UNIT 1

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.

It field of computer technology, where physical devices are communicating over the Internet. Devices are termed as things that are sensors, and actuators that communicate and send information to each other on the web. It is an ecosystem where the interacting devices share data through a communication media known as the internet. These devices are instructed with code to operate during a special event.

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

Here you will get to know about how IOT is involved and also from the explanation of each will let you know how IOT plays a role in this innovations !

- 1982 – Vending machine: The first glimpse of IoT emerged as a vending machine at Carnegie Mellon University was connected to the internet to report its inventory and status, paving the way for remote monitoring.
- 1990 – Toaster: Early IoT innovation saw a toaster connected to the internet, allowing users to control it remotely, foreshadowing the convenience of smart home devices.
- 1999 – IoT Coined (Kevin Ashton): Kevin Ashton coined the term “Internet of Things” to describe the interconnected network of devices communicating and sharing data, laying the foundation for a new era of connectivity.
- 2000 – LG Smart Fridge: The LG Smart Fridge marked a breakthrough, enabling users to check and manage refrigerator contents remotely, showcasing the potential of IoT in daily life.

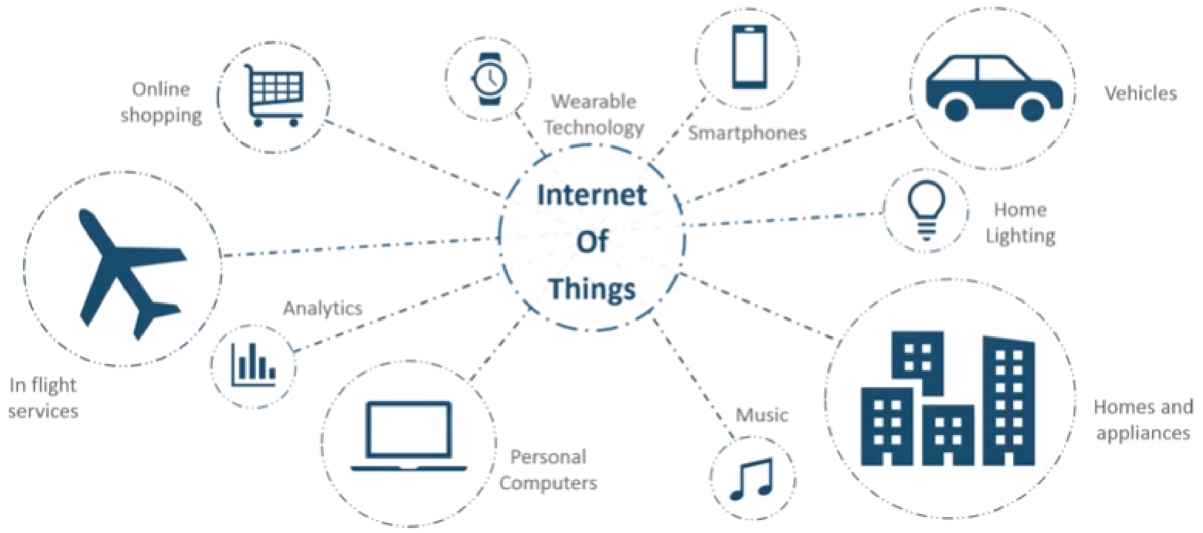
- 2004 – Smart Watch: The advent of smartwatches introduced IoT to the wearable tech realm, offering fitness tracking and notifications on-the-go.
- 2007 – Smart iPhone: Apple’s iPhone became a game-changer, integrating IoT capabilities with apps that connected users to a myriad of services and devices, transforming smartphones into hubs.
- 2009 – Car Testing: IoT entered the automotive industry, enhancing vehicles with sensors for real-time diagnostics, performance monitoring, and remote testing.
- 2011 – Smart TV: The introduction of Smart TVs brought IoT to the living room, enabling internet connectivity for streaming, app usage, and interactive content.
- 2013 – Google Lens: Google Lens showcased IoT’s potential in image recognition, allowing smartphones to provide information about objects in the physical world.
- 2014 – Echo: Amazon’s Echo, equipped with the virtual assistant Alexa, demonstrated the power of voice-activated IoT, making smart homes more intuitive and responsive.
- 2015 – Tesla Autopilot: Tesla’s Autopilot system exemplified IoT in automobiles, introducing semi-autonomous driving capabilities through interconnected sensors and software.

What is an Internet of Things (IoT)

Let's us look closely at our mobile device which contains GPS Tracking, Mobile Gyroscope, Adaptive brightness, Voice detection, Face detection etc. These components have their own individual features, but what about if these all communicate with each other to provide a better environment? For example, the phone brightness is adjusted based on my GPS location or my direction.

Connecting everyday things embedded with electronics, software, and sensors to internet enabling to collect and exchange data without human interaction called as the Internet of Things (IoT).

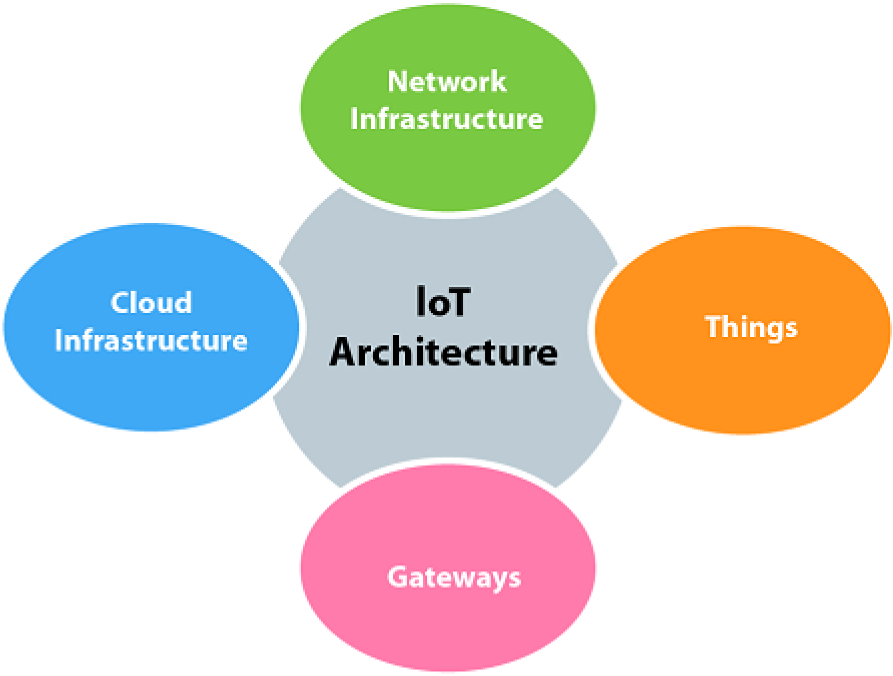
The term "Things" in the Internet of Things refers to anything and everything in day to day life which is accessed or connected through the internet.



IoT is an advanced automation and analytics system which deals with artificial intelligence, sensor, networking, electronic, cloud messaging etc. to deliver complete systems for the product or services. The system created by IoT has greater transparency, control, and performance.

How does Internet of Thing (IoT) Work?

The working of IoT is different for different IoT echo system (architecture). However, the key concept of there working are similar. The entire working process of IoT starts with the device themselves, such as smartphones, digital watches, electronic appliances, which securely communicate with the IoT platform. The platforms collect and analyze the data from all multiple devices and platforms and transfer the most valuable data with applications to devices.



Examples of Internet of Things (IoT)

- IoT Devices at Home
- Wearable Health Monitors: Fitness trackers such as Fitbits.
- Voice Assistants: Devices like Alexa and Siri.
- Smart Appliances: Examples include the iRobot vacuum cleaner.
- Smart Cars: Notably, Tesla's connected vehicles.
- Smart Home Security Systems.

IoT Devices in Industries and Cities

- Smart Grids for efficient energy distribution.
- Smart Supply Chain Management.
- Healthcare Systems with remote monitoring.
- Smart Farming for Precision Agriculture.
- Smart Connected Factories Optimizing Manufacturing

Real Life Example of Working of IoT

In our data to day life, we use many IoT based devices. Some of them are:

- Nowadays, many people wear smartwatches which is none other than an IoT device. It contains an accelerometer that measures the number of steps taken, detects hand movements, etc.

- Using (GPS), these devices can determine your location and compute the distances traveled.

- There are many IoT devices which are now making your home smart. You can lock/unlock you doors using an application. There are many devices designed which has sensors that can detect any type of mishappening in your home, eg: Glass break, smoke, heat, motion detectors, etc.

- Not only this, IoT devices can also help in disaster management. They help in detection of temperature, carbon content in the region. In case of any forest fire, these devices send an alert to the control room, fire department.

How does an IoT System Actually Works?

An IoT device basically uses data from the surroundings or the inputs from the user and then analyzes that data. So firstly, sensors collect data from the environment. It could be one sensor or a collection of sensors(called devices). They collect the data, which is used later. Examples of sensors can be GPS, LDR, temperature sensors, etc. Next, the collected data by the sensor is sent to the cloud via some connection. These connections can be WiFi, LAN, satellite, Bluetooth, etc. Once the data reached the cloud, the software reads and analyzes the data according to the program written in it. This typically includes the processing of data to give predictions. Examples of data processing can be reading temperature values, reading weather conditions, processing any image, etc. The most important part of this process is sending this information to the user. This can be done by creating a user inference and showing them the processed data. This includes alerting the users when the temperature becomes high, alerting them about the weather conditions, etc.

Characteristics of the Internet of Things

The Internet of Things (IoT) is characterized by the following key features that are mentioned below.

1. Connectivity

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, the connection between people through Internet devices like mobile phones, and other gadgets, also a connection between Internet devices such as routers, gateways, sensors, etc.

2. Intelligence and Identity

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3. Scalability

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4. Dynamic and Self-Adapting (Complexity)

IoT devices should dynamically adapt themselves to changing contexts and scenarios. Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, and night).

5. Architecture

IoT Architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ‘ products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6. Safety

There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at risk. Therefore, equipment safety is also critical.

7. Self Configuring

This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Advantages:

- It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.
- By automating activities, it saves us a lot of time.
- Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real time.
- Electric Devices are directly connected and communicate with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.
- Personal assistance can be provided by IoT apps, which can alert you to your regular plans.
- It is useful for safety because it senses any potential danger and warns users. For example, GM OnStar, is a integrated device that system which identifies a car crash or accident on road. It immediately makes a call if an accident or crash is found.
- It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.
- Patient care can be performed more effectively in real time without the need for a doctor's visit. It gives them the ability to make choices as well as provide evidence-based care.
- Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system.

Disadvantages:

- Hackers may gain access to the system and steal personal information. Since we add so many devices to the internet, there is a risk that our information as it can be misused.
- They rely heavily on the internet and are unable to function effectively without it.
- With the complexity of systems, there are many ways for them to fail.

- We lose control of our lives—our lives will be fully controlled and reliant on technology.
- Overuse of the Internet and technology makes people unintelligent because they rely on smart devices instead of doing physical work, causing them to become lazy.
- Unskilled workers are at a high risk of losing their jobs, which could lead to unemployment. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing security guards, maids, ironmen, and dry-cleaning services etc.
- It is very difficult to plan, build, manage, and enable a broad technology to IoT framework.
- Deploying IoT devices is very costly and time-consuming. ✓

Internet of Things Applications

The Internet of Things (IoT) has many applications, including:

- **Healthcare**

IoT can improve healthcare by using smart medical equipment, fitness bands, smartwatches, and stress monitors.

- **Smart farming**

IoT can help farmers monitor and manage their crops and fields, and automate processes to increase productivity.

- **Smart grid**

IoT can help utility companies make energy provision more efficient by enabling real-time monitoring, control, and optimization of electricity generation, distribution, and consumption.

- **Smart home**

IoT can be used to create smart homes by integrating sensor-driven data into various smart home devices.

- **Supply chain management**

IoT can improve supply chain management by reducing costs and improving efficiency.

- **Insurance**

IoT can help insurance companies offer customized policies and encourage healthier habits by offering discounts for IoT wearables.

- **Transportation**

IoT can make transportation applications more efficient and safer by minimizing administrative burden in fleet management and supporting drivers with autonomously operating vehicles.

- **Autonomous driving**

IoT can help with autonomous driving by using smart sensor technology and artificial intelligence to help drivers avoid collisions and drive safely.

Other applications of IoT include: Creating better enterprise solutions, Building smarter cities, Revolutionizing wearables, Integrating connected factories, and Reshaping hospitality.

Below is a table of differences between the Internet of Things and Artificial Intelligence:

S. No.	Based on	Internet of Things	Artificial Intelligence
1.	Connection type	A set of interconnecting devices over a network	The machine is independent and interconnecting is not needed
2.	Cloud Computing	Both are complimentary in efficiency while Cloud gives a pathway to manage data.	Highly Strong – As it facilitates the machine to think, enact and learn from the human instances created.
3.	Capability	Device capabilities are known in prior	Machine capabilities can never be predicted
4.	Interaction	Human Interaction is needed	Human Interaction is not needed
5.	Future Scope	Human instructions are needed	Machines can learn and start to act in a more human way
6.	Need of Instructions	Needed to instruct devices	Machines learn from experiences

S. No.	Based on	Internet of Things	Artificial Intelligence
7.	Learning from data	In the Internet of Things, various sensors are present around us, and each of them has a few facts running through it, and the identifying information is transmitted on the internet.	In artificial intelligence, the system learns from errors or background activity and attempts to grow itself to perform better.
8.	Dependency	IoT won't work without AI.	AI is not dependent on IoT
9.	Cost	Price is substantially lesser.	Price is mostly calculated based on each requirement.
10.	Applications	Applications include Smart Wearables, Smart City, Smart Home, Water Monitoring, etc.	Applications include Chatbots, Job Adverts, Natural language processing, Speech recognition, Machine vision, etc.
11.	Object	IoT is mostly concerned about the objects which are embedded with the technology that can capture sensory movements.	AI doesn't specifically require objects.
12.	Scalability	Scalable being cloud-based.	Less scalable.
13.	Advantages	• Cost-effectiveness • Portable software • Allows you to stay connected. • Energy use is efficient • Extremely adaptable. • Very useful in the health care sector	• It manages the collaboration of humans and machines. • It keeps data in a logical order. • An excellent substitute for repetitious activities • Aids in the resolution of difficult problems.

S. No.	Based on	Internet of Things	Artificial Intelligence
			• It is useful for completing repeated activities. • Provide precise results • Low errors
14.	Disadvantages	• Increase worker drowsiness due to single-click work. • Unemployment rises. • Because we rely on computers and technology, less activity of human brains is there.	• AI is costly. • High reliance on machines • Humans are more inventive than artificial intelligence. • Storage is expensive.

IoT Conceptual Framework

The following equation describes a simple conceptual framework of IoT:

Physical object+Controller, Sensor and Actuators+Internet = Internet of Things

IoT consists of an internetwork of devices and physical objects wherein a number of objects can gather the data at remote locations and communicate to units for managing, acquiring, organizing and analyzing the data in the processes and services.

The equation below conceptually represents the actions and communication of data at successive levels in IoT consisting of internetworked devices and objects.

Gather + Enrich + Stream + Manage + Acquire + Organise and Analyse = Internet of Things with connectivity to data centre, enterprise or cloud server

The above equation is an IoT conceptual framework for the enterprise processes and services based on a suggested IoT architecture given by Oracle. The steps are as follows:

1. At level 1 data of the devices (things) using sensors or the things gather the pre data from the internet.

2. A sensor connected to a gateway, functions as a smart sensor(with computing and communication capacity). The data then enriches at level 2, for example by

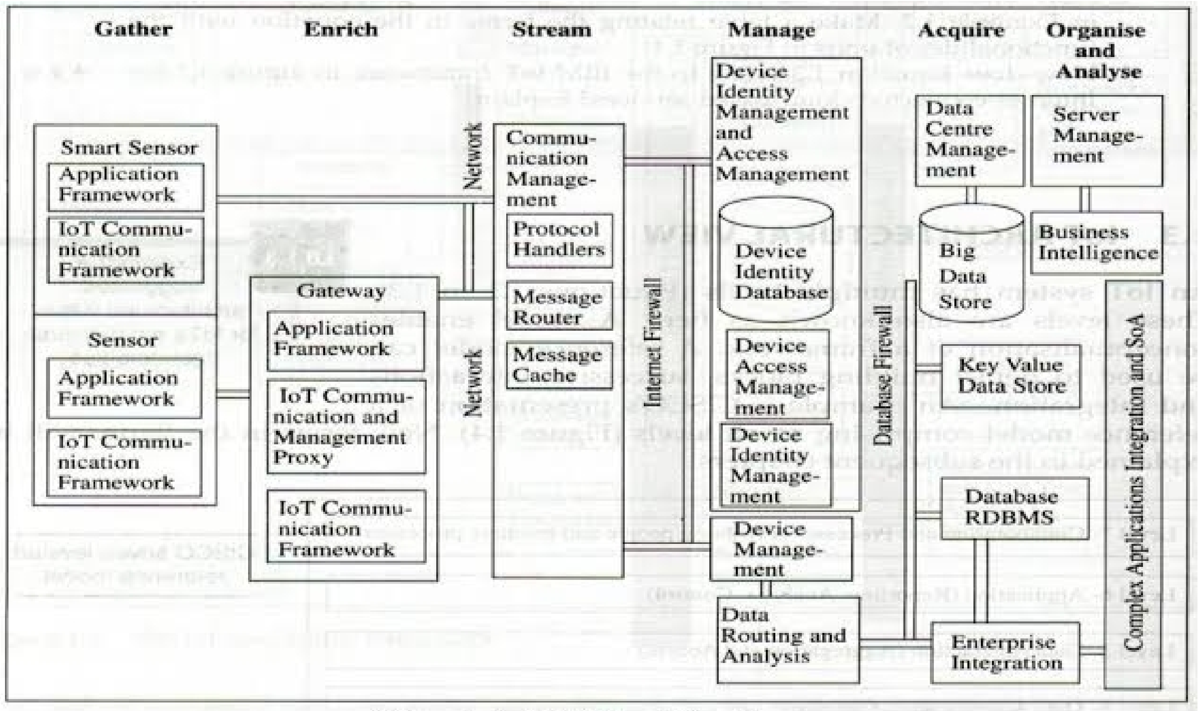
transcoding at the gateway. Transcoding means coding or decoding before data transfer between two entities.

3. A communication management subsystem sends or receives data streams at level3

4. Device management, identity management and access management subsystems receive the device's data at level 4.

5. A data store or database acquires the data at level 5.

6. Data routed from the devices and things organizes and analyses at level 6. For example, data is analyzed for collecting business intelligence in business processes.



The below equation which conceptualizes the general framework for IoT using the cloud based services is:

Gather + Consolidate + Connect + Collect + Assemble + Manage and Analyse = Internet of Things with connectivity to cloud services

Steps are as follows:

- **Level-1 Gather** :- information is gathered via device through via sensor and internet.
- **Level 2 Enrich** :- Gathered information is improved by process like transcoding (encoding and decoding) and act as a gateway between 2 devices .
- **Level 3 Stream** :- It includes the transmission and reception of data stream managed by communication subsistent.

- **Level 4 Managed** :- At this point the device data is received by device management and access management subsistent.
- **Level 5 Acquare :-** The information collected is stored in the data repository .
- **Level 6 organise and analyse :-** It is responsible for organising and analysis the data set by the object.

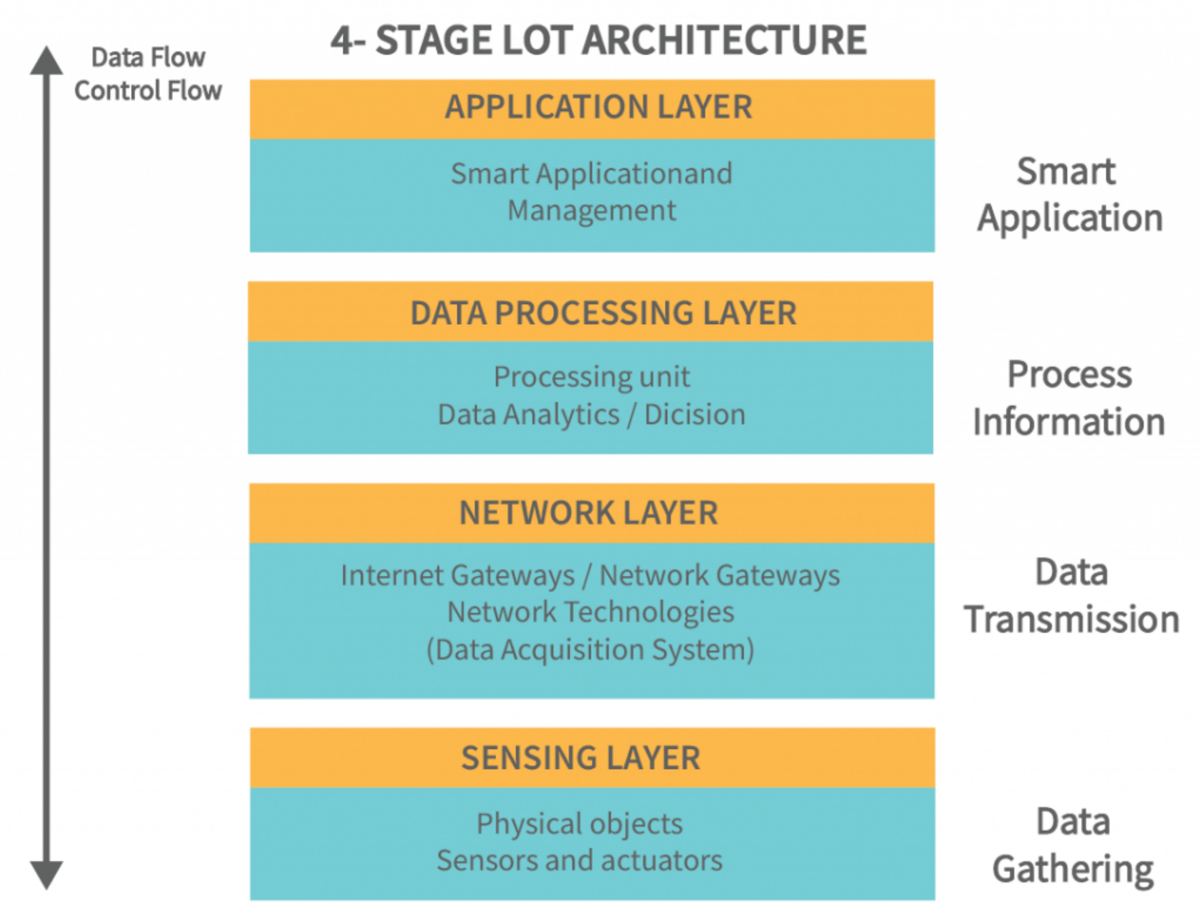
What is IoT Architecture?

The term IoT architecture refers to the framework which defines how various IoT elements (e.g., devices, networks, sensors, apps) interact within an IoT environment. Typically, IoT architecture consists of several layers and components which perform a variety of functions from physical devices, and data acquisition systems, to network devices communicating IoT data to data processing applications, and IoT data storage.

IoT architecture refers to the tangle of components such as sensors, actuators, cloud services, Protocols, and layers that make up IoT networking systems. In general, it is divided into layers that allow administrators to evaluate, monitor, and maintain the integrity of the system. The architecture of IoT is a four-step process through which data flows from devices connected to sensors, through a network, and then through the cloud for processing, analysis, and storage. With further development, the Internet of Things is poised to grow even further, providing users with new and improved experiences.

Different Layers of IoT Architecture

In recent years, IoT technology has grown in popularity and it has a large variety of applications. IoT applications operate according to how they have been designed/developed based on the different application areas. However, there is no standard defined architecture of work that is strictly adhered to across the board. The complexity and number of architectural layers vary according to the specific business task at hand. A four-layer architecture is the standard and most widely accepted format.



Perception/Sensing Layer

The first layer of any IoT system involves "things" or endpoint devices that serve as a conduit between the physical and the digital worlds. Perception refers to the physical layer, which includes sensors and actuators that are capable of collecting, accepting, and processing data over the network. Sensors and actuators can be connected either wirelessly or via wired connections. The architecture does not limit the scope of its components nor their location.

The sensing layer is the first layer of the Internet of Things architecture and is responsible for collecting data from different sources. This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters. Wired or wireless communication protocols connect these devices to the network layer.

Network Layer

Network layers provide an overview of how data is moved throughout the application. This layer contains Data Acquiring Systems (DAS) and Internet/Network gateways. A DAS performs data aggregation and conversion functions (collecting and aggregating data from sensors, then converting analog data to digital data, etc.). It is necessary to transmit and process the data collected by the sensor devices. That's what the network layer does. It allows these devices to connect and communicate with other servers, smart devices, and network devices. As well, it handles all data transmissions for the devices.

The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system. It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet. Examples of network technologies that are commonly used in IoT include WiFi, Bluetooth, Zigbee, and cellular networks such as 4G and 5G technology. Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wider internet, and may also include security features such as encryption and authentication to protect against unauthorized access.

Processing Layer

The processing layer is the brain of the IoT ecosystem. Typically, data is analyzed, pre-processed, and stored here before being sent to the data center, where it is accessed by software applications that both monitor and manage the data as well as prepare further actions. This is where Edge IT or edge analytics enters the picture.

This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action. The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms. These tools are used to extract meaningful insights from the data and make decisions based on that data.

Application Layer

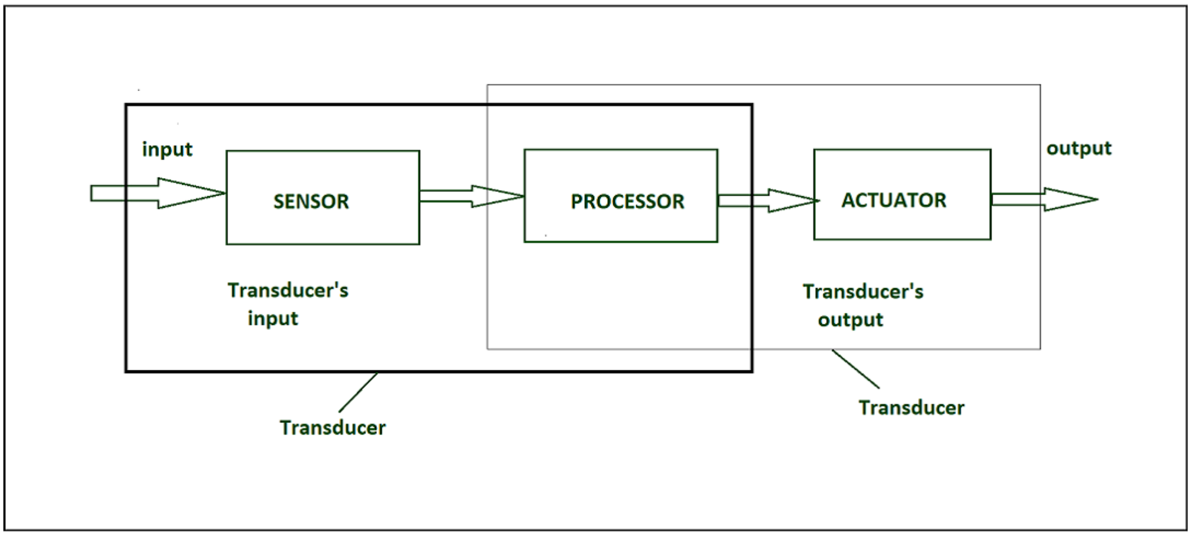
User interaction takes place at the application layer, which delivers application-specific services to the user. An example might be a smart home application where users can turn on a coffee maker by tapping a button in an app or a dashboard that shows the status of the devices in a system. There are many ways in which the Internet of Things can be deployed such as smart cities, smart homes, and smart health.

It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices.This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure.

Sensor

Sensor is a device used for the conversion of physical events or characteristics into the electrical signals. This is a hardware device that takes the input from environment and gives to the system by converting it. For example, a thermometer takes the temperature as physical characteristic and then converts it into electrical signals for the system.

Sensors play an important role in IoT which will make an ecosystem for collecting, analyzing, and processing data about a specific environment so that it can be monitored, managed, and controlled more easily and efficiently. Sensors bridge the gap between the physical world and the logical world.



Transducer : It converts the signal from one physical form to another physical form. it is also called energy converter. For example, microphone converts sound to electrical signal . It is based on the principle of conservation of energy.

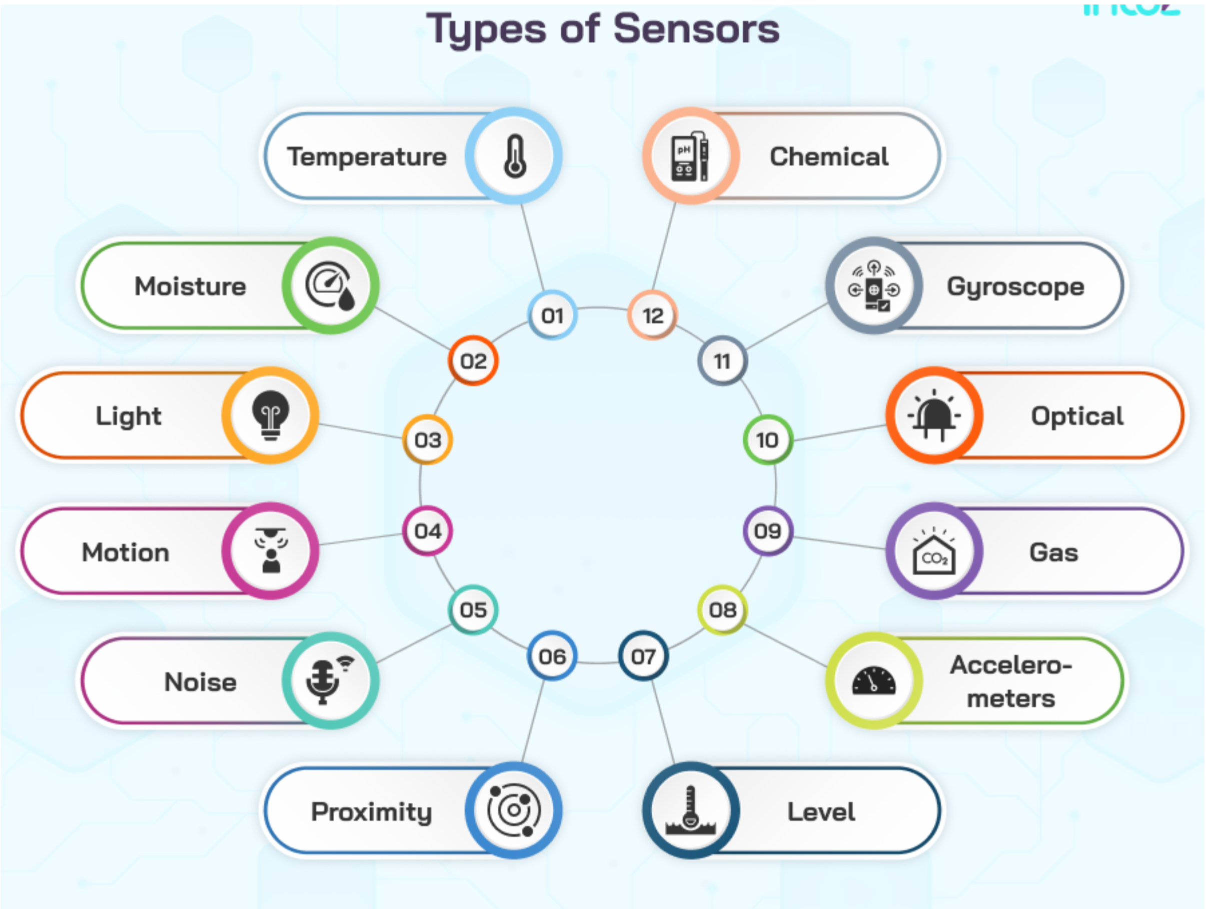
Classification of Sensors

The Sensor can be classified as

Based on Power Requirement

- **Active Sensors:** These Sensors require an external excitation signal or power source to work.
- **Passive Sensors**: These Sensors do not require any external power source and it can directly generate the output response.

Types of Sensors



1. Temperature: Beginning with the most common type of sensor, the temperate sensor records the amount of heat in a given setting. It can be a machine, a room, a car, a lab, etc. This information can be used to take the desired action, like changing the temperature to optimal settings. The same can be automated according to some specific environmental conditions and settings.

2. Moisture: Where temperature sensors record the heat, moisture sensors record the amount of humidity. They have a wide array of applications in the environment, food supply chains, medicinal labs, agriculture, etc. Moisture sensors either have a hair tension moisture element or a psychrometer to record the moisture content.

3. Light: Light sensors record and assess the ambient light settings in a defined area and recommend actions to change the same. In your smartphone, when the brightness is adjusted according to the exposure to light, the light sensor and the electrical actuator play their part. In the modern homes that have automated light settings, these sensors are used.

4. Motion: Motion sensors are usually installed in security systems and help detect unauthorized activity. Upon sensing activity either by changes in the heat or weight, the sensor activates an alarm system sending notifications to the right people. Motion IoT sensors use radar, infrared, or ultrasonic waves to detect activity in their vicinity.

5. Noise: Noise sensors, as the name suggests, record the noise levels in the given environment. It can be an entire city, a room, a car, etc. In IoT, these sensors are used to build safe working and living environments for people. They are also used to send warning notifications to the right people when noise levels go beyond the stipulated threshold limit.

6. Proximity: Motion sensors and proximity sensors can be kept in the same basket, as the majority of their functions are similar. These sensors record activity nearby with the help of electromagnetic waves, including infrared. They are used in cars, parking lots, retail stores, stadiums, airports, and in several other places to notify the people about their proximity to different components.

7. Level: From granular materials to semi-solid liquids, level sensors detect the quantity or level of different substances. Manufacturing industries, particularly beverage, water treatment, and waste management organizations, have the best use of level sensors.

8. Accelerometers: Accelerometers are an impressive type of IoT sensor used to record and measure an object's acceleration. These types of sensors record the rate of change of an object's speed in relation to time. Plus, they have the added advantage of recording changes in gravity. They can be popularly used in driving fleets and smart pedometers or to detect movement in a stationary object, helping to identify theft.

9. Gas: Gas sensors are used to detect changes in air quality. These sensors are built to detect the presence of toxic, combustible, and other hazardous gasses in a given area. Most of the time, we see the installation of this type of sensor in mining, oil, gas, and energy organizations. However, they are also installed in smart homes and buildings to detect levels of CO2, carbon monoxide, particulate matter, etc.

10. Optical: Optical sensors have several use cases but have become an important part of driverless cars. These sensors are used to detect signals and signs to provide information about the surrounding environment. In a driverless car, these sensors are used to detect objects and signs on the road, send the signals to the central control unit and dictate a change in behavior if required.

11. Gyroscope: These sensors are used to measure the velocity of a moving object. Velocity refers to the speed and rotation of an object around its axis. Gyroscope sensors are commonly used in car navigation systems and in stability control systems.

12. Chemical: We can put chemical sensors and gas sensors in the same category. With these sensors, we can expect measurements and detection of several types of chemicals. To build IoT solutions in a factory setting, these sensors can play an important role in ensuring workers' safety and that of the environment.

Based on Means of Detection

The Sensors can be according to detection method they use such as electrical, biological, chemical, or radioactive detection.

Based on the Conversion Phenomenon

This classification is based on the input and output conversion

- **Photoelectric**: It Changes light to electrical signals.
- **Thermoelectric:** It Changes temperature difference to electrical voltage.
- **Electrochemical**: It Changes chemical reactions to electrical signals.
- **Electromagnetic**: It Changes magnetic fields to electrical signals.
- **Thermoptic**: It Changes temperature changes to electrical signals.

Based on Output Type

- **Analog Sensors:** It produce an output signal which is usually in the form of voltage, current, or resistance, proportional to the measured quantity.
- **Digital Sensors**: It provide discrete or digital data as output.

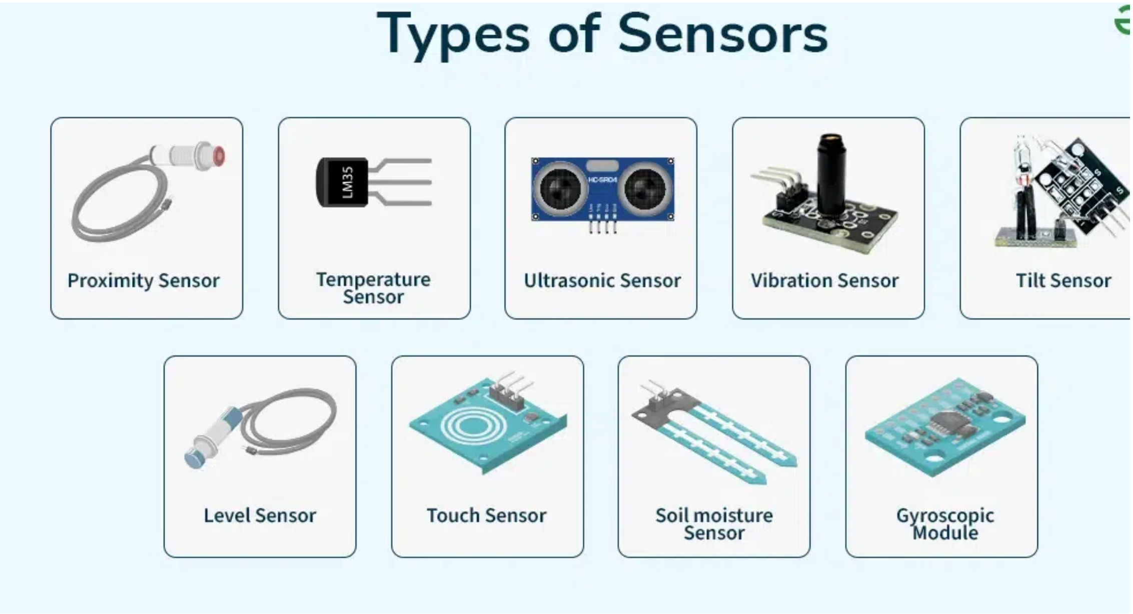
Types of Sensors

We live in the world of sensors, there are different types of sensors in our homes, offices, cars etc. by working to make our lives easier by turning on the lights by detecting our presence, adjusting the room temperature, detect smoke or fire, make us delicious coffee, and automatic door closing and so on. here we will discuss types of sensors one by one in detail:

- **Temperature sensors:** Monitoring temperature of used devices in industrial applications. it is used to measure temperature. this can be air temperature, liquid temperature or the temperature of solid. It can be analog or digital. In an **Analog Temperature Sensor**, the change in the Temperature correspond to change in its physical property like resistance or voltage.

- **Accelerometer sensors:** It measures the rate of change of velocity and this sensor generate magnitude and acceleration of the acceleration. it is used in car electronics, ships, and agricultural machines.
- **Alcohol sensors:** as the name suggests it detects alcohol. Usually, alcohol sensors are used in breathalyzer devices, which determine whether the person is drunk or not. Law enforcement personnel uses breathalyzers to catch drunk-and-drive culprits.
- **Radiation sensors:** Radiation Sensors/Detectors are electronic devices that sense the presence of alpha, beta, or gamma particles and provide signals to counters and display devices. Radiation detectors are used for surveys and sample counting.
- **Position sensors:** Position Sensors are electronic devices used to sense the positions of valves, doors, throttles, etc. and supply signals to the inputs of control or display devices. Key specifications include sensor type, sensor function, measurement range, and features that are specific to the sensor type. Position sensors are used wherever positional information is needed in a myriad of control applications. A common position transducer is a so-called string-pot, or string potentiometer.
- **Gas sensors:** It measures and detects concentration of different gases which is present in the atmosphere or any other environment.
- **Torque sensors:** This sensor is used for measuring the rotating torque and it is used to measure the speed of the rotation.
- **Optical sensors:** it is also called photosensors which can detect light waves at different points in the light spectrum including ultraviolet light, visible light, and infrared light. it is extensively used in smartphone, robotics and Blu-ray players.
- **Proximity sensors:** This sensor is used to detect the distance between two objects or detect the presence of an object. it is used in elevators, parking lots, automobiles, robotics, and numerous other environment.
- **Touch sensors:** Touch sensing devices detect physical contact on a monitored surface. Touch sensors are used extensively in electronic devices to support trackpad and touchscreen technologies. They're also used in many other systems, such as elevators, robotics and soap dispensers.
- **Image sensor:** it is used for distance measurement, pattern matching, color checking, structured lighting, and motion capture and it is also used

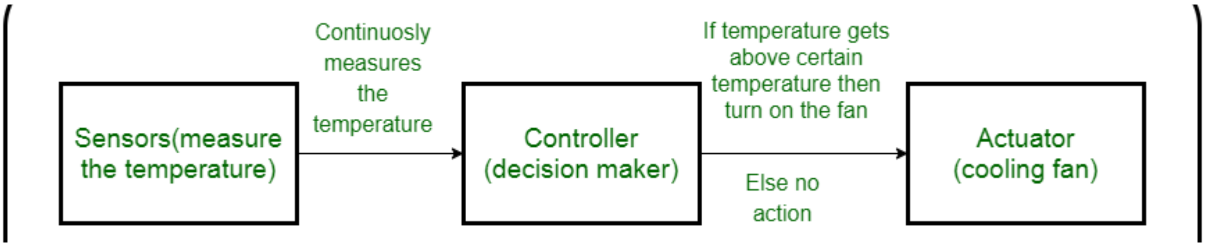
in different applications such as 3D imaging, video/broadcast, space, security, automotive, biometrics, medical, and machine vision.



Actuator

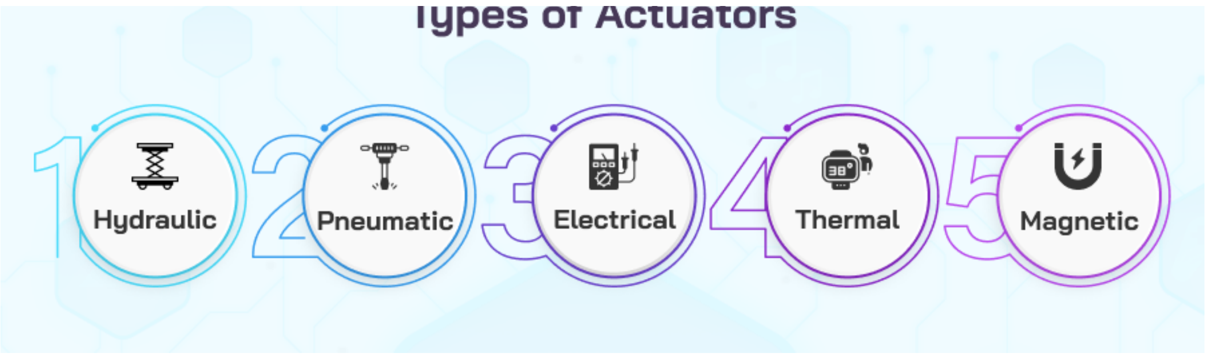
Actuator is a device that converts the electrical signals into the physical events or characteristics. It takes the input from the system and gives output to the environment. For example, motors and heaters are some of the commonly used actuators.

he following diagram shows what actuators do, the controller directs the actuator based on the sensor data to do the work.


Sensors(measure the temperature)
Continuosly measures the temperature
Controller (decision maker)
If temperature gets above certain temperature then turn on the fan
Else no action
Actuator (cooling fan)

The control system acts upon an environment through the actuator. It requires a source of energy and a control signal. When it receives a control signal, it converts the source of energy to a mechanical operation.

Types of Actuators



1. Hydraulic: These actuators harness hydraulic power to perform mechanical functions and operations. Generally, these types of actuators are powered by a cylinder or a fluid motor. According to the requirements and recommendations, the mechanical motion is converted into oscillatory, linear, or rotary.

2. Pneumatic: Pneumatic actuators create two types of motions, rotary or linear. They are powered by a vacuum or compressed air at high pressure to implement the required type of motion. Compared to other types of actuators, pneumatic actuators are low-cost and low-maintenance actuators.

3. Electrical: In these actuators, a motor converts electrical energy into mechanical motion. These actuators are powered by electricity and provide precision control. These actuators are heavily used in industrial settings to automate mechanical operations.

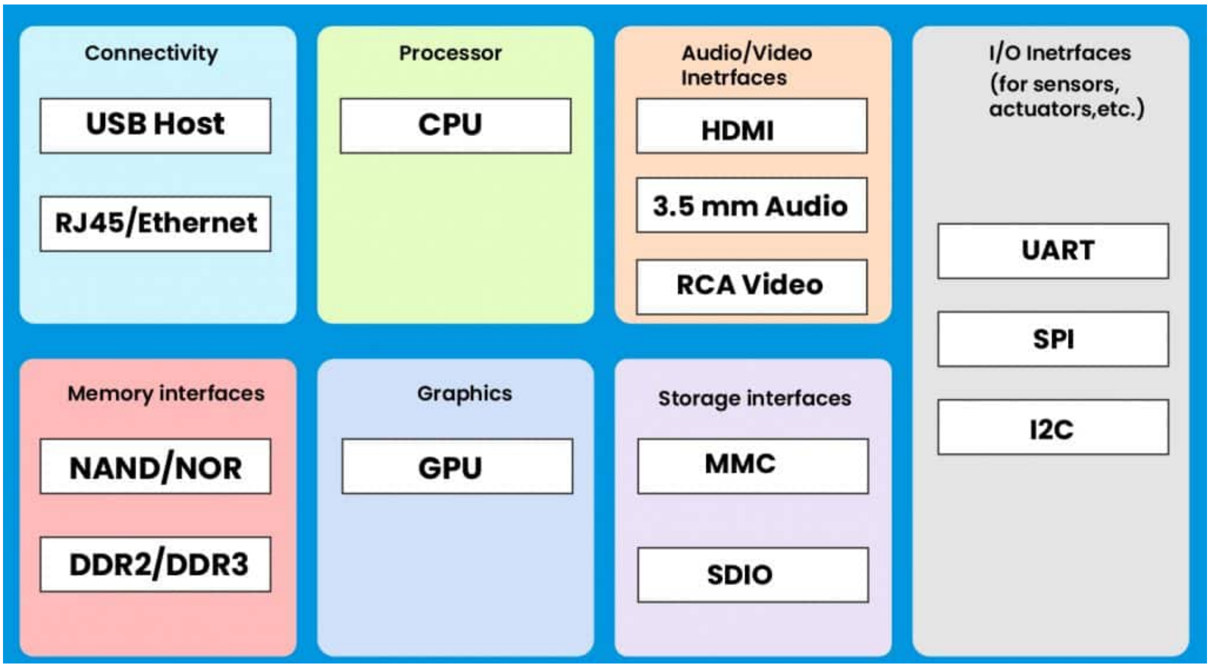
4. Thermal: The thermal actuators have thermal-sensitive material fitted inside, which is used to produce linear motion. The word thermal implies that these actuators are used in response to temperature changes. The most popular use case includes shutting off valves and operating latches or switches.

5. Magnetic: These types of actuators convert electromagnetic energy into mechanical output and operate in a linear or rotary direction. Magnetic actuators can provide continuous mechanical operation and are popularly used in the automotive and aerospace industries.

Where IoT is shaping the new face of the industry, sensors and actuators are used to provide the required infrastructure for building a robust industry. They are essential in almost every industrial function helping organizations achieve streamlined output and higher productivity powered by automation.

The key to harnessing their potential is identifying the correct type of IoT sensors and installing them to manage and control mechanical operations.

Physical Designs of IoT



Connectivity: Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

Processor: A processor like a CPU and other units are used to process the data. these data are further used to improve the decision quality of an IoT system.

Audio/Video Interfaces: An interface like HDMI and RCA(Root Cause Analysis," which is a systematic method used to identify the underlying cause of a problem or malfunction within an IoT system, allowing for targeted solutions and preventative measures to be implemented) devices is used to record audio and videos in a system.

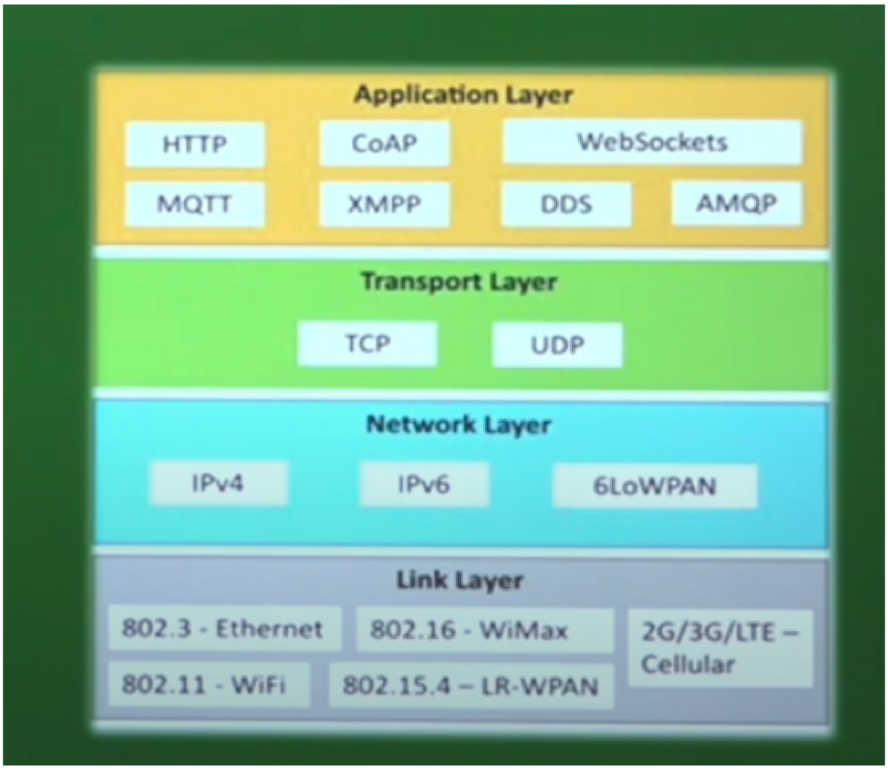
Input/Output interface: To give input and output signals to sensors, and actuators we use things like UART(Universal Asynchronous Receiver/Transmitter), SPI(Serial Peripheral Interface), CAN(Controller Area Network), etc.

Storage Interfaces: Things like SD(Secure Digital), MMC(MultiMediaCard), and SDIO are used to store the data generated from an IoT device.

Other things like DDR(double data rate, a type of computer memory technology that increases the speed of data transfer between the memory and the processor) and GPU(graphics processing unit) is a specialized electronic circuit that processes graphics and performs mathematical calculations. GPUs are used in many applications, including gaming, video editing, and machine learning.) are used to control the activity of an IoT system.

IoT Protocols

These protocols are used to establish communication between a node device and a server over the internet. it helps to send commands to an IoT device and receive data from an IoT device over the internet. we use different types of protocols that are present on both the server and client side and these protocols are managed by network layers like application, transport, network, and link layer.



Application Layer protocol

In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface. these protocols include HTTP, WebSocket, XMPP, MQTT, DDS, and AMQP protocols.

HTTP

Hypertext transfer protocol is a protocol that presents in an application layer for transmitting media documents. it is used to communicate between web browsers and servers. it makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between the two requests.

CoAP (Constrained Application Protocol)

CoAP or Constrained Application Protocol, as the name suggests, is an application layer protocol that was introduced by the Internet Engineering Task Force in the year 2014. CoAP is designed for the constrained environment. It is a web-based protocol that resembles HTTP. It is also based on the request-response model.

Designed to address the needs of HTTP-based IoT systems, CoAP relies on the User Datagram Protocol (UDP) for establishing secure communication between endpoints. By allowing for broadcasting and multicasting, UDP is able to transmit data to multiple hosts while retaining communication speed and low bandwidth usage, which makes it a good match for wireless networks typically employed in resource-constrained M2M environments.

This being said, the communication process between devices would be able to occur without needing any connection to be established prior.

Applications of CoAP

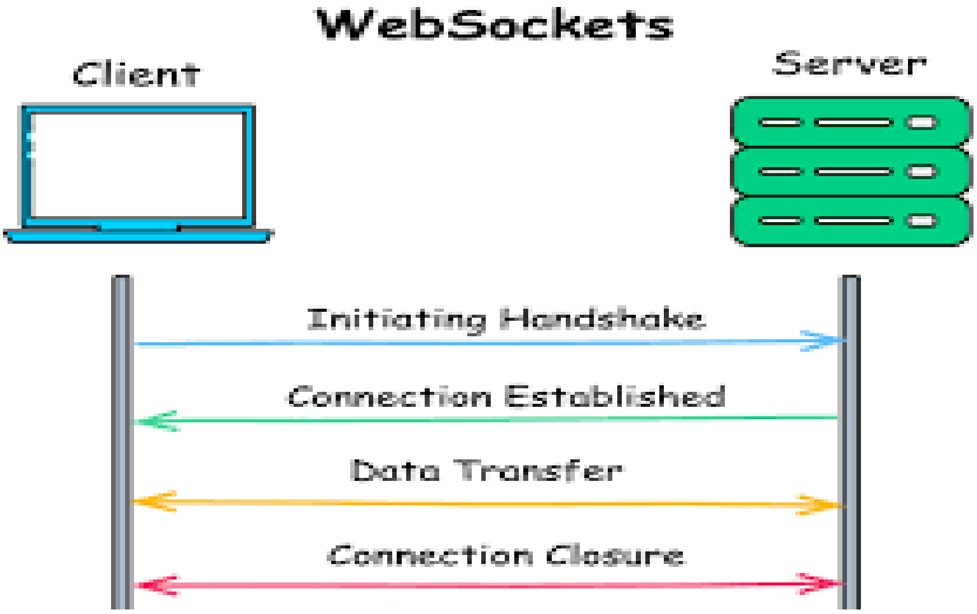
- **Real Time Monitoring in Grid -** Smart cities can monitor the distribution and generation of power remotely. The CoAP sensors could be embedded inside the transformers and the data could be transferred over GPRS or 6LowPAN.
- **Defense utilities -** The armory and tanks are now-a-days fitted with sensors so that information could be communicated remotely without any interference. The CoAP sensors could detect any intrusion. This makes them capable to transfer more data even under low bandwidth network.
- **Aircraft utilities -** The Aircraft sensors and actuators could be connected with other sensors and communication can take place using smart CoAP based sensors and actuators.

WebSocket

This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. This protocol is commonly used by web browsers.

How it works

- WebSocket uses a TCP connection to create a persistent connection between a client and a server
- The client and server use an HTTP/HTTPS handshake to establish a connection
- The client sends an Upgrade: websocket header, and the server responds with 101 Switching Protocols
- The WebSocket protocol supports text and binary data formats



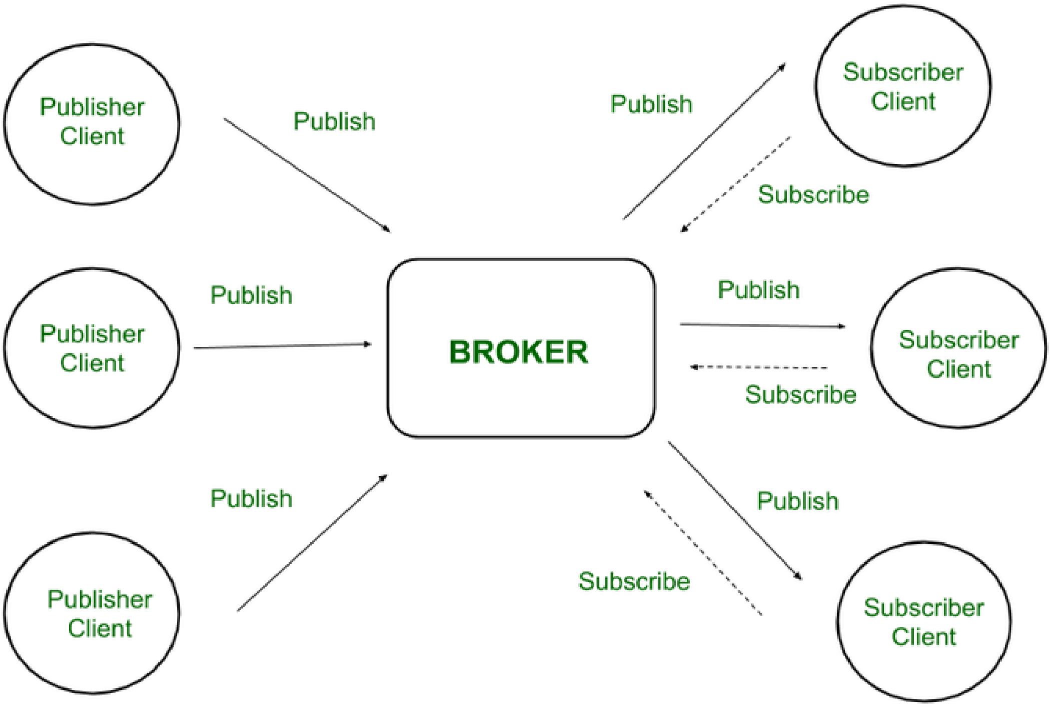
MQTT

Developed as an open OASIS standard and an ISO recommended protocol, the MQTT was aimed to operate on data transmissions with a small bandwidth and minimum resources (e.g. on microcontrollers). It usually uses the TCP/IP protocol suite, which runs by first establishing connections, then allows multiple exchanges of data until one party finally disconnects itself.

The MQTT technology runs using the MQTT Publish/Subscribe architecture and establishes the network from 2 different component categories: Clients (Publisher and Subscriber) and Brokers.

The Publish/Subscribe architecture first divides the network's client devices into 2 categories, publishers and subscribers. These publishers are devices or nodes that input data to the system. On the other hand, the subscribers are the end devices or nodes that receive the data.

The data sent are in the form of different topics, in which the broker sorts the topic sent from the publisher, and sends it out to the appropriate client which has previously subscribed to the said topic.

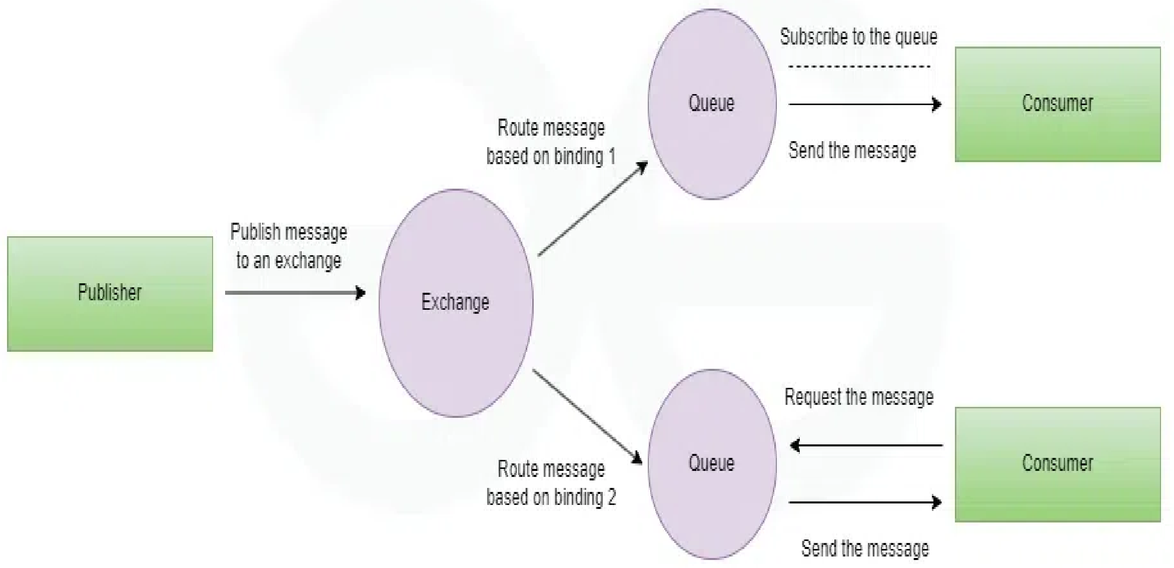


AMQP (Advanced Message Queueing Protocol)

AMQP (Advanced Message Queuing Protocol) and HTTP (Hypertext Transfer Protocol) are two communication protocols used in distributed systems, however, they perform different functions and have different properties. In this article, we are going to discuss the differences between AMQP and HTTP protocols.

What is AMQP?

AMQP is an acronym used for the Advanced Message Queuing Protocol. It is a protocol that is used for communication between applications. It is a lightweight, protocol that supports the applications for data transfer. This protocol is used for its scalability and modularity with the technologies.



Components of AMQP

- **Exchanges: The exchange** is responsible for fetching messages and properly arranging them in the appropriate queue
- **Channel:** A channel is a multiplexed virtual connection between AMQP peers that is built into an existing connection.
- **Message Queue:** It is a unique entity that connects messages to their resources or points.
- **Binding:** Bindings are a set of predetermined instructions for queuing and exchanging. It manages message transmission and delivery.
- **Virtual Host:** Vhost is a platform that provides isolation capabilities within the broker. Multiple vhosts may be functional at the same time, depending on the users and their access rights.

XMPP (Extensible Messaging and Presence Protocol)

XMPP, developed in the year 1999, is an open-source protocol that was based on XML (Extensive Markup Language). Hence, it supports rapid structured data exchange between two or more network entities and enables the addition of extension for operation.

XMPP is a short form for Extensible Messaging Presence Protocol. It’s protocol for streaming XML elements over a network in order to exchange messages and present information in close to real-time.

Let’s dive into each character of word **XMPP**:

- **X :** It means eXtensible. XMPP is an open-source project which can be changed or extended according to the need.
- **M :** XMPP is designed for sending messages in real time. It has very efficient push mechanism compared to other protocols.
- **P :** It determines whether you are online/offline/busy. It indicates the state.
- **P :** XMPP is a protocol, that is, a set of standards that allow systems to communicate with each other.

The structure of an XMPP network is very similar to that of an email, giving the protocol its decentralized property. This means that anyone could establish their own server with the protocol anywhere.

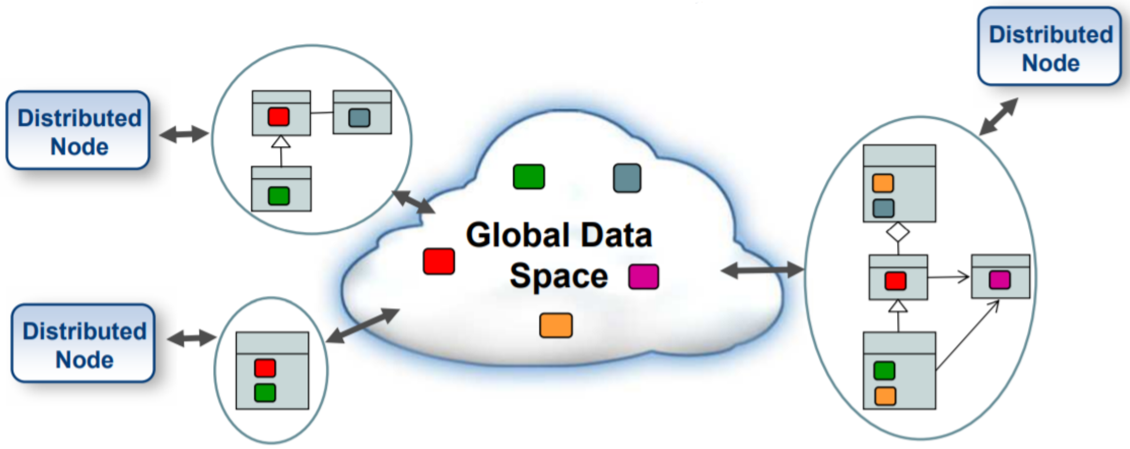
The XMPP protocol is used commonly for instant messaging purposes, including voice and video calls, multi-person chats, etc.

However, the protocol also serves IoT function properly as it's flexible for connection protocols, secure, and enables middleware communication without requiring human intervention. A few applications of IoT with XMPP include the Google Cloud Print and Logitech Harmony Hub (home automation and media control).

DDS (Data Distribution Service)

DDS is the first open interoperable middleware protocol, developed by the Object Management Group (OMG). Its operation claims to provide a secure and real-time data distribution. Like MQTT, DDS works in a Publisher/Subscriber architecture. However, the protocol doesn't implement the use of Brokers together with its Clients, hence its topic distribution occurs across its Global Data Space (GDS) by applying a QoS (Quality of Service) contract system.

The GDS acts as a 'memory' during DDS transmission application. However, it's actually not a physical memory in the DDS server, it's just a virtual concept. The GDS is actually the combination of local stores in nodes connected to the system.



Transport Layer

This layer is used to control the flow of data segments and handle error control. also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP

The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.

UDP

a user datagram protocol is a part of an internet protocol called the connectionless protocol. this protocol is not required to establish the connection to transfer data.

Network Layer

This layer is used to send datagrams from the source network to the destination network. we use IPv4 and IPv6 protocols as host identification that transfers data in packets.

IPv4

This is a protocol address that is a unique and numerical label assigned to each device connected to the network. an IP address performs two main functions host and location addressing. IPv4 is an IP address that is 32-bit long.

IPv6

It is a successor of IPv4 that uses 128 bits for an IP address. it is developed by the IETF task force to deal with long-anticipated problems.

Link Layer

Link-layer protocols are used to send data over the network's physical layer. it also determines how the packets are coded and signaled by the devices.

Ethernet

It is a set of technologies and protocols that are used primarily in LANs. it defines the physical layer and the medium access control for wired ethernet networks.

WiFi

It is a set of LAN protocols and specifies the set of media access control and physical layer protocols for implementing wireless local area networks.

Logical Design of IoT

A logical design for an IoT system is the actual design of how its components (computers, sensors, and actuators) should be arranged to complete a particular function. It doesn't go into the depth of describing how each component will be built with low-level programming specifics.

IoT systems include several functional blocks such as Devices, communication, security, services, and application.

The functional blocks provide sensing, identification, actuation, management, and communication capability. These functional blocks consist of devices that handle the communication between the server and the host, enable monitoring control functions, manage the data transfer, secure the IoT system using authentication and different functions, and provide an interface for controlling and monitoring various terms.

The **Functional blocks** are:

Device: An IoT system comprises of devices that provide sensing, actuation, monitoring, and control functions.

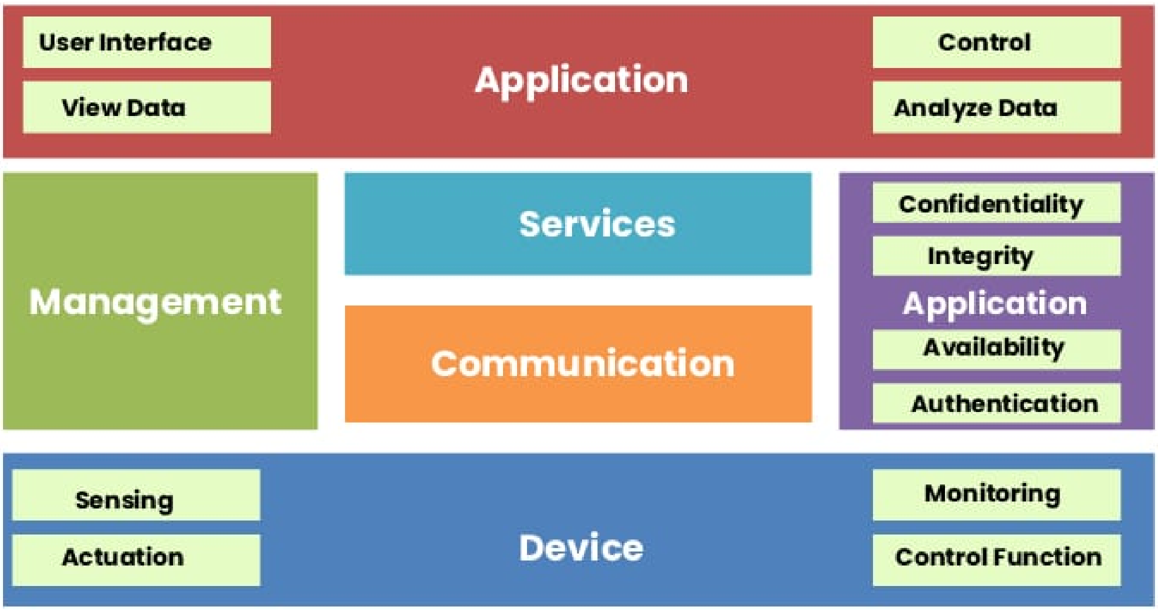
Communication: Handles the communication for the IoT system.

Services: services for device monitoring, device control service, data publishing services, and services for device discovery.

Management: this block provides various functions to govern the IoT system.

Security: This block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and data security.

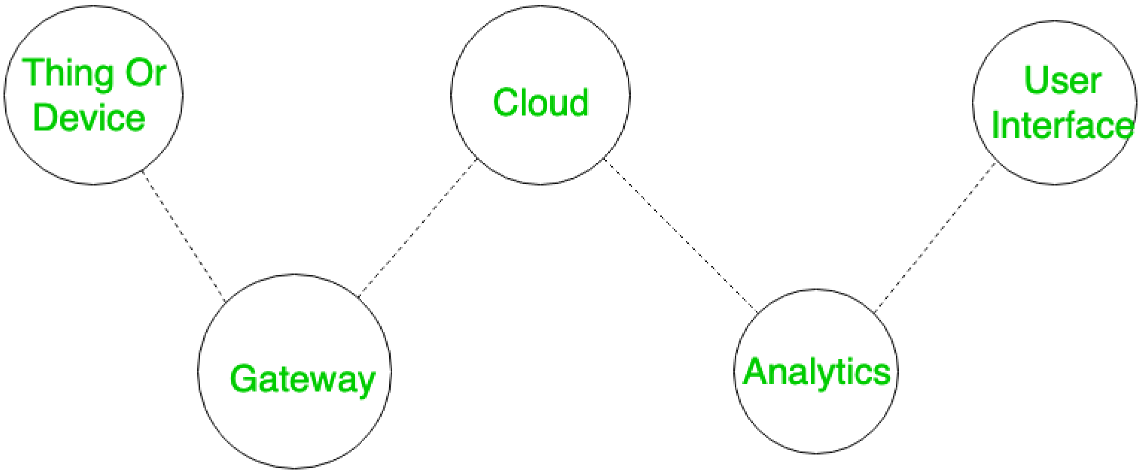
Application: This is an interface that the users can use to control and monitor various aspects of the IoT system. The application also allows users to view the system status and view or analyze the processed data.



Physical Designs of IoT	Logical Designs of IoT
It provide an elaborate and detailed overview	It provide a high level overview which is brief
It emphasizes the configuration and assembling of any specific entity.	It emphasizes the design factors which include the assumptions, requirement, onstrainsts, and risk.
It contains more graphic content than textual content	It comprises both, the textual as well as the graphic content.

Components of IOT

Major Components of IOT:
These are explained as following below.



Major Components of IOT

1. **Things or Device Sensors or Devices**
   These are fitted with sensors and actuators. Sensors collect data from the environment and give to gateway where as actuators performs the action (as directed after processing of data).

   Sensors or Devices are basically used to collect and transmit the data and also perform actions based on those data. For example, the sensors can be used for measuring temperature and humidity. There are different types of sensors; here are as follows: Temperature Sensors, Humidity Sensors, Proximity Sensors, Motion Sensors, Light Sensors, Pressure Sensors, Gas Sensors, and GPS Sensors

2. **Gateway**
   The sensors give data to Gateway and here some kind of pre-processing of data is even done. It also acts as a level of security for the network and for the transmitted data.

   Gateway is also a device component that basically acts as an intermediate between the sensors and the central cloud. Gateway is one of the essential components of IoT that offers communication, management, and data processing. Here are some of the functions of Gateway in IoT: Data Aggregation, Communication, Security, Protocol Translation, Load Balancing, and Latency Reduction.

3. **Cloud**
   The data after being collected is uploaded to cloud. Cloud in simple terms is basically a set of servers connected to internet 24*7.

Cloud in IoT refers to the service that provides the management, storage, and processing of the data that is generated by IoT (Internet of Things) devices. Here are some key aspects of Cloud in IoT: Data Storage, Data Collection, Security, Connectivity, Integration, and Cost Efficiency.

4. **Analytics**
   The data after being received in the cloud processing is done . Various algorithms are applied here for proper analysis of data (techniques like Machine Learning etc are even applied).

   This is the crucial component of IoT that basically harness the potential of IoT. In analytics, meaningful insights are analyzed that are generated by IoT devices and sensors. There are some functions included in Analytics, such as data processing, machine learning, and statistical analysis. Here are some of the applications of analytics in IoT: Anomaly Detection, Environmental Monitoring, Energy Management, Smart Cities, and Agriculture.

5. **User Interface**
   User end application where user can monitor or control the data. User Interface, also known as UI in the Internet of Things (IoT) and provides an interface by which the users can interact with the applications and systems. Here are some of the key points in the user interface of IoT (Internet of Things): Data Visualization, User-Friendly Design, Personalization, Remote Management, Integration, Authentication, and Security.

Technology Behind IOT

Sensors and Actuators

- Sensors collect data from the environment, such as temperature, humidity, motion, or light.
- Actuators perform actions based on the data received from sensors or user commands

Connectivity

- Wireless protocols like Wi-Fi, Bluetooth, Zigbee, and cellular networks
- (4G/5G) enable devices to connect and communicate with each other and the internet.
- Wired connections, such as Ethernet, are also used in some IoT applications.

Communication Protocols

- Lightweight communication protocols like **MQTT (Message Queuing Telemetry Transport)** and
- **CoAP (Constrained Application Protocol)** are used for efficient data transfer between devices.
- These protocols are designed to work well with limited bandwidth and power-constrained devices.

Edge Computing

- Edge computing brings data processing closer to the source (IoT devices) to reduce latency and improve real-time decision-making.
- It allows for local data analysis and filtering before sending relevant information to the cloud.

Cloud Platforms

- Cloud platforms, such as **Amazon Web Services (AWS), Microsoft Azure, and Google Cloud,**
- provide scalable infrastructure for storing, processing, and analyzing IoT data.
- They offer IoT-specific services for device management, data ingestion, and analytics.

Integration and Interoperability

- **Middleware platforms and APIs** facilitate integration between diverse IoT devices, protocols, and applications,
- ensuring interoperability and seamless data exchange.
- **Example:** An IoT middleware platform translates data from different sensors into a common format for analytics and decision-making.

Sources of IoT

The Internet of Things (IoT) relies on various sources and technologies to enable connectivity, data exchange, and automation.

Wi-Fi

- Wi-Fi technology allows IoT devices to connect to local area networks (LANs) and the internet wirelessly,

- providing high-speed data transmission and connectivity within a certain range.
- **Example**: Smart home devices like cameras, and speakers connect to Wi-Fi networks for remote control and data sharing.

Bluetooth

- Bluetooth technology enables short-range wireless communication between IoT devices, s
- martphones, and accessories,facilitating seamless data transfer and device pairing.
- **Example:** Wearable fitness trackers use Bluetooth to sync data with mobile apps for activity tracking and analysis.

Zigbee and Z-Wave

- These low-power wireless protocols are commonly used in smart home automation for creating mesh networks,
- allowing devices to communicate efficiently with minimal energy consumption.
- **Example:** Smart lighting systems use Zigbee or Z-Wave to control and coordinate multiple light bulbs in a home network.

Cellular Networks

3G/4G/5G

- Cellular networks provide IoT devices with wide-area connectivity,
- allowing them to transmit data over long distances using cellular infrastructure and SIM cards.
- **Example:** GPS trackers for vehicles use cellular networks to send real-time location data to fleet management systems.

Satellite Communication

- In remote or rural areas with limited terrestrial connectivity, satellite internet service**s enable IoT devices to access the internet and communicate globally.**
- **Example:** Environmental monitoring systems in remote regions use satellite communication to transmit weather data and alerts.

Machine-to-Machine (M2M) Communication

- M2M means no human intervention .
- It is a direct communication system between device using wired and wireless communication without human intervention.
- It collects and share it with other machine .
- for eg Controlling air condition with a smartphone using bluetooth we are in home so on internet is required thi is M2M when we control from a far distance over internet is called IOT .

Internet of Things (IoT) Enabling Technologies

1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

1. Wireless Sensor Network(WSN) :
A **WSN** comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.
Example –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

2. Cloud Computing :
It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.
With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.
Characteristics –

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

Provides different services, such as –

- **IaaS (**Infrastructure as a service**)**
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.
  Ex : Web Hosting, Virtual Machine etc.

- **PaaS (**Platform as a service**)**
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.
  Ex : App Cloud, Google app engine

- **SaaS (**Software as a service**)**
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.
  SaaS Applications are sometimes called web-based software on demand software or hosted software.
  SaaS applications run on a SaaS provider's service and they manage security availability and performance.
  Ex : Google Docs, Gmail, office etc.

3. Big Data Analytics :
It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.
Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.
Several steps involved in analyzing big data –

1. Data cleaning

2. Munging
3. Processing
4. Visualization

Examples –

- Bank transactions
- Data generated by IoT systems for location and tracking of vehicles
- E-commerce and in Big-Basket
- Health and fitness data generated by IoT system such as a fitness bands

4. Communications Protocols :
They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.
They are used in

1. Data encoding
2. Addressing schemes

5. Embedded Systems :
It is a combination of hardware and software used to perform special tasks.
It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).
It collects the data and sends it to the internet.
Embedded systems used in
Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

Types of Communications in IOT

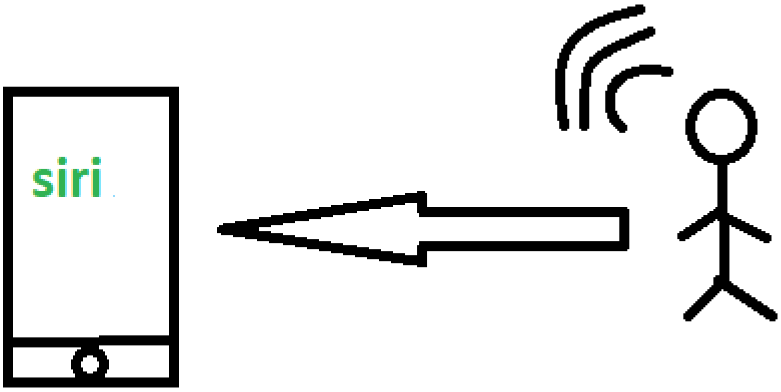
IoT Communication: IoT is the connection of devices over the internet, where these smart devices communicate with each other , exchange data , perform some tasks without any human involvement. These devices are embedded with electronics, software, network and sensors which help in communication. Communication between smart devices is very important in IOT as it enables these devices to gather, exchange data which contribute in success of that IOT product/project.

Types of Communications in IOT:

The following are some communication types in IoT:-

1. Human to Machine (H2M):

In this human gives input to IOT device i.e as speech/text/image etc. IOT device (Machine) like sensors and actuators then understands input, analyses it and responds back to human by means of text or Visual Display. This is very useful as these machines assist humans in every everyday tasks. It is a combo of software and hardware that includes human interaction with a machine to perform a task.



H2M communication

Merits: This H2M has a user-friendly interface that can be quickly accessed by following the instructions. It responds more quickly to any fault or failure. Its features and functions can be customized.

Examples:

- Facial recognition.
- Bio-metric Attendance system.
- Speech or voice recognition.

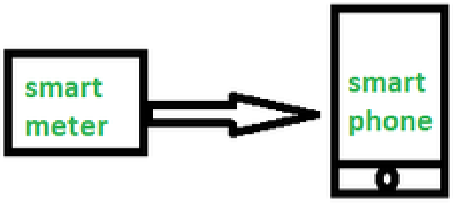
2. Machine to Machine (M2M):

The process of exchanging information or messages between two or more machines or devices is known as Machine to Machine (M2M) communication.

It is the communication among the physical things which do not need human intervention.

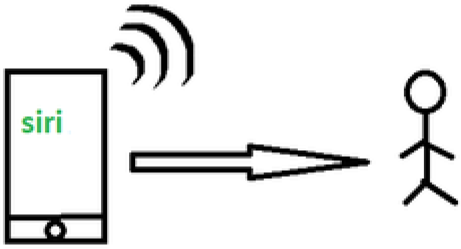
In this the interaction or communication takes place between machines by automating data/programs.

At this machine level instructions are required for communication. Here communication takes place without human interaction. The machines may be either connected through wires or by wireless connection. An M2M connection is a point-to-point connection between two network devices that helps in transmitting information using public networking technologies like Ethernet and cellular networks. IoT uses the basic concepts of M2M and expands by creating large "cloud" networks of devices that communicate with one another through cloud networking platforms.



3. Machine to Human (M2H) :

In this machine interacts with Humans. Machine triggers information(text messages/images/voice/signals) respective / irrespective of any human presence. This type of communication is most commonly used where machines guide humans in their daily life. It is way of interaction in which humans co-work with smart systems and other machines by using tools or devices to finish a task.



Examples:

- Fire Alarms
- Traffic Light
- Fitness bands
- Health monitoring devices

How does M2M work?

M2M technology taps into sensor data collected by devices and transmits it over a network. Unlike traditional remote monitoring tools, M2M systems commonly employ public networks such as cellular or Ethernet connections, which makes the technology more cost-effective.

Key components of an M2M system include sensors, radio frequency identification (RFID), a Wi-Fi or cellular communications link, and autonomic computing software that interprets data and triggers preprogrammed automated actions.

M2M applications and examples

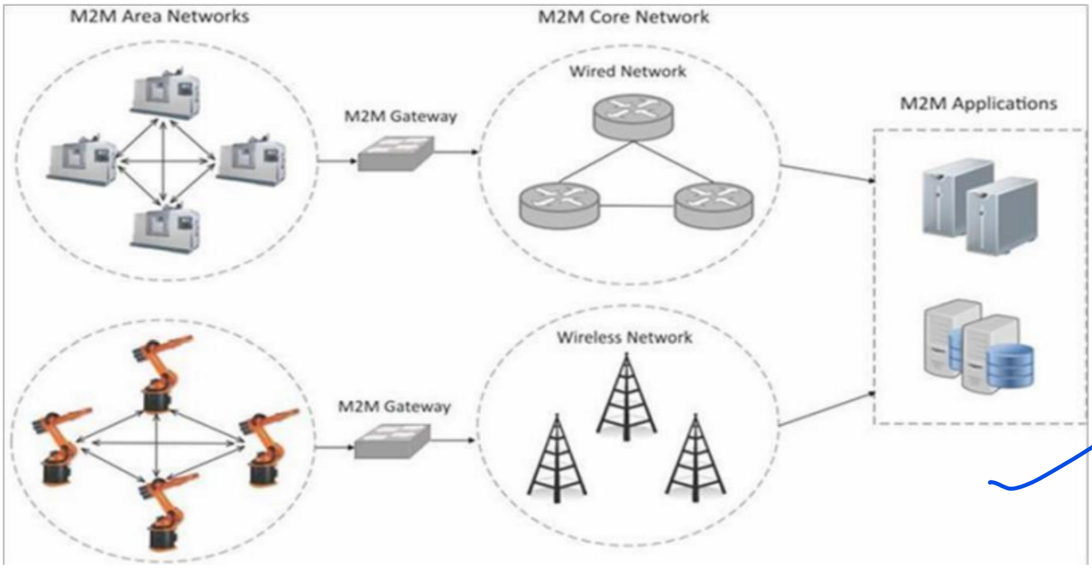
Machine-to-machine communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor's network, or *machine*, when a particular item is running low to send a refill. An enabler of asset tracking and monitoring, M2M is vital in warehouse management systems (WMS) and supply chain management (SCM).

IoT and M2M

Machine-to-Machine (M2M) refers to networking of machines(or devices) for the purpose of remote monitoring and control and data exchange.

• Term which is often synonymous with IoT is Machine-to-Machine (M2M).

• IoT and M2M are often used interchangeably. Fig. Shows the end-to-end architecture of M2M systems comprises of M2M area networks, communication networks and application domain.



- An M2M area network comprises of machines(or M2M nodes) which have embedded network modules for sensing, actuation and communicating various communication protocols can be used for M2M LAN such as ZigBee, Bluetooth, M-bus, Wireless M-Bus etc., These protocols provide connectivity between M2M nodes within an M2M area network.

- The communication network provides connectivity to remote M2M area networks. It can use either wired or wireless networks (IP-based). While M2M networks use proprietary or non-IP-based communication protocols, the communication network uses IP-based networks. Since non-IP-based protocols are used within M2M area networks, the M2M nodes within one network cannot communicate with nodes in an external network.
- To enable the communication between remote M2M are network, M2M gateways are used.

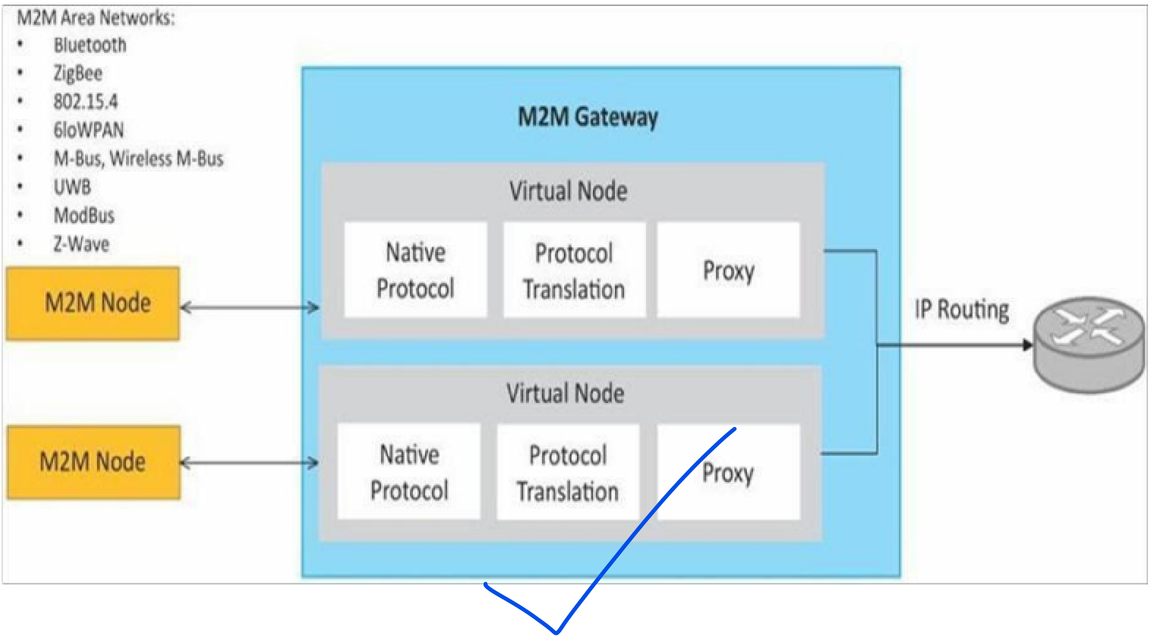


Fig. Shows a block diagram of an M2M gateway. The communication between M2M nodes and the M2M gateway is based on the communication protocols which are naive to the M2M are network. M2M gateway performs protocol translations to enable Ip-connectivity for M2M are networks. M2M gateway acts as a proxy performing translations from/to native protocols to/from Internet Protocol(IP). With an M2M gateway, each mode in an M2M area network appears as a virtualized node for external M2M area networks

How is M2M used?

M2M technology is employed in a wide range of use cases, including but not limited to the following:

- **Remote monitoring:** M2M enables remote monitoring of equipment, such as vending machines, that can communicate with distributors to request refills when running low on certain products.

- **Asset tracking:** M2M plays a crucial role in warehouse management systems and supply chain management, allowing the tracking and monitoring of assets in real time.
- **Telecommunications:** M2M is utilized in monitoring network performance, measuring signal quality, detecting faults or outages, and facilitating quicker response times.
- **Home automation:** M2M is integrated into smart home systems, allowing appliances and devices to be controlled remotely and communicate in real time.

1. In-car telemetry services

Several car manufacturers offer internet connectivity services for their customers. Occasionally, these services allow you to use a built-in SIM card to access the world wide web on your smart-phone or tablet, but in-car connectivity isn't just about letting you browse your favorite sites.

Built-in SIM cards are also used to relay important information about your car, sending a steady stream of data to your manufacturer's computer systems so they can see how well it is performing.

Some manufacturers use this data to improve future models, and may also offer more hands-on help; contacting you if it looks like a part will need replacing soon, or automatically booking service once your car clocks a certain number of miles.

All of these services can be hugely convenient for the end-user, and allow car manufacturers to offer a better service than they'd be able to if they couldn't obtain information about your vehicle. All of these services are also completely reliant on M2M technology, which allows your car to send information to the processing computer.

2. Smart meters

Smart meters (sometimes called utility meters) allow you to track energy consumption in real-time. They also allow your energy provider to see how much energy you're using, which means that:

- You know exactly how much it costs to keep the lights on
- Your energy provider can track fluctuations in power consumption, and manufacture power in more efficient ways
- You'll never be surprised by a large bill

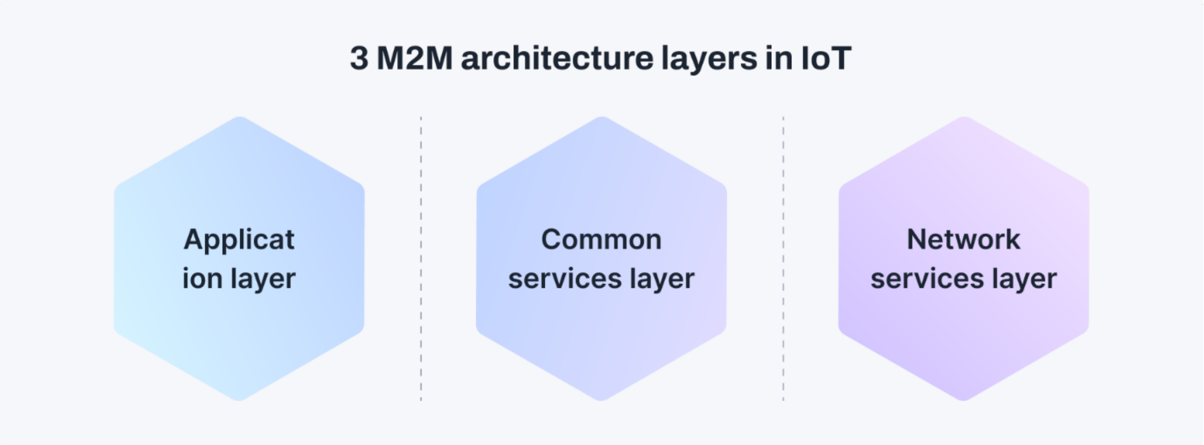
Smart meters also require M2M technology in order to function. They work by tracking your energy usage using a series of sensors, then transmit the information directly to your energy provider using a foolproof M2M network.

3. Smart asset tracking services

Asset tracking is an important concern for many businesses. Particularly businesses in the shipping industry and/or businesses with a large fleet of vehicles. Thanks to recent advances in M2M technology, businesses that need to track their assets can now do so using relatively inexpensive GPS trackers that are connected to an M2M network.

These GPS trackers allow the movement of vehicles to be tracked in real-time. They also allow companies to gather useful data about the fuel consumption, average trip times and driver performance, that can be used to improve the efficiency of journeys and processes.

M2M architecture in IoT



Application Layer

It is the oneM2M architecture's top layer. IoT applications and services reside in this layer. IoT applications may take many different forms, from industrial monitoring to smart home automation. To access and manage IoT resources and data, the application layer communicates with the services layer. The role of the IoT M2M Application Layer is to integrate IoT devices with apps, such as connecting smart devices to your phone. Additionally, it ensures that these gadgets can exchange data with other crucial systems, such as business intelligence tools.

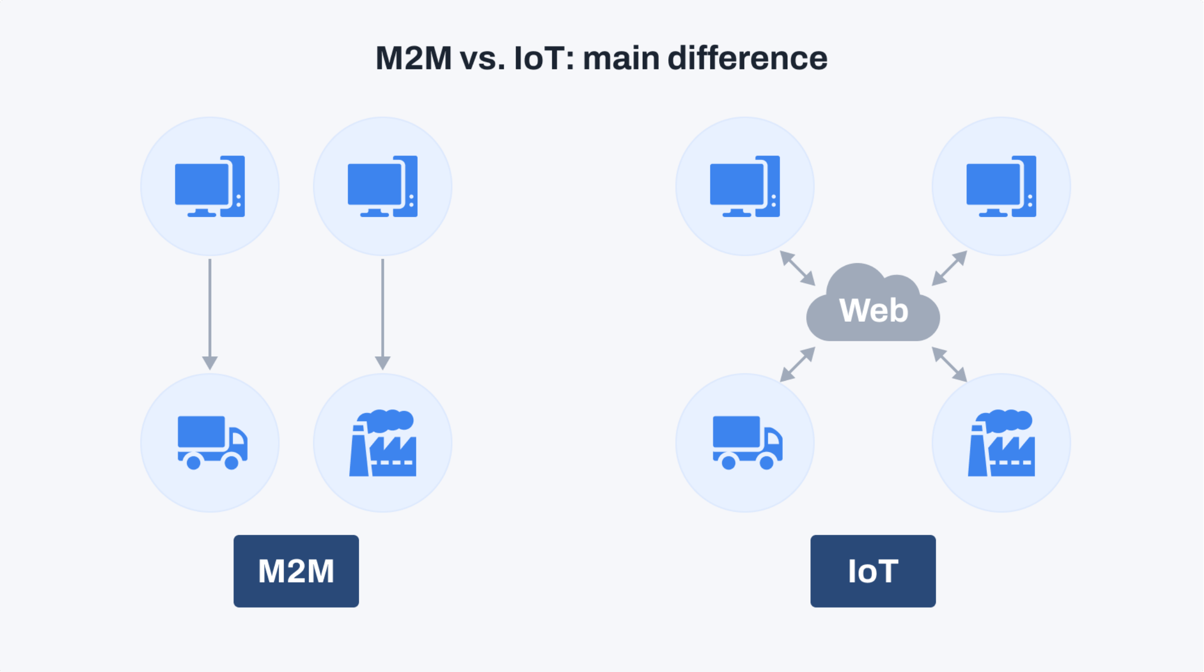
Services Layer

The service layer acts as a connecting layer between IoT devices and communication networks. It is essential for abstracting away the difficulties of device connectivity and data transfer. This layer standardizes data formats and communication protocols, providing interoperability across IoT platforms and devices. We can also say this layer functions as the background control hub. It manages the logical parts of the network and the rules they follow to work together efficiently.

Network Layer

All devices, or "things," connect at the network layer. It also includes the physical network connections, such as cellular or Wi-Fi networks that link them. The network layer manages the connectivity and data transmission between IoT devices. It ensures that data is sent quickly and securely between devices, the cloud, and other data processing facilities.

Differences between M2M and IoT



The main differences between M2M and IoT lie in their connectivity, scalability, and scope. Here are the key distinctions based on the provided search results:

1. Connection type

M2M involves point-to-point communication between two or more devices without human interaction, often wired or wireless. IoT extends the internet into machines, allowing them to connect and communicate with each other via various communication types over networks.

2. Data sharing

In IoT, data is shared between multiple applications to enhance the end-user experience. M2M shares data only between the communicating parties involved in direct communication.

3. Internet dependency

IoT devices require an internet connection for communication and operation. M2M systems can function without internet connectivity, relying on direct point-to-point communication.

4. Communication protocol

IoT typically uses internet protocols like HTTP, FTP, and Telnet for communication. Instead, M2M relies on traditional protocols and communication technologies for data exchange.

5. Scope

IoT has a broader scope, supporting many devices and users within a connected ecosystem. M2M has a more limited scope, often focusing on specific applications or industries with point-to-point communication.

M2M vs. IoT comparison table

	IoT	**M2M**
Intelligence	Devices have objects for decision-making	Some degree of intelligence is observed in this
Communication protocol	HTTP, FTP, and Telnet	Traditional protocol
Internet	An internet connection is required	Devices aren't dependent on the internet
Requirements	Generic commodity devices	Specialized device solution
Business type	B2B, B2C	B2B
Communication type	Cloud communication	Point-to-point
Examples	Smart cities, Big data, etc.	Sensors, data, information, etc.

While many use the terms interchangeably, M2M and IoT are not the same. IoT needs M2M, but M2M does not need IoT.

Both terms relate to the communication of connected devices, but M2M systems are often isolated, stand-alone networked equipment. IoT systems take M2M to the next level, bringing together disparate systems into one large, connected ecosystem.

M2M systems use point-to-point communications between machines, sensors and hardware over cellular or wired networks, while IoT systems rely on IP-based networks to send data collected from IoT-connected devices to gateways, the cloud or middleware platforms.

Advantages –
This M2M can operate over cellular networks and is simple to manage. It can be used both indoors and outdoors and aids in the communication of smart objects without the need for human interaction. The M2M contact facility is used to address security and

privacy problems in IoT networks. Large-scale data collection, processing, and security are all feasible.

Disadvantages –
However, in M2M, use of cloud computing restricts versatility and creativity. Data security and ownership are major concerns here. The challenge of achieving interoperability between cloud/M2M IoT systems is daunting. M2M connectivity necessitates the existence of a reliable internet connection.

Examples:

- Smart Washing machine sends alerts to the owners' smart devices after completion of washing or drying of clothes.
- Smart meters tracks amount of energy used in household or in companies and automatically alert the owner.

IoT M2M Systems Layers and Design Standardization

The Internet Engineering Task Force (IETF) is the body that defines standard operating internet protocols such as TCP/IP.

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

M2M systems layers and designs standardizations

Design Standardization

The Internet Engineering Task Force (IETF) is the body that defines standard operating internet protocols such as TCP/IP.

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

ETSI (European Telecommunications Standards Institute)

ETSI is an independent, non-profit organization that develops globally applicable standards for information and communication technologies (ICT), including telecommunications, broadcasting, and other related areas. It is particularly important in shaping standards for emerging technologies like IoT (Internet of Things), 5G, and smart cities.

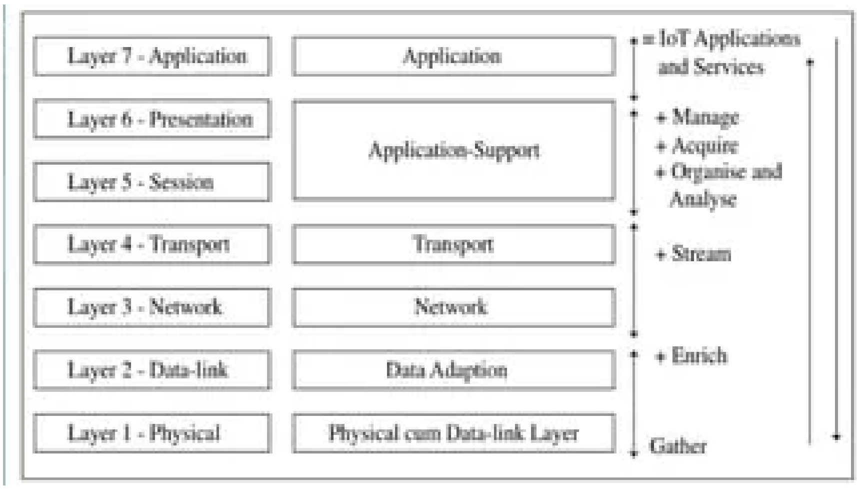
OGC (Open Geospatial Consortium)

The **OGC** is an international organization that develops standards for **geospatial** and **location-based services**. These standards allow different systems and applications to share and access geospatial data, such as maps, satellite imagery, and location-based services, in an interoperable and standardized way.

IETF six layer modified OSI model for IoT/M2M Internet Engineering Task Force (IETF) suggests the specifications for the layers, and the engineering aspects for the IoT communication, networks and applications.

The seven-layer OSI model is a standard model. It gives the basic outline for designing a communication network. IETF suggests modifications in the OSI model for the IoT/M2M. The following figure shows a classical seven-layer OSI model (on the left) and the modifications in that model proposed by IETF (in the middle). Data communicates from device end to application end. Each layer processes the received data and creates a new data stack which transfers it to the next layer. The processing takes place at the in-between layers, i.e. between the bottom functional-layer to the top layer. Device end also receives data from an application/service after processing at the in-between layers.

This figure also shows a similarity with the conceptual framework suggested by Oracle: **Gather + Enrich + Stream + (Manage + Acquire + Organise +Analyse) = IoT Applications and Services**



Application layer L6: New applications and services are present at the application layer 6.

Application-support layer L5:A modification to the OSI is that the application-support layer 5, it uses CoAP protocol for network communication. The CoAP protocol at the layer is used for the request/response interactions between the client and server at the network. Similarly, the application-support layer may include processes for data managing, acquiring, organising and analysing which are mostly used by applications and services.

Transport layer L4: The transport layer does device identity management, identity registry and data routing to the next layer.

Network Layer L3: It communicates a network stream on the Internet to the next layer.

Data-adaptation layer L2: Modifications to the OSI are also at the data-link layer 2 (L2) and physical layer 1 (L1). The new layers are data-adaptation (new L2) and physical cum data-link (new L1). The data adaptation layer includes a gateway. The gateway enables communication between the devices network and the web.

Physical cum data-link layer L1: It senses the data and transferring the sensed data to L2. A physical IoT/M2M device hardware may integrate a wireless transceiver using a communication protocol as well as a data-link protocol for linking the data stacks of L1 and L2.

Example : IETF six-layer OSI model for Internet of streetlights. Consider a model for Internet of streetlights. Following are the layers for data interchange in the modified OSI model:

● L1: It consists of smart sensing and data-link circuits with each streetlight transferring the sensed data to L2.

● L2: It consists of a group-controller which receives data of each group through Bluetooth or ZigBee, aggregates and compacts the data for communication to the Internet, and controls the group streetlights as per the program commands from a central station.

● L3: It communicates a network stream on the Internet to the next layer.

● L4: The transport layer does device identity management, identity registry and data routing to the next layer

● L5: The application-support layer does data managing, acquiring, organising and analysing, and functionalities of standard protocols such as CoAP, UDP and IP.

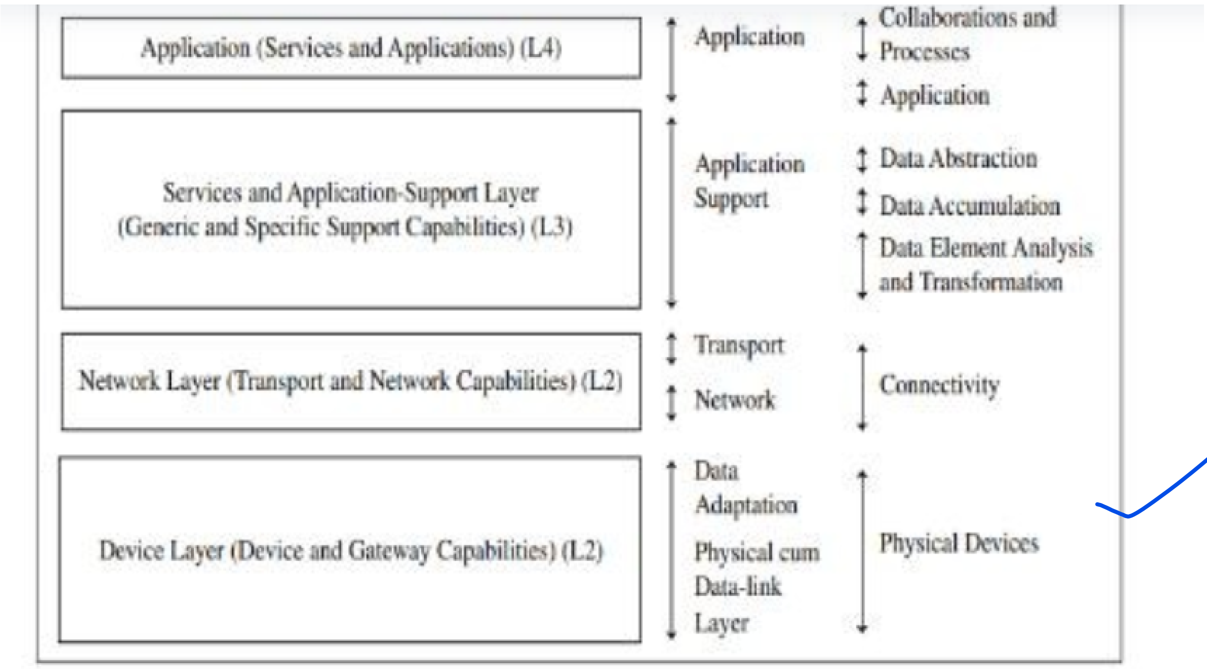
● L6: The application layer enables remote programming and issue of central station directions to switch on-off and commands of services to the controllers along with monitoring each group of streetlights in the whole city.

ITU-T Reference Model

International Telecommunication Union for Telecommunication (ITU-T) suggested a reference model for IoT domain, network and transport capabilities for the IoT services and the applications at the application and application-support layers. The following figure shows the ITU-T reference model RM1. It also shows correspondence of the model with the six-layers modified OSI model. The figure also shows a comparison with CISCO IoT reference model RM2.

ITU-T recommends four layers, each with different capabilities.

- Lowest layer, L1, is the device layer and has device and gateway capabilities.
- Next layer, L2, has transport and network capabilities.
- Next layer, L3, is the services and application-support layer. The support layer has two types of capabilities—generic and specific service or application-support capabilities.
- Top layer, L4, is for applications and services.



Application (Services and Applications) (L4)
Services and Application-Support Layer (Generic and Specific Support Capabilities) (L3)
Network Layer (Transport and Network Capabilities) (L2)
Device Layer (Device and Gateway Capabilities) (L2)
Application
Application Support
Transport
Network
Data Adaptation
Physical cum Data-link Layer
Collaborations and Processes
Application
Data Abstraction
Data Accumulation
Data Element Analysis and Transformation
Connectivity
Physical Devices

Figure 2.2 ITU-T reference model RM1, its correspondence with six layers of modified OSI and a comparison with seven levels suggested in CISCO IoT reference model RM2

A comparison of ITU-T RM1 with the six-layer OSI model:

- RM1 device layer capabilities are similar to data-adaptation and physical cum datalink layers.

- RM1 network layer capabilities are similar to transport and network layers.

- RM1 upper two layer capabilities are similar to top two layers.

A comparison of ITU-T RM1 with the CISCO IoT reference model (RM2):

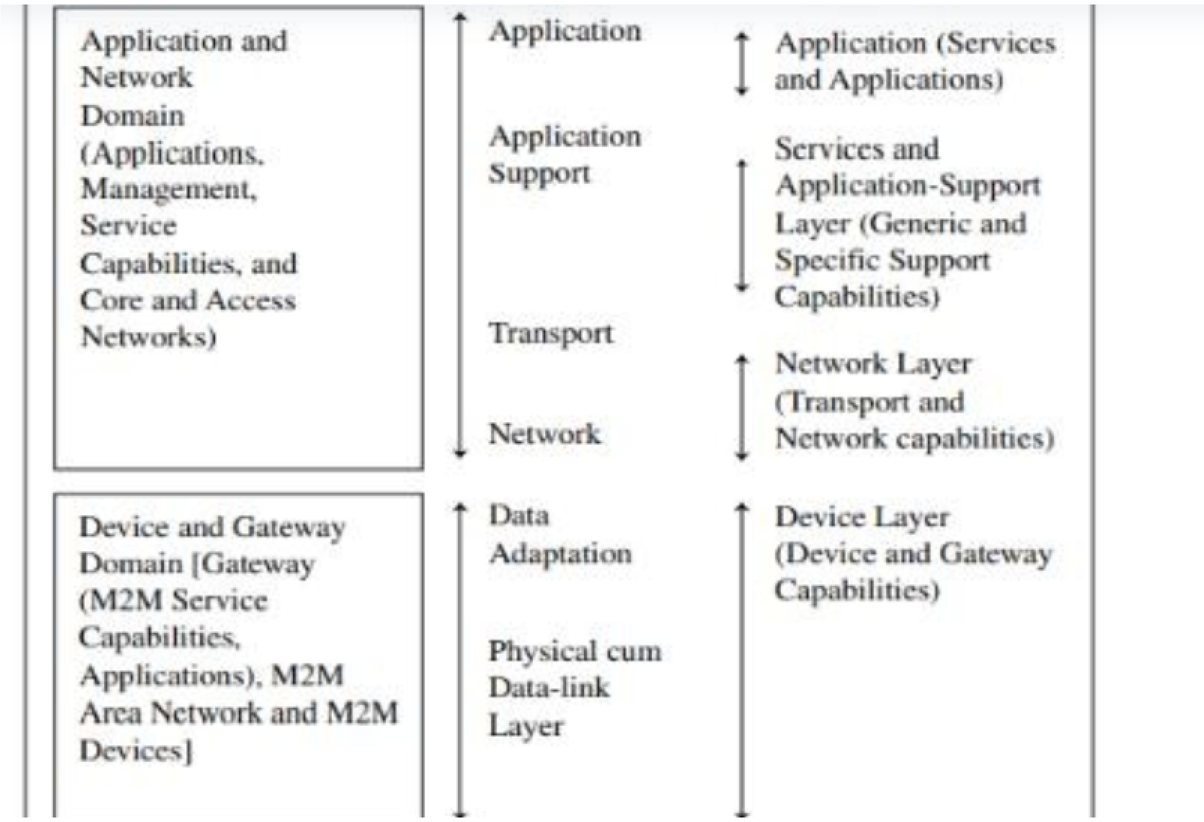
- RM1 L4 capabilities are similar to RM2 collaborations and processes, and application top two levels.

● RM1 L3 capabilities are similar to RM2 three middle-level functions of data abstraction, accumulation, analysis and transformation.

● RM1 L2 layer capabilities are similar to RM2 functions at connectivity level.

● RM1 L1 device layer capabilities are similar to RM2 functions at physical devices level.

ETSI M2M Domains and High-level Capabilities European Telecommunication Standards Institute (ETSI) initiated the development of a set of standards for the network, and devices and gateway domains for the communication between machines (M2M). ETSI proposed high-level architecture for applications and service capabilities. A domain specifies the functional areas. High-level architecture means architecture for functional and structural views. The following figure shows ETSI M2M domains and architecture, and the high-level capabilities of each domain. It also shows that the architecture correspondences with the six-layer modified OSI model as well as the four layers of the ITU-T reference mode.



Application and Network Domain (Applications, Management, Service Capabilities, and Core and Access Networks)	Application	Application (Services and Applications)
	Application Support	Services and Application-Support Layer (Generic and Specific Support Capabilities)
	Transport	Network Layer (Transport and Network capabilities)
	Network	
Device and Gateway Domain [Gateway (M2M Service Capabilities, Applications), M2M Area Network and M2M Devices]	Data Adaptation	Device Layer (Device and Gateway Capabilities)
	Physical cum Data-link Layer	

The ETSI network domain has six capabilities and functions:

1. M2M applications

2. M2M service capabilities

3. M2M management functions

4. Network management functions

5.CoRE network (for example, 3G and IP networks, network control functions, interconnections among networks)

6. Access network (for example, LPWAN (low power wide area network), WLAN (Wi-Fi) and WiMax networks)

The ETSI device and gateway domain has the following functional units:

● Gateway between M2M area network, and CoRE and access network, possessing M2M service capabilities and applications

● M2M area network (for example, Bluetooth, ZigBee NFC, PAN, LAN)

● M2M devices