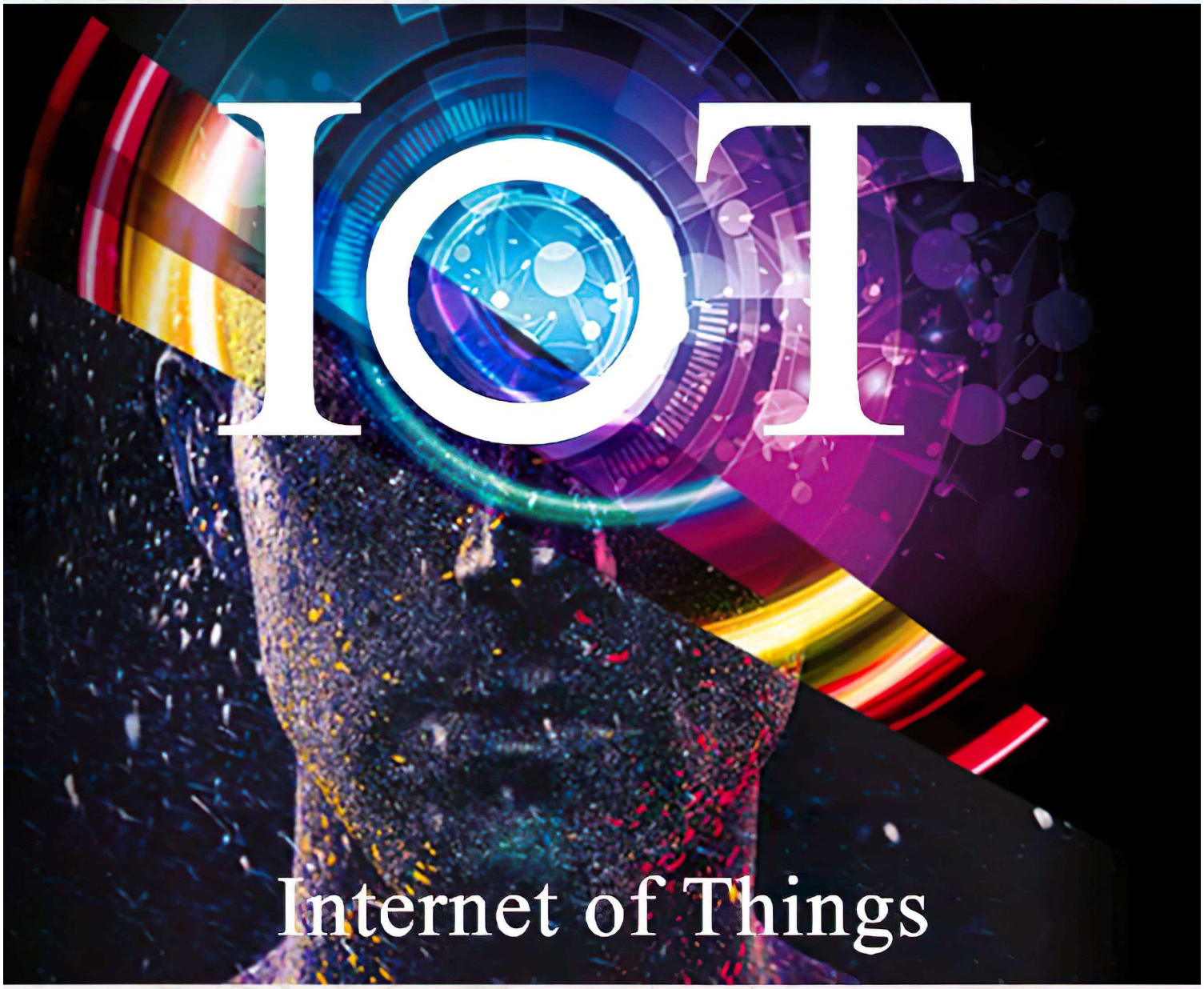
Jump2Learn
PUBLICATION

www.jump2learn.com



Internet of Things

Jump2Learn - The Online Learning Place

Mr. Vijesh Shukla | Ms. Khushbu A. Patel | Mr. Ankit R. Patel

UNIT – 2

IOT AND M2M

2.1 Introduction M2M

Machine-to-machine, or M2M, is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans. Artificial intelligence (AI) and machine learning (ML) facilitate the communication between systems, allowing them to make their own autonomous choices. M2M technology was first adopted in manufacturing and industrial settings, where other technologies, such as SCADA and remote monitoring, helped remotely manage and control data from equipment. M2M has since found applications in other sectors, such as healthcare, business and insurance. M2M is also the foundation for the internet of things (IoT).

How M2M works

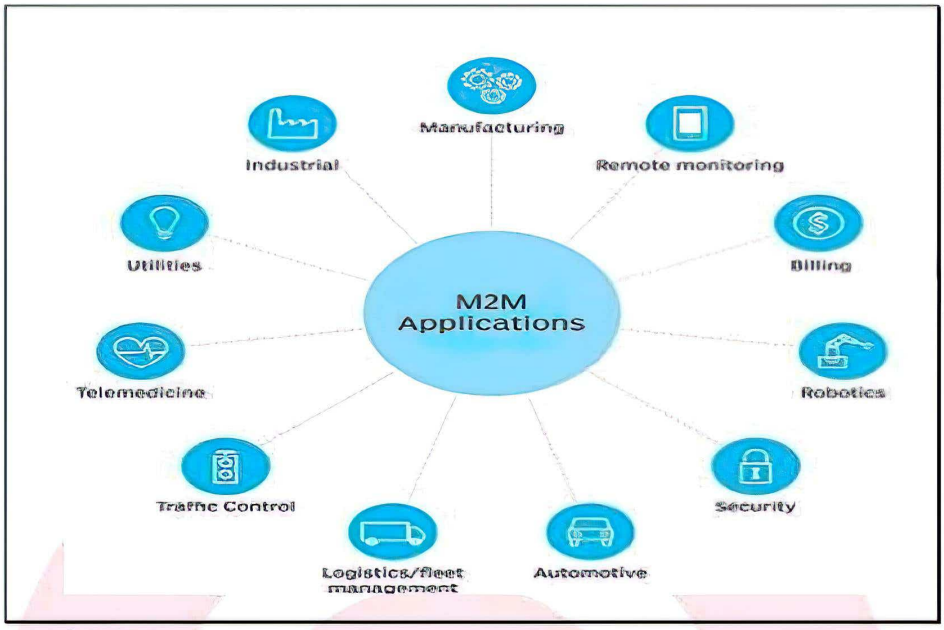
The main purpose of machine-to-machine technology is to tap into sensor data and transmit it to a network. Unlike SCADA or other remote monitoring tools, M2M systems often use public networks and access methods -- for example, cellular or Ethernet -- to make it more cost-effective.

The main components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link, and autonomic computing software programmed to help a network device interpret data and make decisions. These M2M applications translate the data, which can trigger preprogramed, automated actions.

One of the most well-known types of machine-to-machine communication is telemetry, which has been used since the early part of the last century to transmit operational data. Pioneers in telemetrics first used telephone lines, and later, radio waves, to transmit performance measurements gathered from monitoring instruments in remote locations.

The Internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday use in products such as heating units, electric meters and internet-connected devices, such as appliances.

M2M application



Key features of M2M

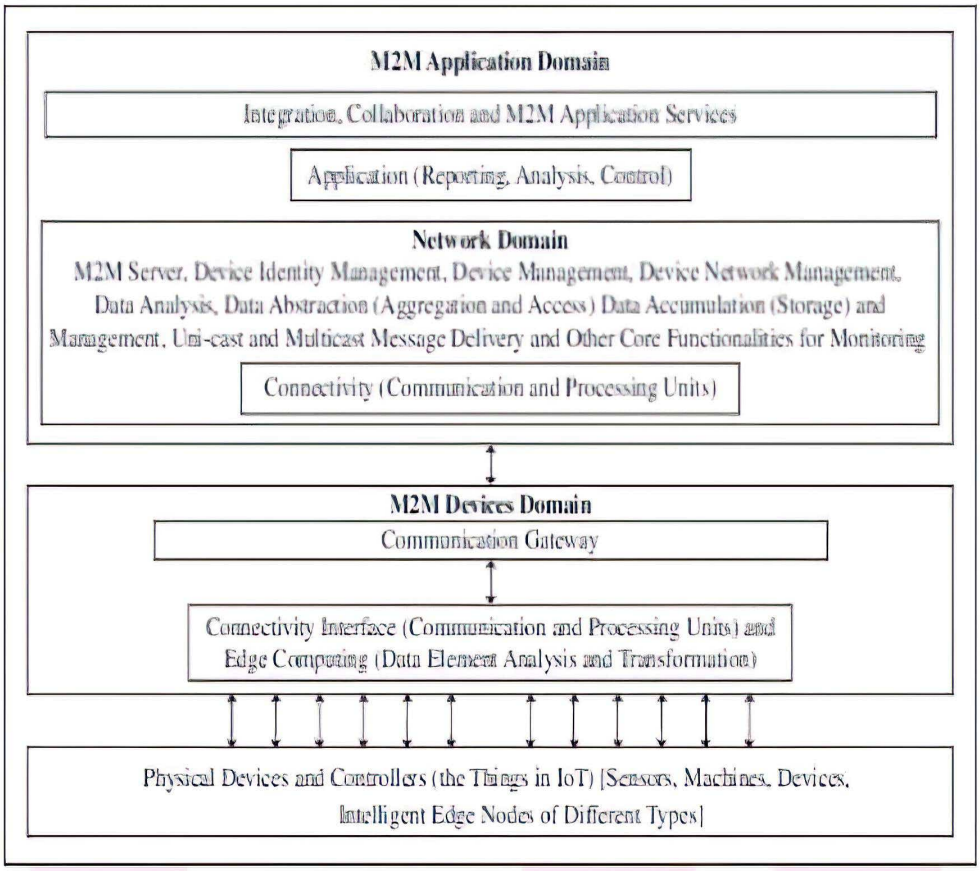
Key features of M2M technology include:

1. Low power consumption, in an effort to improve the system's ability to effectively service M2M applications.
2. A Network operator that provides packet-switched service.
3. Monitoring abilities that provide functionality to detect events.
4. Time tolerance, meaning data transfers can be delayed.
5. Time control, meaning data can only be sent or received at specific predeterminedperiods.
6. Location specific triggers that alert or wake up devices when they enter particular areas.
7. The ability to continually send and receive small amounts of data.

M2M Architecture

M2M architecture consists of three domains:

1. M2M device domain
2. M2M network domain
3. M2M application domain



[Fig. 2.1 Three domains of M2M architecture]

M2M device communication domain consists of three entities: physical devices, communication interface and gateway. Communication interface is a port or a subsystem, which receives the input from one end and sends the data received to another

M2M network domain consists of M2M server, device identity management, data analytics and data and device management similar to IoT architecture (connect + collect +assemble + analyse) level.

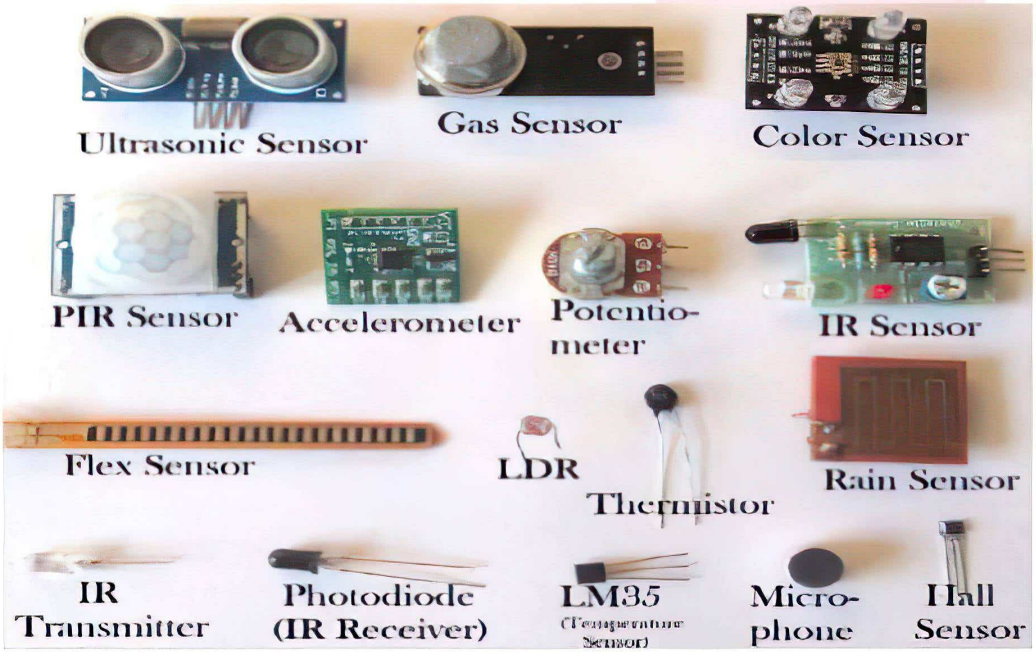
M2M application domain consists of application for services, monitoring, analysis andcontrolling of devices networks.

2.2 Introduction to Sensor Technology

Sensor technology is a technology used for designing sensors and associated electronic readers, circuits and devices. A sensor can sense a change in physical parameters, such as temperature, pressure, light, metal, smoke and proximity to an object. Sensors can also sense acceleration, orientation, location, vibrations or smell, organic vapors or gases. A microphone senses the voice and changes in the sound, and is used to record voice or music. A sensor converts physical energy like heat, sound, strain, pressure, vibrations and motion into electrical energy. An electronic circuit connects to the input at a sensor. The circuit receives the output of the sensor. The output is according to the variation in physical condition. A smart sensor includes the electronic circuit within itself, and includes computingand communication capabilities.

The circuit receives energy in form of variations through currents, voltages, and phase angles or frequencies. Analog sensors measure the variations in the parameters with respect to a reference or normal condition and provide the value of sensed parameter after appropriate calculations.

The change of states with respect to a reference or normal condition senses the states inthe form of 0s and 1s in digital sensors.



[Fig. 2.2 Different Types of Sensors]

There are two types of sensors:

1. Analog and
2. Digital

ANALOG SENSOR

The sensors that produce continuous analog output signal these are considered as analog sensors. There are various types of analog sensors such as temperature, moisture, accelerometer, pressure, light, sound sensor etc.

DIGITAL SENSOR

Sensors in which data conversion & transmission takes place digitally are known as digital sensors.

In digital sensors, the signal measured is converted into digital signal by the sensor itself. And this digital signal is transmitted through wire digitally. Somehow it overcomes the disadvantages of analog sensors.

Examples of digital sensors are IR, ultrasonic, float, moisture sensor etc.

2.3 Difference between IoT and M2M

1. Internet of Things:

IOT is known as the Internet of Things where things are said to be the communicating devices that can interact with each other using a communication media. Usually every daysome new devices are being integrated which uses IoT devices for its function. These devices use various sensors and actuators for sending and receiving data over the internet. It is an ecosystem where the devices share data through a communication mediaknown as the internet.

2. Machine to Machine:

This is commonly known as Machine to machine communication. It is a concept where twoor more than two machines communicate with each other without human interaction using a wired or wireless mechanism. M2M is an technology that helps the devices to connect between devices without using internet. M2M communications offer several applications such as security, tracking and tracing, manufacturing and facility management.

Difference between IoT and M2M :

Basis of	IoT	M2M
Abbreviation	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making	Some degree of intelligence is observed inthis
Connection type used	The connection is via Network and using various communication types.	The connection is a point to point
Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.	Traditional protocols and communication technology techniques areused
Data Sharing	Data is shared between other applications that are used to improve the end-user experience.	Data is shared with only the communicating parties.
Internet	Internet connection is required for communication	Devices are not dependent on the Internet.
Scope	A large number of devices yet scope is large.	Limited Scope for devices.
Business Type used	Business 2 Business(B2B) and Business 2 Consumer(B2C)	Business 2 Business (B2B)
Open API support	Supports Open API integrations.	There is no support for Open Api's
Examples	Smart wearables, Big Data and Cloud, etc.	Sensors, Data and Information, etc.

2.4 Security for IoT

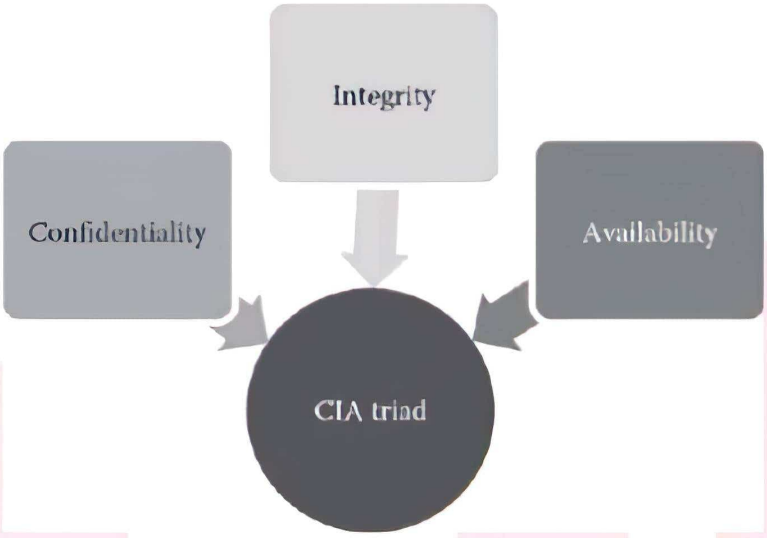
Confidentiality, Integrity, and Availability Triad

The confidentiality, integrity, and availability (CIA) triad, which are the three fundamental requirements that need to be kept in mind during the design and development phase of

theunderlying IoT infrastructure, are depicted in Figure 2.3.

Confidentiality

It ensures that only authorized users will have access to the underlying information. In otherwords, it ensures that privacy by preventing unauthorized access to the information, which isstored and transmitted using the IoT infrastructure.



[Fig.2.3 CIA triad]

Integrity

It ensures that only authorized users are allowed to modify the underlying information. It ensures that unauthorized users will not be able to alter the information in any manner. Alteration involves write, delete, and update operations.

Availability

It ensures that authorized users have access to the underlying information as and when it is required. This includes ensuring the fact that the IoT infrastructure has fault tolerance capabilities built into them. Fault tolerance can be built into the IoT infrastructure by ensuring that backup components are present for each of the IoT infrastructure components, namely,servers, storage, and networks. Server backup can be ensured by clustering the servers in order to provide a high availability environment. It is also important to ensure that the backupserver is an identical copy of the primary server and can take over the role of the primary server immediately upon the failure of the primary server. Storage backup can be ensured byusing the highly scalable RAID architecture for hard disks in which

same data is striped and mirrored across multiple hard disks, so that even if one hard disk fails, data will not be lost asit will stored in the other disks of the array. Fault tolerance in networks can be ensured by providing multiple switches, multiple ports, and multiple cables between the two connectingendpoints in order to ensure that the failure of any network component will not hamper thetransfer of data through the network.

These components, Confidentiality, Integrity, and Availability, are commonly referred to as the CIA triad.

Authentication, Authorization, and Audit Trial (AAA) Framework

AAA framework is a security requirement, which is of paramount importance for the IoT infrastructure. The various components of the framework are described below.

Authentication

This process checks to ensure that a user's credentials are valid, so that users with invalid credentials will not be allowed to access the underlying information. The simplest way to useauthentication is with the help of user names and passwords. But as hacking techniques are evolving day by day, it is very important to ensure that sophisticated authentication techniques are in place. One such authentication mechanism that is used is called multifactor authentication. Multifactor authentication is a special authentication technique, which uses a combination of parameters to verify a user's credentials. An example of multifactor authentication mechanism is described below:

First Factor: A user name and password, which will be unique for the specific user and whichmay be sometimes unique for the specific session as well.

Second Factor: A secret key, which is generated by a random number generator, or a secret key phrase, which is known only to the user, or answer to a secret question, which is specificto a particular user.

Third Factor: This could be any biometric parameter of the user, which could be used as theuser's biometric signature. This could include aspects like iris recognition, finger print recognition, and so on.

A multifactor authentication uses a combination of all the parameters mentioned above in order to verify a user's credentials. In some cases, only two factors mentioned above may beused for authentication, and in that case, it is called two-factor authentication.

Authorization

Authorization is a process which ensures that a specific user has rights to perform specific operations on a specific object. This is generally by granting different types of permissions todifferent types of users based on their role in a city government. For example, a fire station executive will just be able to read the data pertaining to other city departments like water; he/she may not be able to edit it. Edit permissions may be given only to the city supervisors or executives who belong to the water department of the city. The different types ofpermissions for different users on different objects are mapped and stored in a table, which is called Access Control List (ACL).

The different types of permissions, which are given for users, are classified as the following:

Read only: The user has permission to only read the object. The user cannot delete or edit theobject. These types of permissions are granted to staff who are not required to perform any alteration on the data.

Read and write: The user has permission to read and alter the object. These types of permissions are granted to authorities who have the overall authority and discretion to validate the rights and access permissions of other users.

Audit Trial

Audit trial is an activity, which is conducted periodically, to assess the effectiveness of the security measures that are implemented in the IoT infrastructure. Audit trial is performed with the help of audit logs, which track the operations that are performed by different users.

2.5 IoT Enabling Technologies

IoT(internet of things) enabling technologies are:

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 –

- Broad network access
- On demand self-services
- Rapid scalability
- Measured service
- 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

- Data encoding
- 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-Fiadapters), input output units (display keyword etc.) and storage devices (flash memory).

It collects the data and sends it to the internet.Examples –

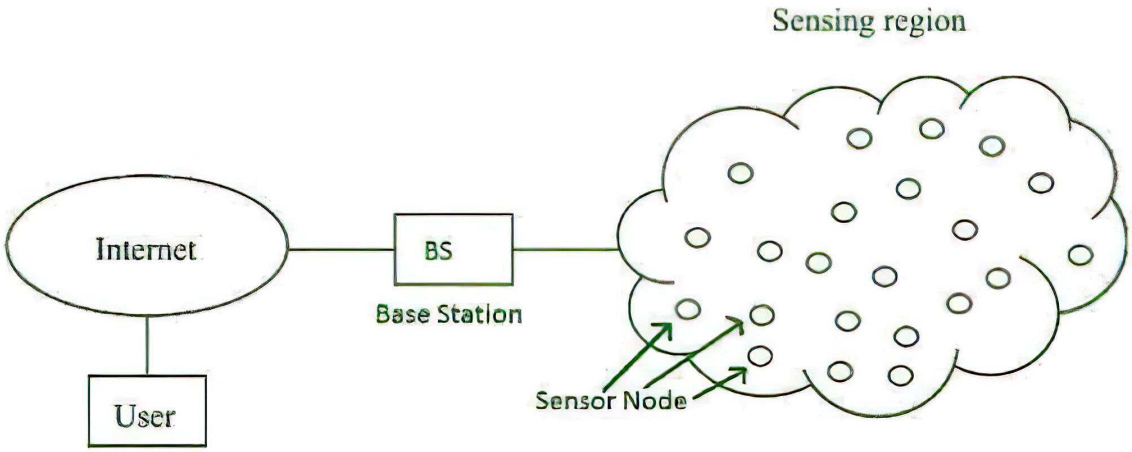
- Digital camera
- DVD player, music player
- Industrial robots
- Wireless Routers etc.

2.5.1 Wireless Sensor Networks

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed ina large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the on-board processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data's can be used for processing, analysis, storage, and mining of the data.

Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensornode is equipped with sensing and computing devices, radio transceivers and power components.



Applications of WSN:

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

Components of WSN:

Sensors: Sensors in WSN are used to capture the environmental variables and which is usedfor data acquisition. Sensor signals are converted into electrical signals.

Radio Nodes: It is used to receive the data produced by the Sensors and sends it to theWLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

WLAN Access Point: It receives the data which is sent by the Radio nodes wirelessly,generally through the internet.

Evaluation Software: The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of thedata.

Applications of wireless sensor network

Military applications: Wireless sensor networks be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.

Area monitoring: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored. When the sensors detect the event being monitored(heat, pressure etc.), the event is reported to one of the base stations, which then takes appropriate action.

Transportation: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.

Health applications: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.

Environmental sensing: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc. Some other major areas are listed below:

- Air pollution monitoring
- Forest fires detection
- Greenhouse monitoring
- Landslide detection

Structural monitoring: Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc. enabling Engineering practices to monitor assets remotely without the need for costly site visits.

Industrial monitoring: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

Agricultural sector: using a wireless network frees the farmer from the maintenance of

wiringin a difficult environment. Irrigation automation enables more efficient water use and reduceswaste.

2.5.2 Big Data Analytics

What is Big Data Analytics?

Big Data analytics is a process used to extract meaningful insights, such as hidden patterns, unknown correlations, market trends, and customer preferences. Big Data analytics provides various advantages—it can be used for better decision making, preventing fraudulent activities, among other things.

Why is big data analytics important?

In today's world, Big Data analytics is fueling everything we do online—in every industry.

Take the music streaming platform Spotify for example. The company has nearly 96 million users that generate a tremendous amount of data every day. Through this information, the cloud-based platform automatically generates suggested songs—through a smart recommendation engine—based on likes, shares, search history, and more. What enables thisis the techniques, tools, and frameworks that are a result of Big Data analytics.

If you are a Spotify user, then you must have come across the top recommendation section, which is based on your likes, past history, and other things. Utilizing a recommendation engine that leverages data filtering tools that collect data and then filter it using algorithms works. This is what Spotify does.

What is Big Data?

Big Data is a massive amount of data sets that cannot be stored, processed, or analyzedusing traditional tools.

Today, there are millions of data sources that generate data at a very rapid rate. These data sources are present across the world. Some of the largest sources of data are social media platforms and networks. Let's use Facebook as an example—it generates more than 500

terabytes of data every day. This data includes pictures, videos, messages, and more.

Data also exists in different formats, like structured data, semi-structured data, and unstructured data. For example, in a regular Excel sheet, data is classified as structured data—with a definite format. In contrast, emails fall under semi-structured, and your pictures and videos fall under unstructured data. All this data combined makes up Big Data.

Benefits & Advantages of Big Data Analytics

1. Risk Management

Use Case: Banco de Oro, a Philippine banking company, uses Big Data analytics to identify fraudulent activities and discrepancies. The organization leverages it to narrow down a listof suspects or root causes of problems.

2. Product Development and Innovations

Use Case: Rolls-Royce, one of the largest manufacturers of jet engines for airlines and armed forces across the globe, uses Big Data analytics to analyze how efficient the engine designs are and if there is any need for improvements.

3. Quicker and Better Decision Making Within Organizations

Use Case: Starbucks uses Big Data analytics to make strategic decisions. For example, the company leverages it to decide if a particular location would be suitable for a new outlet or not. They will analyze several different factors, such as population, demographics, accessibility of the location, and more.

4. Improve Customer Experience

Use Case: Delta Air Lines uses Big Data analysis to improve customer experiences. They monitor tweets to find out their customers' experience regarding their journeys, delays, and so on. The airline identifies negative tweets and does what's necessary to remedy the situation. By publicly addressing these issues and offering solutions, it helps the airline build good customer relations.

The Lifecycle Phases of Big Data Analytics

Stage 1 - Business case evaluation - The Big Data analytics lifecycle begins with a businesscase, which defines the reason and goal behind the analysis.

Stage 2 - Identification of data - Here, a broad variety of data sources are identified.

Stage 3 - Data filtering - All of the identified data from the previous stage is filtered here toremove corrupt data.

Stage 4 - Data extraction - Data that is not compatible with the tool is extracted and thentransformed into a compatible form.

Stage 5 - Data aggregation - In this stage, data with the same fields across different datasetsare integrated.

Stage 6 - Data analysis - Data is evaluated using analytical and statistical tools to discoveruseful information.

Stage 7 - Visualization of data - With tools like Tableau, Power BI, and QlikView, Big Dataanalysts can produce graphic visualizations of the analysis.

Stage 8 - Final analysis result - This is the last step of the Big Data analytics lifecycle, wherethe final results of the analysis are made available to business stakeholders who will take action.

Different Types of Big Data Analytics

1. Descriptive Analytics

This summarizes past data into a form that people can easily read. This helps in creating reports, like a company's revenue, profit, sales, and so on. Also, it helps in the tabulation ofsocial media metrics.

Use Case: The Dow Chemical Company analyzed its past data to increase facility utilization across its office and lab space. Using descriptive analytics, Dow was able to identify underutilized space. This space consolidation helped the company save nearly US $4 millionannually.

2. Diagnostic Analytics

This is done to understand what caused a problem in the first place. Techniques like drill-down, data mining, and data recovery are all examples. Organizations use diagnostic analyticsbecause they provide an in-depth insight into a particular problem.

Use Case: An e-commerce company's report shows that their sales have gone down, althoughcustomers are adding products to their carts. This can be due to various reasons like the formdidn't load correctly, the shipping fee is too high, or there are not enough payment options available. This is where you can use diagnostic analytics to find the reason.

3. Predictive Analytics

This type of analytics looks into the historical and present data to make predictions of the future. Predictive analytics uses data mining, AI, and machine learning to analyze current data and make predictions about the future. It works on predicting customer trends, market trends, and so on.

Use Case: PayPal determines what kind of precautions they have to take to protect their clients against fraudulent transactions. Using predictive analytics, the company uses all the historical payment data and user behaviour data and builds an algorithm that predicts fraudulent activities.

4. Prescriptive Analytics

This type of analytics prescribes the solution to a particular problem. Perspective analytics works with both descriptive and predictive analytics. Most of the time, it relies on AI and machine learning. Use Case: Prescriptive analytics can be used to maximize an airline's profit. This type of analytics is used to build an algorithm that will automatically adjust the flight fares based onnumerous factors, including customer demand, weather, destination, holiday seasons, and oil prices.

Big Data Analytics Tools

Hadoop - helps in storing and analyzing data **MongoDB** - used on datasets that change frequently**Talend** - used for data integration and management

Cassandra - a distributed database used to handle chunks of data

Spark - used for real-time processing and analyzing large amounts of data

STORM - an open-source real-time computational system

Kafka - a distributed streaming platform that is used for fault-tolerant storage

Big Data Industry Applications

Ecommerce - Predicting customer trends and optimizing prices are a few of the ways e-commerce uses Big Data analytics

Marketing - Big Data analytics helps to drive high ROI marketing campaigns, which result in improved sales

Education - Used to develop new and improve existing courses based on market requirements

Healthcare - With the help of a patient's medical history, Big Data analytics is used to predict how likely they are to have health issues

Media and entertainment - Used to understand the demand of shows, movies, songs, and more to deliver a personalized recommendation list to its users

Banking - Customer income and spending patterns help to predict the likelihood of choosing various banking offers, like loans and credit cards

Telecommunications - Used to forecast network capacity and improve customer experience

Government - Big Data analytics helps governments in law enforcement, among other things.

2.5.3 Embedded Systems.

As its name suggests, Embedded means something that is attached to another thing. An embedded system can be thought of as a computer hardware system having software embedded in it. An embedded system can be an independent system or it can be a part of alarge system. An embedded system is a microcontroller or microprocessor based system which is designed to perform a specific task. For example, a fire alarm is an embedded system; it will sense only smoke.

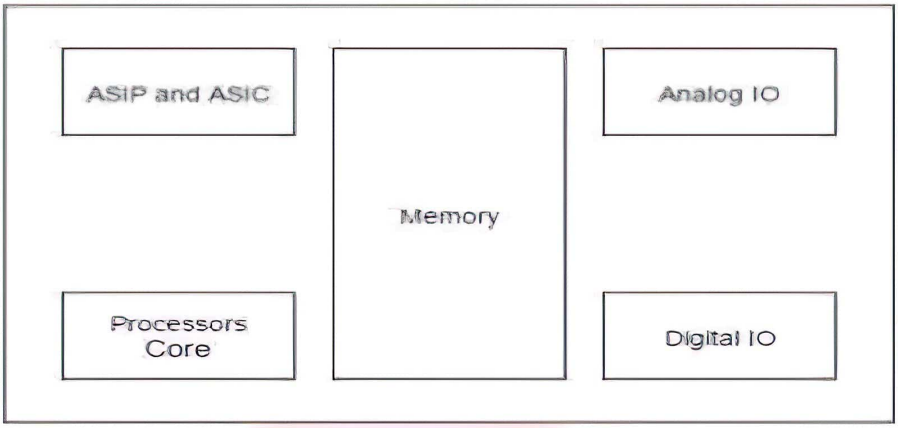
An embedded system has three components –

- It has hardware.
- It has application software.
- It has Real Time Operating system (RTOS) that supervises the application software and provide mechanism to let the processor run a process as per scheduling by following a plan to control the latencies. RTOS defines the way the system works. It sets the rules during the execution of application program. A small scale embedded system may not have RTOS.

So we can define an embedded system as a Microcontroller based, software driven, reliable,real-time control system.

Characteristics of an Embedded System

- **Single-functioned** – an embedded system usually performs a specialized operation and does the same repeatedly. For example: A pager always functions as a pager.
- **Tightly constrained** – All computing systems have constraints on design metrics, but those on an embedded system can be especially tight. Design metrics is a measure of an implementation's features such as its cost, size, power, and performance. It must be of a size to fit on a single chip, must perform fast enough to process data in real time and consume minimum power to extend battery life.
- **Reactive and Real time** – Many embedded systems must continually react to changes in the system's environment and must compute certain results in real time without any delay. Consider an example of a car cruise controller; it continually monitors and reacts to speed and brake sensors. It must compute acceleration or de-accelerations repeatedly within a limited time; a delayed computation can result in failure to control of the car.
- **Microprocessors based** – It must be microprocessor or microcontroller based.
- **Memory** – It must have a memory, as its software usually embeds in ROM. It does not need any secondary memories in the computer.
- **Connected** – It must have connected peripherals to connect input and output devices.
- **HW-SW systems** – Software is used for more features and flexibility. Hardware isused for performance and security.



Advantages

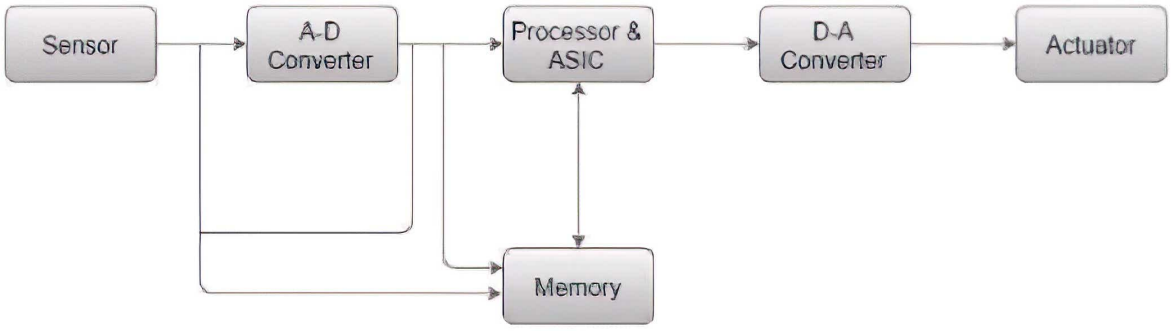
- Easily Customizable
- Low power consumption
- Low cost
- Enhanced performance

Disadvantages

- High development effort
- Larger time to market

Basic Structure of an Embedded System

The following illustration shows the basic structure of an embedded system –



- **Sensor** – It measures the physical quantity and converts it to an electrical signal whichcan be read by an observer or by any electronic instrument like an A2D converter. Asensor stores the measured quantity to the memory.
- **A-D Converter** – An analog-to-digital converter converts the analog signal sent

by thesensor into a digital signal.

- **Processor & ASICs** – Processors process the data to measure the output and store it to the memory.
- **D-A Converter** – A digital-to-analog converter converts the digital data fed by the processor to analog data
- **Actuator** – An actuator compares the output given by the D-A Converter to the actual(expected) output stored in it and stores the approved output.

Short Questions:

1. What does M2M mean?
2. Give examples of M2M applications.
3. What are the three architectural domain functionalities in M2M architecture?
4. What is WSN?
5. What is Analog Sensor?
6. What is Digital Sensor?
7. Define big data Analytics.
8. Write a full form : IaaS,PaaS,SaaS

Long Questions:

1. Difference between IoT and M2M.
2. Explain Wireless Sensor Networks detail.
3. Explain Embedded Systems in detail.
4. Write a note on Security for IOT.
5. Write a Detail note on big data Analytics.

****