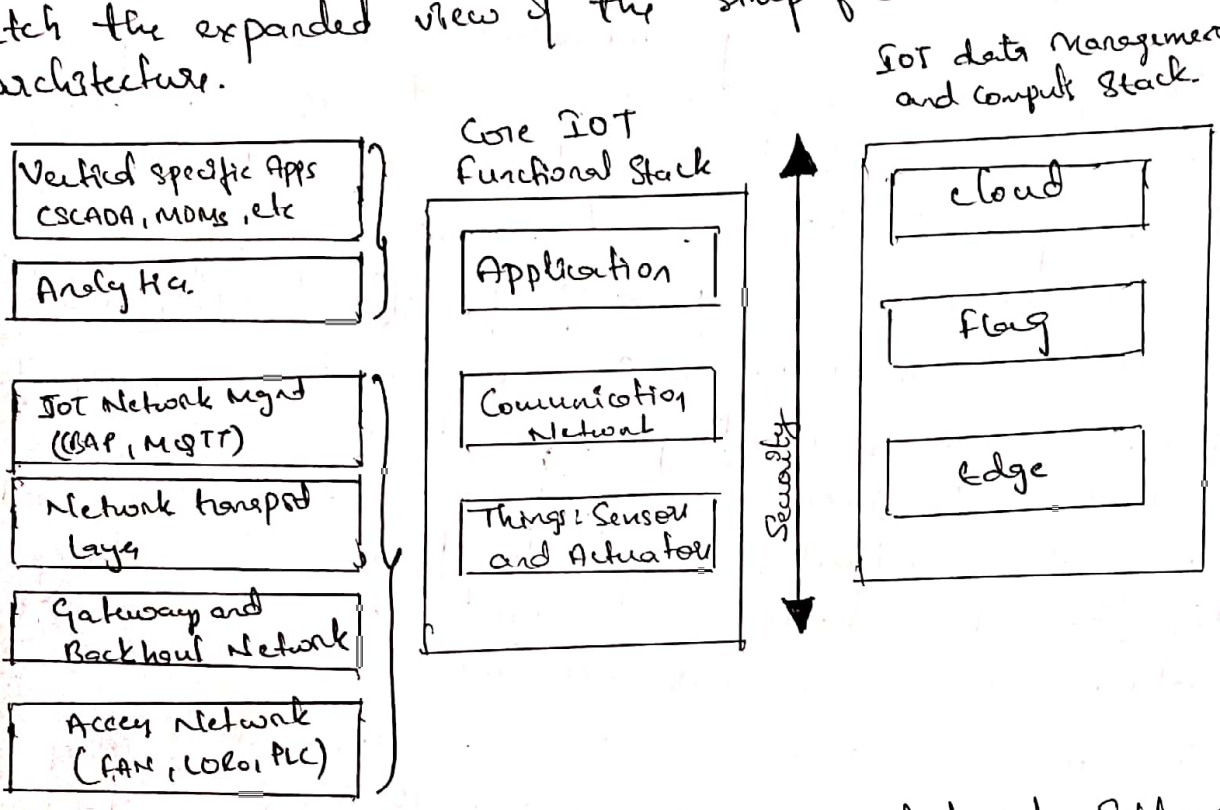
The one M2M architecture divides IoT functions into 3 major domains:

- Application layer: The one M2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application layer protocols and attempts to standardize northbound API definitions for interactions with business intelligence systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

* Service layer: This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols and the hardware.

* Network layers: This is the communication domain for the IoT devices and endpoints. It includes the devices themselves and the communication network that links them. Embodiments of this communication infrastructure include wireless mesh technologies, such as IEEE 802.11ah

4. Sketch the expanded view of the simplified IOT architecture.



The Core IOT functional stack can be expanded into sublayers containing greater detail and specific network functions. For example, the communication layer is broken down into four separate sublayers: The access network, gateways and backhaul, IP transport, and operations and management sublayers.

The application layer of IOT network is quite different from the application layer of a typical enterprise network. Instead of simply using business application, IOT often involves a strong big data analytics component. IOT is not just about the control of IOT devices but, rather the useful insights gained from the data generated by these devices. Thus the application layer typically has both

analytics and industry-specific IOT control system components.

5. Illustrate the characteristics of small object.

1. Processing Unit: A small object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensors, coordinating control signals to any actuators, and controlling a variety of functions on the smart object, including the communication and power systems. The specific type of processing unit that is used can vary greatly, depending on the specific processing needs of different applications.

2. Sensors and/or actuators: A smart object is capable of interacting with the physical world through sensors and actuators. A sensor hears and measures its environment, while as an actuator is able to produce some change in the physical world. A smart object does not need to contain both sensors and actuators.

3. Communication device:- The communication unit is responsible for connecting a smart object with other smart objects can be either wired or wireless. In IOT networks smart objects are wirelessly interconnected for a number of reasons, including cost, limited infrastructure availability etc.

4. Power Source: Smart objects have components that need to be powered. The most significant power consumption usually comes from the communication unit of a smart object. As with the other three smart object building blocks, the power requirements also very greatly from application. Typically, smart objects are limited in power, are deployed for a very long time, and are not easily accessible.

6. Illustrate how sensors are grouped and clustered into different categories and explain the different types of sensors with example.

There are a number of ways to group and cluster sensors into different categories, include the following

1. Active & passive: Sensors can be categorized based on whether they produce an energy output and typically require an external power supply & whether they ~~supply~~ simply receive energy and typically require no external power supply.
2. Invasive & non-Invasive: Sensors can be categorized based on whether a sensor is part of the environment it is measuring & external to it
3. Contact & non-contact: Sensors can be categorized based on whether they require physical contact with what they are measuring & not.
4. Absolute & relative: Sensors can be categorized based on whether they measure on an absolute scale & based on a difference with a fixed as variable reference value.
5. Area of Application: Sensors can be categorized based on the specific industry or vertical where they are being used.
6. How Sensors measure: Sensors can be categorized based on the physical mechanism used to measure sensory input.
7. What Sensors measure: Sensors can be categorized based on their applications or what physical variables they measure

Different types of Sensors:

Sensor	Description	Examples
1. Position	A position Sensor measures the position of an object	Potentiometer, inclinometer
2. Occupancy and motion	Occupancy Sensor detect the presence of people and animals in surveillance area	Electric eye, radar.
3. Velocity and acceleration	Velocity Sensor may be linear or angular, indicating how fast an object moves along a straight line. Acceleration Sensor measure changes in velocity.	Accelerometer, gyroscope
4. Force	Force Sensor detect whether a physical force is applied & whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile Sensor.
5. Pressure	Pressure Sensor are related to force a Sensors, measuring force applied by liquids & gases. Pressure is measured in terms of force per unit area.	Barometer
6. Flow	Flow Sensor detect the rate of fluid flow	Anemometer, mass flow Sensor.

7) Highlight how Sensors and actuators interact in physical world and Compare Sensors and actuator functionality with human.

1) Type of motion: Actuators can be classified based on the type of motion they produce.
Eg:- Linear, Rotatory, etc.

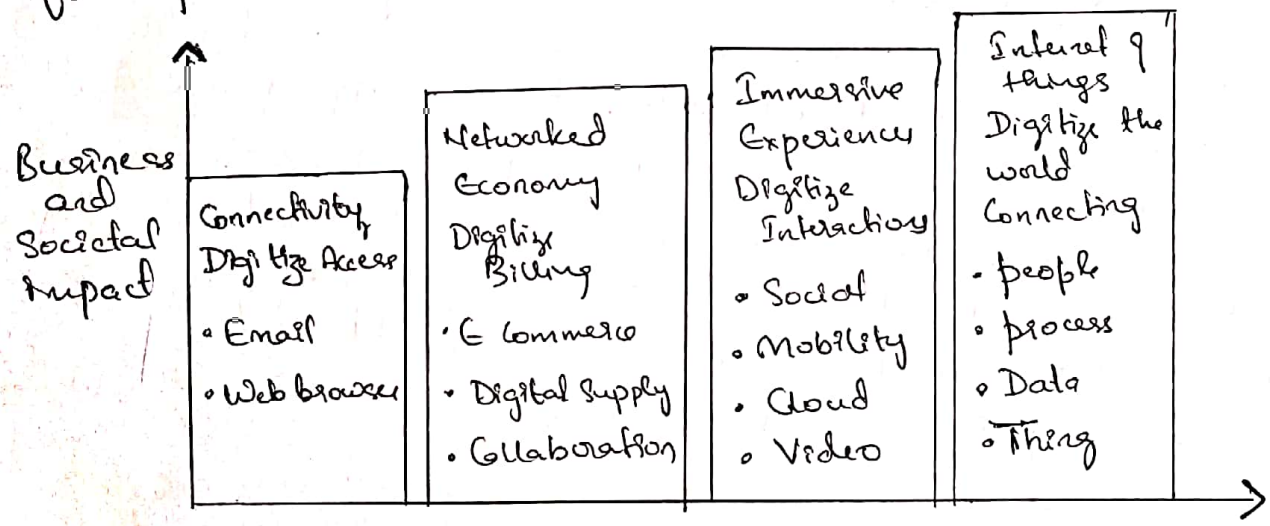
2) Power: Actuators can be classified based on their power output. Eg:- High power, low power, micro power.

3) Binary or Continous: Actuators can be classified based on the number of stable state output.

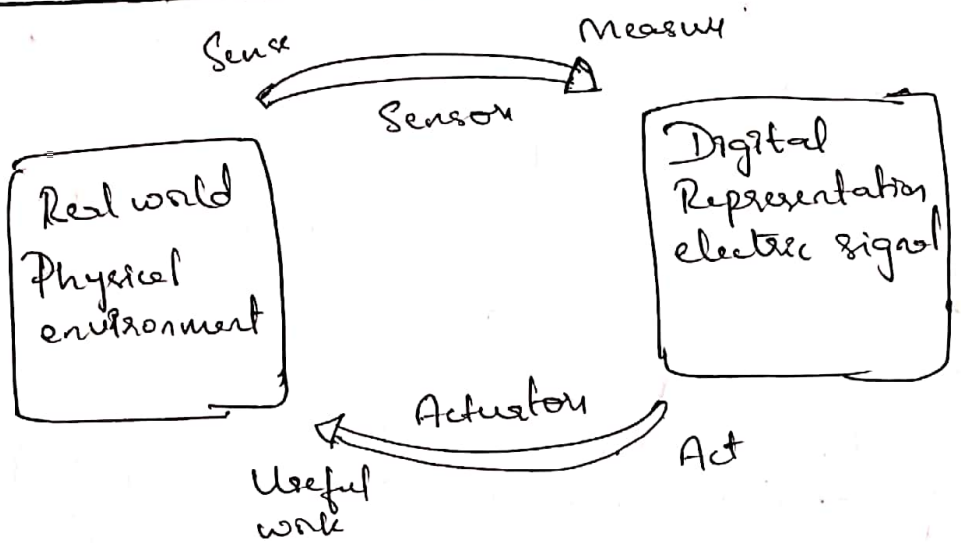
4) Area of Application: Actuators can be classified based on the specific industry or vertical where they are used.

5) Type of energy: Actuators can be classified based on their energy type.

8. Illustrate the evolutionary phase of Internet along with the current challenges addressed by Connected roadways
The evolution of the Internet can be categorized into four phases:

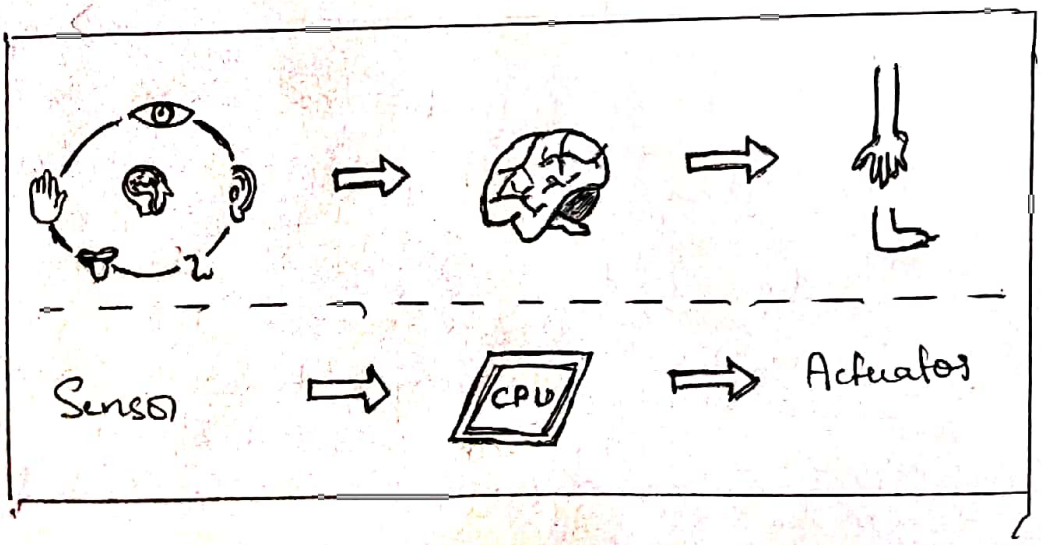


Internet phase	Definition
• Connectivity	This phase connected people to email, web, services, and search so that information is easily accessed.
• Networked Economy	This phase enabled e-commerce and supply chain enhancement along with Collaborative engagement to drive increased efficiency in business applications



Humans use their five senses to sense and measure their environment. The sensory organs convert this sensory information into electrical impulses that the nervous system sends to the brain for processing.
Likewise, IOT Sensors are devices that sense and measure the physical world and signal this measurements as electric signal sent to some type of microprocessor or microcontroller for additional processing. The human brain signals motor function and movement, and the nervous system carries that information to the appropriate part of the muscular system. Correspondingly, a processor can send an electric signal to an actuator that translate the signal into some type of movement or useful work that has measurable impact on the physical world.

Comparison of sensor and actuator functionality with humans:



- Immersive experiences — This phase extended the internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud
- Internet of things — This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

Current challenges addressed by connected roadways:

Challenge	Supporting data
Safety	According to the US department of transportation, 5.6 million crashes were reported in 2012 alone.
Mobility	More than a billion cars are on the roads worldwide connected vechicle mobility applications can enable system operator and driver to make more informed decision.
Environment	According to American public transportation association each year transit systems can collectively reduce carbon dioxide emissions.

9. List and briefly explain how the core IoT functional stack is being operated.

From an architectural standpoint, several component have to work together for an IoT Network to be operation:

→ "Things" layer: At this layer, the physical device need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.

→ Communication network layer: When smart objects are not self contained, they need to communicate with an external system. In many cases, this communication use a wireless technology. This layer has four sublayers.

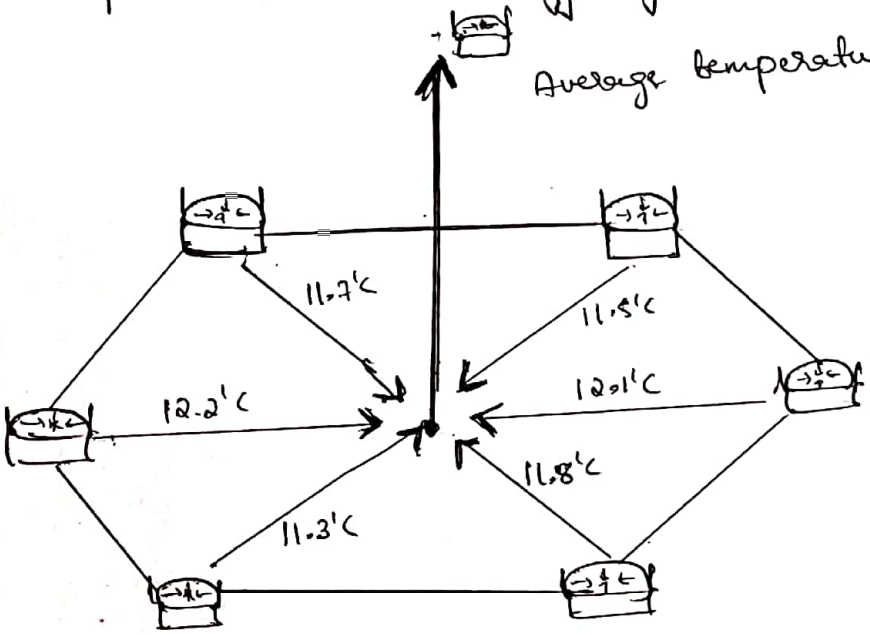
- Access network sublayer: The last mile of the IOT network is the access network. This is typically made up of wireless technologies such as 802.11ah.
- Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects.
- Network transport sublayer: For communication to be successful network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect & media to use.
- IOT network management sublayer: Additional protocols must be in place to allow the headend application to exchange data with the sensor.

→ Application and analytics layer: At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary but to make intelligent decision based on information collected.

10. Illustrate the data aggregation function in wireless sensor networks and explain how smart objects are wirelessly connected.

In data aggregation function the temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.

Figure depicts the data aggregation in WSN:



→ The data aggregation function at the network edges is where fog and mist Computing are critical IOT architectural elements needed to deliever the Scale and performance required by so many IOT use cases wirelessly Connected Smart objects generally have one of the following 2 - Communication patterns:

1. Event driven: Transmission of Sensory information is triggered only when smart objects detects a particular event or predetermined threshold.
2. Periodic: Transmission of Sensory information occurs at only at a periodic intervals.