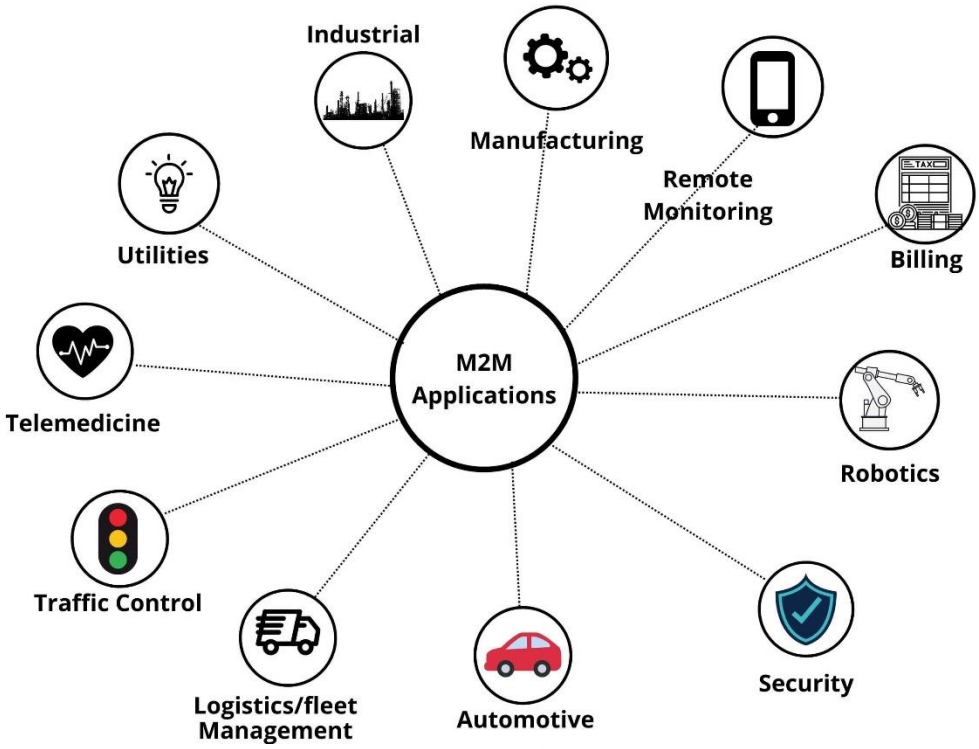
## Introduction to M2M:

- Machine-to-Machine describes any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.
- Artificial Intelligence and Machine Learning facilitate the communication between systems, allowing them to make their own autonomous choices.
- M2M was first adopted in manufacturing and industrial settings, where other technologies, such as SCADA (Supervisory Control And Data Acquisition) and remote monitoring that helped to remotely manage and control data from equipment.
- It is a foundation for the IOT.

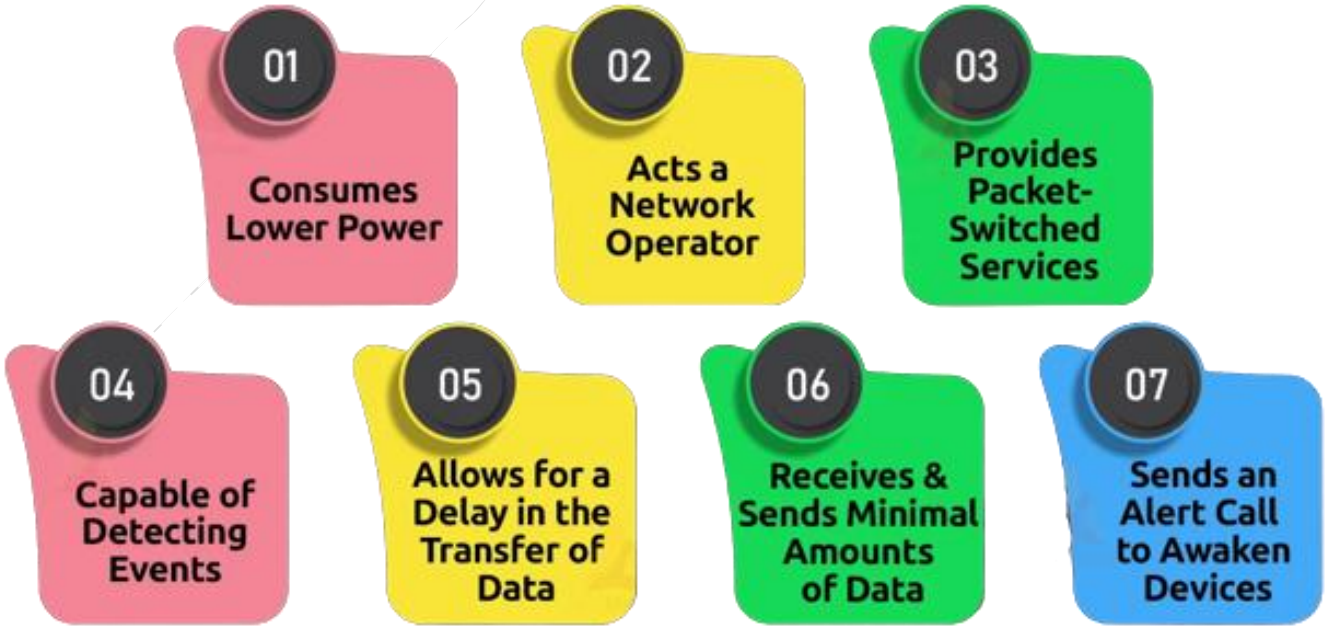
## How M2M works:

- The main purpose of M2M technology is to tap into sensor data and transmit it to a network.
- M2M often uses public networks and access methods, ex.: cellular o Ethernet to make it more cost-effective.
- Main components of M2M system includes sensors, RFID, a Wi-Fi or cellular communication link and autonomic computing software programmed to help a network device and make decisions.
- These M2M applications translate the data, which can trigger pre-programmed, automated actions.
- Telemetry is one of the M2M communication, it is used since the early part of the last century to transmit operational data.
- The internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing t everyday use products such as heating units, electric meters, and internet connected devices.

## M2M applications:



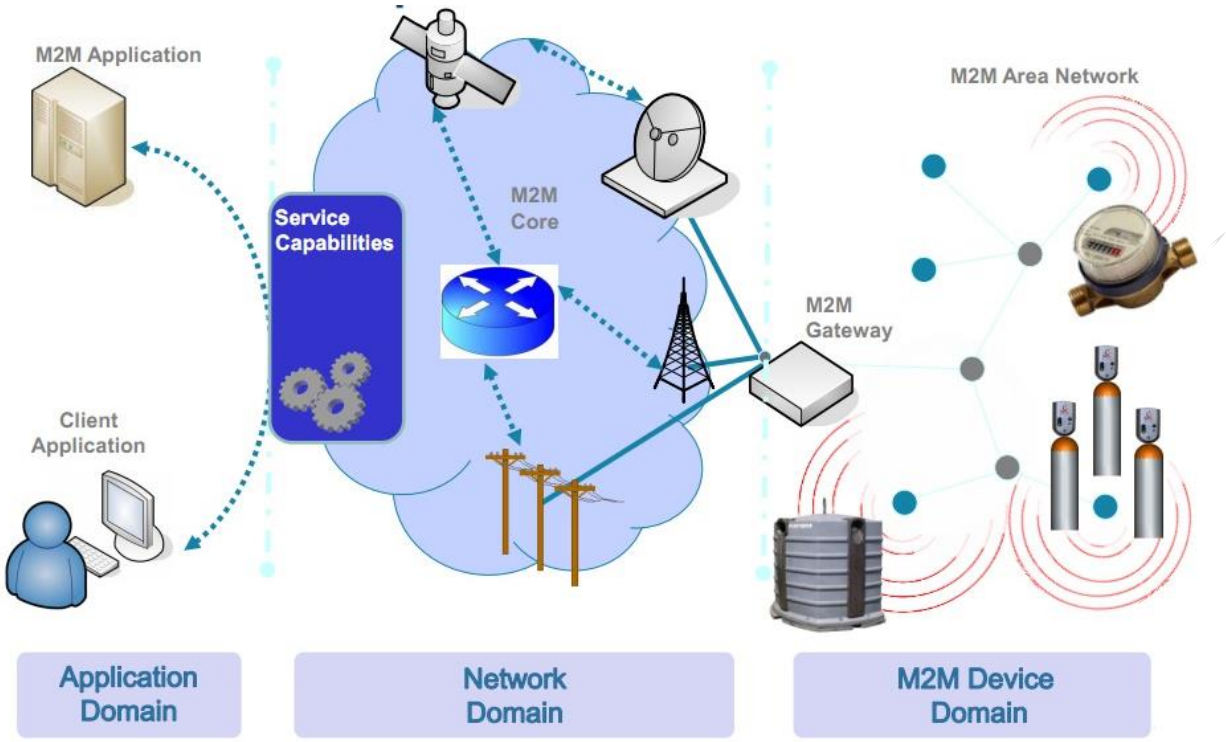

## Key features of M2M:



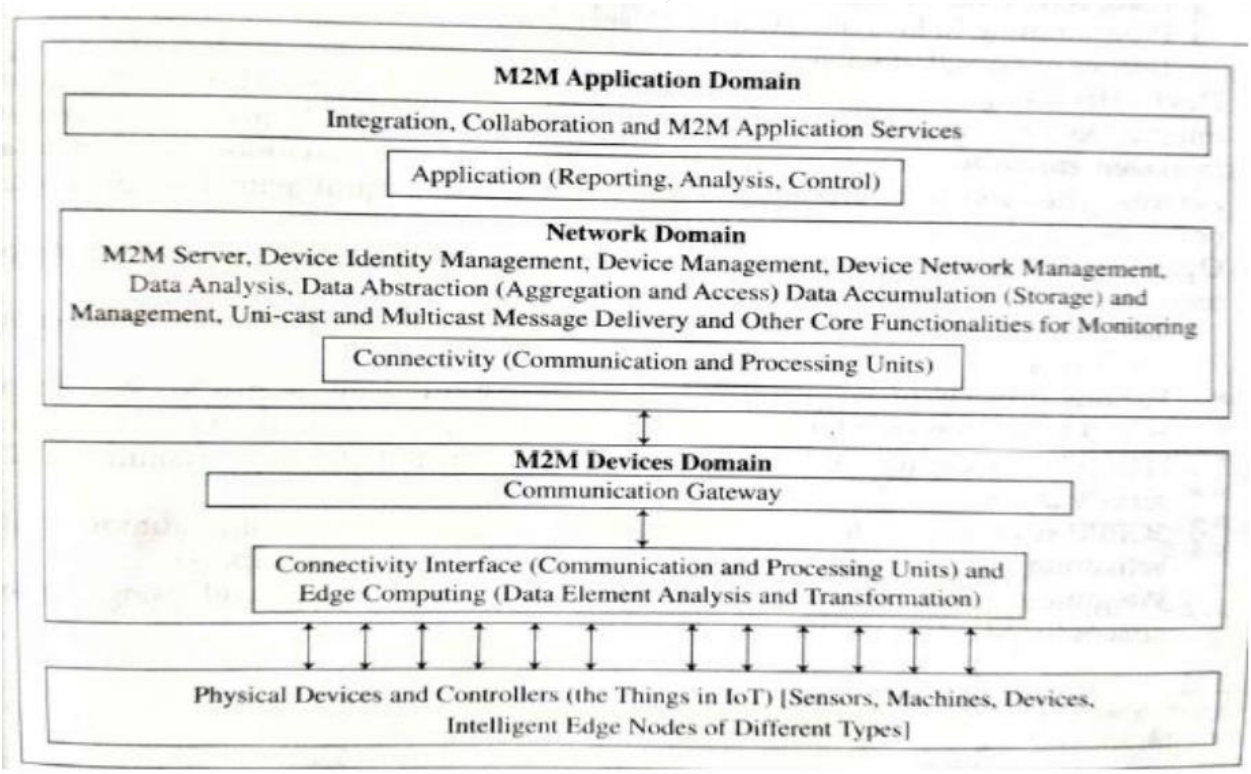
- Lower power consumption – to improve the system's ability to effectively service M2M applications.
- A network operator that provides packet-switched service.
- Time control (i.e. data can only be sent or received at specific pre-determined periods)
- Monitoring abilities that provide functionality to detect events.
- Time tolerance (i.e. data transfer can be delayed)
- The ability to continually send and receive small amounts of data.
- Location specific triggers (i.e. alert or wake up devices when they enter particular areas)

## M2M Architecture:

1. **M2M Device Communication Domain:**
   - It consists of 3 entities:
     (a) Physical devices (i.e. sensors, physical devices, controllers, machines which are capable of transmitting data autonomously)
     (b) Communication interface (It is the port or processing unit that receives data from one interface and transmit it to other interface.)
     (c) Gateway (Gateways and routers are the endpoints of the operator's network in scenarios where sensors and M2M devices do not connect directly to the network)
   - It is a port or a part of subsystem, which receives the input from one end and sends the data received to another.
2. **M2M Network Domain:**
   - It consists of M2M server, device identity management, data analytics and data/device management, somehow to similar to IOT architecture (connect + collect + assemble + analyze) level.
3. **M2M Application Domain:**
   - It consists of applications for services, monitoring, analysis and controlling of devices networks.




(Fig. A – M2M Architecture)




(Fig. B – M2M Architecture)

## Sensor Technology:

- A sensor can sense a change in physical parameters, such as temperature, pressure, light, smoke, and proximity to an object and also sense acceleration, orientation, location, vibrations.
- A microphone senses the voices and changes in the sound, and is used to record voice or music.
- A sensor converts physical energy like heat, sound, pressure, vibrations and motions into electrical energy.
- An electronic circuit connects to the input at a sensor.
- The circuit receives the output of the sensor.
- The circuit receives energy in form of variations through currents, voltages and frequencies.

### 1. Analog Sensors:

- They produce continuous analog output signals.
- Analog sensors measure the variations in the parameters with respect to a reference and provide the value of sensed parameter after appropriate calculations.
- It includes temperature, moisture, pressure, light, sound, etc.

### 2. Digital Sensors:

- Here data conversion and transmission takes place digitally.
- Signals are converted into digital format by the sensor itself.
- These signals are transmitted digitally through wire.
- In digital sensors, change of states is sensed in the form of 0s and 1s.
- It includes IR (infrared sensor), ultrasonic, float, moisture sensors, etc.

| Point of difference | IOT | M2M |
|---|---|---|
| Full form | Internet of Things | Machine to Machine |
| Intelligence | IOT devices have objects that are responsible for decision making | Some degree of intelligence is observed in this. |
| 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 are used |
| 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. |
| Type of Communication | It supports cloud communication | It supports point-to-point communication. |
| Computer System | Involves the usage of both Hardware and Software. | Mostly hardware-based technology |
| 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 APIs |

| | | |
|---|---|---|
| It requires | Generic commodity devices. | Specialized device solutions. |
| Centric | Information and service centric | Communication and device centric. |
| Approach used | Horizontal enabler approach | Vertical system solution approach. |
| Components | Devices/sensors, connectivity, data processing, user interface | Device, area networks, gateway, Application server. |
| Examples | Smart wearable, Big Data and Cloud, etc. | Sensors, Data and Information, etc. |

## Security in IOT:

### 1. CIA Triad:

#### a. Confidentiality:

- It ensures that only authorized users will have the access to the underlying information.
- It ensures the privacy by preventing unauthorized access to the information which is stored and transmitted using the IOT infrastructure.

#### b. Integrity:

- It ensures that only authorized users are allowed to modify the stored information.
- It makes sure that unauthorized users will not be allowed to change (i.e. read, write, delete or update) the data in any manner at any time.

### c. Availability:

- It ensures that only authorized users can have access to the information as and when it is required. Including the fault tolerance.
- Fault tolerance can be built into the IOT architecture by ensuring that the backup components are present for each of the component (i.e. server, storage, networks).
- It also ensures that the **backup server** is an identical copy of the primary server so that backup server can immediately take over the role of primary server whenever they fail.
- **Storage backup** can be ensured by using highly scalable RAID (Redundant Array of Independent Disks) architecture where duplicate data is striped and mirrored across the multiple hard disk, so even if one disk fails the data would not be lost and be there on some other disk.
- Fault tolerance in **networks** can be ensured by providing multiple switches, ports and cables between the two connecting endpoints. This will ensure that the failure of any one network component will not harm the transfer of data over the network.

## 2. AAA Framework:

### a. Authentication:

- It checks that a user's credentials are valid, so the users with invalid credentials will not be allowed to access the information.
- Most common form of authentication can be by using user names and passwords, but as the hacking techniques are evolving so the authentication techniques also have to be sophisticated.
- Thus **multi-factor authentication** comes into picture, where it uses a combination of parameters to authenticate user credentials.
- Ex: 1st factor: user name and password, 2nd factor: a secret random key is being generated which is only known to the user,

3rd factor: verifying biometrics (i.e. fingerprint scan, iris recognition, face recognition, voice detection, etc.)

- Multi-factor authentication could use multiple ways to verify user credentials.
- Sometimes it may be done using only two factors, and thus it is termed as **"two-factor authentication"**.

**b. Authorization:**

- It ensures that a specific user has rights to perform specific operations on a specific object, by providing different permissions.
- The permissions are granted to the user based on their role in the organization.
- The permissions could be as follows:
  - Read only: the user can only view/read the data.
  - Read & Write: the user can view, add, update and delete the data.

**c. Audit Trial:**

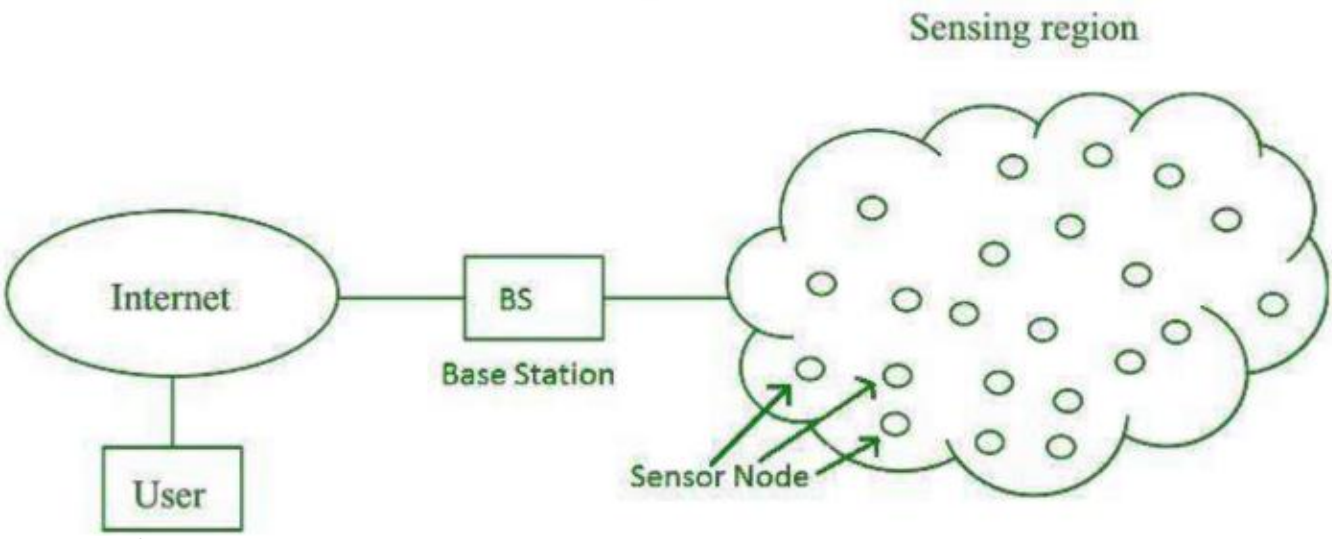
- It is an activity conducted periodically to assess the effectiveness of the security measures by keeping an audit log.
- **Audit log** keeps a track of the operations that are performed by the different users.

## IOT enabling techniques:

- IOT enabling techniques are as follows:
  - Wireless Sensor Network (WSN)
  - Cloud Computing
  - Big Data Analytics
  - Communication Protocols
  - Embedded Systems

## 1. Wireless Sensor Network (WSN):

- It comprises of devices with sensors which are used to monitor the environmental and physical condition.
- WSN is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.
- It consists of **end nodes, routers and coordinators.**
- End nodes have several routers attached to them where the data is passed to the coordinator by the routers.
- The coordinator acts as the gateways that connects WSN to the internet.
- Example:
  - Weather monitoring devices
  - Soil moisture monitoring devices
  - Surveillance systems
  - Health monitoring systems, etc.




- Sensor nodes are used in WSN with the on-board processor that manages and monitors the environment at particular area.
- They are connected to the base station which acts as a processing unit in WSN system.

- Base stations are connected through the internet to share data used for processing, analysis, storage and mining of the data.
- Base station or sink acts like an interface between the users and the network.
- Sensor nodes can communicate amongst themselves using radio signals.
- A WSN contains hundreds of thousands of sensor nodes.
- A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components.

- **Applications of WSN:**
  - Military applications
    - Communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting system.
  - Surveillance and monitoring security, threat detection
  - Environmental temperature, humidity
    - Pollution monitoring, forest fire detection, greenhouse monitoring, etc.
  - Transportation
    - Real-time traffic information to alert drivers of traffic problems.
  - Medical applications
    - Diagnosis, drug administration in hospitals, tracking and monitoring doctors and patients in the hospital.
  - Agriculture
    - Automated irrigation, cultivation according to the weather.
  - Industrial monitoring
    - Significant cost savings and enabling new functionalities.
  - Infrastructural monitoring
    - Monitoring the movement within infrastructure such as bridges, flyover, embankments, tunnels, etc. enabling engineering practices to monitor assets remotely without the need for costly site visit.

## ➢ Challenges of WSN:

- Quality of service
- Security issue
- Energy efficiency
- Network throughput
- Performance
- Ability to cope with network failure
- Scalability to large scale of deployment
- Cross layer optimization

## ➢ Components of WSN:

- **Sensors:** They capture the environmental variables and use it for data acquisition. Sensor signals are converted in to electrical signals.
- **Radio Nodes:** It receives the data produced by the sensors and sends it to access points.
- It consists of microcontroller, transceiver, external memory and power source.
- **WLAN Access Points:** It receives the data which is sent by the radio nodes wirelessly, generally through internet
- **Evaluation Software:** The data received by the access point is processed by this software for presenting it to the users for further processing of the data which is used for processing, analysis, storage and mining of the data.

## 2. Cloud Computing:

- It provides a means by which we can access applications as utilities over the internet.
- Cloud is something that is present at remote locations.
- The users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.
- Characteristics of cloud computing includes:
  - Broad network access
  - On demand self-service
  - Rapid scalability
  - Measured services
  - Pay-per-use

### ➢ Services provided by Cloud Computing

#### (a) Infrastructure as a Service (IaaS):

- It provides online services such as physical machines, virtual machines, servers, storage on pay per use service.
- Major IaaS providers are Google Compute Engine, Amazon Web Services, Microsoft Azure, etc.

#### (b) Platform as a Service (PaaS):

- It provides a cloud based environment required to support the complete life cycle of building and delivering cloud applications without the cost and complexity of buying and managing the required hardware, software 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.

**(c) Software as a Service (SaaS):**

- Delivering applications as a service over the internet.
- SaaS applications are sometimes called web-based software, on-demand software or hosted software.
- Instead of installing and maintaining the software, you simply access it via the internet, and no complex software and hardware management.
- Ex: Google docs, Gmail, Google slides, etc.

## 3. Big Data Analytics:

- It refers to the method of studying massive volumes of data.
- Collection of data whose volume, velocity and variety is simply too massive and tough to store, control, process and examine the data using traditional databases.
- Big data can be gathered from social network videos, digital images, sensors and sales transaction records, etc.
- It is a process used to extract meaningful insights, such as hidden patterns, unknown correlation, market trends and customer preferences.
- Ex: Spotify, youtube, etc. In such platforms, they have millions of users that generate a tremendous amount of data every day. Through this information, the cloud-based platform automatically generates the suggested songs through a smart recommendation engine based on likes, shares, search history, etc.
- **Big Data:** it is a massive amount of data sets that cannot be stored, processed, or analyzed using traditional tools.
- Today there are millions of data sources that generates data at a very rapid rate which are present across the world.
- This data exists in different formats like, structured, semi-structured and unstructured format data.

## ➢ Benefits or Advantages of Big Data Analytics:

- Risk Management
  - Banking companies use big data analytics to identify fraudulent activities and discrepancies. The organization would use it to get a list of suspects or root cause of the problem.
- Product Development and Innovations:
  - Ex: Rolls-Royce (one of the largest manufacturers of jet engines) uses big data analytics to analyze how efficient the engine designs are and if there is any need for improvements.
- Quicker and Better Decision Making within the Organization:
  - Ex: Starbuck uses big data analytics to make strategic decision about opening a new outlet at a specific location by analyzing multiple factors like population, demographics, accessibility of the location and many more.
- Improve Customer Experience:
  - Ex: Delta Air Lines uses big data analytics to improve its customer's experience. It monitors tweets to find out their experience regarding their journey, delays and other things. The airline will identify negative tweets and do whatever is necessary for that particular situation.

## ➢ Life cycle or Phases of Big Data Analytics:

- **Business Case Evaluation –** Define the reason and goal behind the analysis.
- **Identification of data –** Broad variety of data sources are identified.
- **Data filtering –** Variety of data sources are filtered here to remove corrupt data.
- **Data Extraction –** Incompatible data are transformed into the compatible data.
- **Data aggregation –** Data with the same fields across different datasets are integrated.

- **Data analysis –** Data is evaluated using analytical and statistical tools to discover useful information.
- **Visualization of data –** Graphic visualization (i.e. generating graphs, charts, pictures, etc.) of the analysis is prepared using the tools like Tableau, QlikView, etc.
- **Final analysis result –** The final results of the analytics is made available to the stakeholders who will take the action.

## ➢ Types of Big Data Analytics:

### (a) Descriptive Analytics:

- This summarizes past data into a form that people can easily read.
- This helps in creating company's reports. Like a company's revenue, sales, profit/loss, etc.
- Scenario: A company uses data to analyze facility utilization across its office and lab space. Using the analytics, company can identify the underutilized space and thus can use it effectively saving a lot of money and space.

### (b) Diagnostic Analytics:

- This helps to understand what caused a problem in the first place.
- It provides an in-depth insight into a particular problem.
- Ex: data mining, data recovery, etc.
- Scenario: sales of an e-commerce company going down. Many customers are adding their products to the cart but not buying them due to many different reasons like delivery charges, taxes, delivery duration and location, less payment options available, etc. The company diagnosis the reason behind the issue.

**(c) Predictive Analytics:**

- This analytics looks into past and present data to make predictions of the future.
- It uses artificial intelligence, data mining and machine learning to analyze current data and make predictions about the future.
- Ex: studying customer trends, market trends, etc.
- Scenario: precautions required to protect clients of PayPal. The company uses predictive analytics to study the historical payment data of a user and determine the user's behavior to generate an algorithm that predicts the future fraudulent activities.

**(d) Prescriptive Analytics:**

- It prescribes the solution to a particular problem and works with both descriptive and predictive analytics.
- It mostly relies on artificial intelligence and machine learning.
- Scenario: to maximize airlines' profit. Using prescriptive analytics the airlines company will generate an algorithm which will automatically adjust the flight fares based on various factors like customer demand, weather conditions, destination, holiday season and oil prices.

## Big Data Analytics Tools:

- **Hadoop –** It 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 amount of data
- **Storm –** An open-source real-time computational system
- **Kafka –** A distributed streaming platform that is used for fault-tolerant storage.

- **Applications of Big Data Analytics:**
  - Ecommerce – Predicting customer trends and optimizing prices.
  - Marketing – Big data analytics helps to drive high return on investments marketing campaigns, which results in improved sales.
  - Education – Used to develop new and improve existing courses based on user requirements.
  - Healthcare – With the help of patient's past medical history, big data analytics helps to predict the future health issues.
  - Media and Entertainment – Used to understand the demand of any show, movie, songs and deliver a personalized recommendation list to the users.
  - Banking – Customer's income and spending patterns helps to predict various banking offers like loans or credit cards.
  - Telecommunications – used to forecast network capacity and improve customer experience.
  - Government – Big data analytics helps the government for law enforcements among the other things.

## 4. Communication Protocols:

- They are the backbones of IOT systems and enable network connectivity and linking to applications.
- It allows devices to exchange data over the network.
- A group of protocols designed to work together is known as **protocol suite.**
- When implemented in software they are a **protocol stack.**
- It is used in:
  - Data encoding
  - Addressing schemes

## 5. Embedded Systems:

- It is a combination of hardware and software used to perform some special task.
- Embedded systems can be thought of as a computer hardware system having software embedded in it.
- Embedded system can be independent or it can be a part of any large system.
- It includes microcontroller and microprocessor memory, networking units, input-output units and storage devices.
- It collects the data and sends it to the internet.
- Embedded systems are designed for specific task, ex.: fire alarm system will only sense the smoke and provide fire alert based on the signals.
- Ex: digital camera, DVD player, industrial robots, wireless routers, etc.
- Embedded system has a hardware, an application software and a real time OS.
- The **Real-Time Operating System (RTOS)** supervises the application software and provides mechanism to let the processor run as per the scheduling done by following a plan to control the latency (i.e. the delay in network communication). RTOS defines the way system will work. RTOS sets the rules during the execution of an application program.

### Characteristics of Embedded Systems:

- **Single functioned:**
  - Embedded systems usually perform a specialized operation and odes the same task repeatedly as they are designed for a specific task only.
- **Tightly constrained:**
  - Design metrics is a measure of implementation's features such as cost, size, power and performance.
  - It must be of a size to fit on a single chip, and must perform fast enough to process the data in real-time and consume minimum power to entend the battery life.

- **Reactive and Real-time:**
  - Many embedded systems (like fire-alarm system, radar-system in army, etc.) must continuously react to the changes in the system's environment and generate some results based on real-time without any delays.
- **Microprocessor based:**
  - It must be microprocessor or microcontroller based.
- **Memory:**
  - It must have a memory, as its software is usually embedded into ROM.
  - It does not need any secondary memory.
- **Connected:**
  - It must have connected peripheral for the input and output devices.
- **HW-SW systems:**
  - Software is used for more features and flexibility.
  - Hardware is used for performance and security.

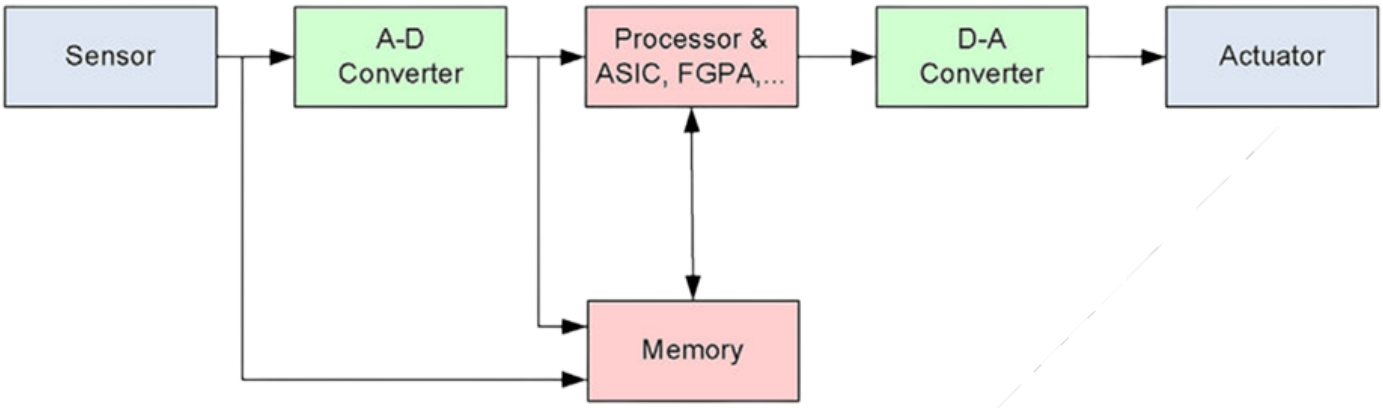
## ➢ Advantages of Embedded Systems:

- Easily customizable
- Lower power consumption
- Low cost
- Enhanced performance

## ➢ Disadvantages of Embedded Systems:

- High development efforts
- Larger time to market

## ➢ Basic structure of Embedded Systems:




- **Sensor –**
  - It measures the physical quantity and converts it to an electrical signals which can be read by any electronic instrument.
  - A sensor stores the measured quantity to the memory.
- **Memory –**
  - It stores all the inputs and the outputs (i.e. analog signals to processed digital data).
- **A-D Converter –**
  - An analog-to-digital converter converts the analog signal sent by the sensor into digital signal.
- **Processor & ASICs –**
  - It processes the data to measure the output and store it to the memory. (ASIC - Application Specific Integrated Circuits)
- **D-A Converter –**
  - A digital-to-analog converter converts the digital data generated by the processor to the analog data.
- **Actuator –**
  - It compares the output given by the D-A converter to the actual or expected output stored in it and stores the approved output.