Unit 2. IoT and M2M

Sonawane Khushbu K.

Introduction M2M

- Machine-to-Machine (M2M) communication, also called M2M/IoT, is a more advanced form of the Internet where many devices connect with each other. Imagine a world where devices communicate without human intervention – it's like they're sharing secrets. Moreover, M2M makes our gadgets work together smoothly, like an unseen director backstage at a play. These devices share info effortlessly, helping things run better in industries and cities. So, if you're curious about how things behind the scenes work and make our world smarter, let's dive in together!

What Exactly Is Machine-to-Machine (M2M) Communication?

- Machine-to-machine is a term for technology that lets machines talk to each other and do things without people helping them. This works with AI and machine learning, which help the machines communicate and make their own choices.

- At first, M2M was used in factories and industries to control machines from far away using things like SCADA and remote monitoring. Now, M2M is used in healthcare, business, insurance, and more. It’s also the basis for the Internet of Things (IoT), where lots of devices connect and share information

- **Supervisory control and data acquisition (SCADA)**

Are IoT and M2M the Same? (IoT vsM2M)

- Although some use these terms interchangeably, M2M and IoT have distinct differences. Think of IoT as a bigger concept, while M2M is a part of it.

- Often, machines communicate directly, either on their own or via M2M. The IoT, on the other hand, is a network of different systems that work together.

- Moreover, M2M connects or interacts with devices directly, while IoT uses the internet to link them and establish a connection.

- In simple terms, machine-to-machine helps manage processes, while IoT goes beyond that, enhancing businesses and user experiences.

- For instance, M2M might help a vending machine alert someone that it’s low on snacks. On the other hand, with IoT, the vending machine could even predict your favourite snacks and offer them to you. Remember, IoT expands on M2M, making it even more powerful.

Now Let's Look at a Few Key features of M2M

- **Efficient Energy Use for Enhanced M2M:** The M2M system conserves energy, leading to improved performance in M2M applications.

- **Seamless Data Exchange in M2M:** Network operators utilize organized data packets to ensure smooth information sharing among machines in M2M communication.

- **Rapid Event Detection:** Through monitoring, the system swiftly identifies events.

- **Flexible Data Timing:** Data transfers can tolerate minor delays.

- **Scheduled Information Sharing:** Data is transmitted or received at specific, pre-defined times.

- **Location-Based Device Notifications:** Devices receive alerts when entering specific areas.

- **Steady and Small-Scale Data Transfer:** The system maintains a consistent flow of small data packets.

How Exactly Does Machine-to-Machine (M2M) Work?

- Let’s think of machine-to-machine (M2M) technology as a way for gadgets to interact or communicate with each other. They use special info sensors to share information about things like temperature or if they’re working right. Then, they send these messages to a big network.

- Unlike other ways of keeping an eye on gadgets from far away, M2M uses regular networks like Wi-Fi or cell signals. This makes it way more cost-effective.

- **M2M has three important parts:** sensors (like tiny detectors), RFID (a tag that tracks things), a way for gadgets to talk (like Wi-Fi or cell signals), and smart software that helps devices understand info and make choices. This software can also make devices do things independently based on the information they get.

- **Radio-frequency identification** (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects.

- **Read Also:** **Can IoT Make A Difference In Smart Manufacturing And Industrial Sector?**

- We knew people used phones and radios to send info long ago. But now, we use the internet and better wireless devices to do the same thing. Even everyday things like heaters and meters can use this kind of communication.

- The interesting fact here is it saves money. The interesting fact here is that it leads to cost savings. This is because gadgets experience fewer breakdowns, resulting in reduced repair expenses.

- In addition, companies can explore new revenue streams by effectively maintaining their equipment. And if something might go wrong, they can fix it before it gets bad. So, it's like gadgets helping each other and making life easier for us all!

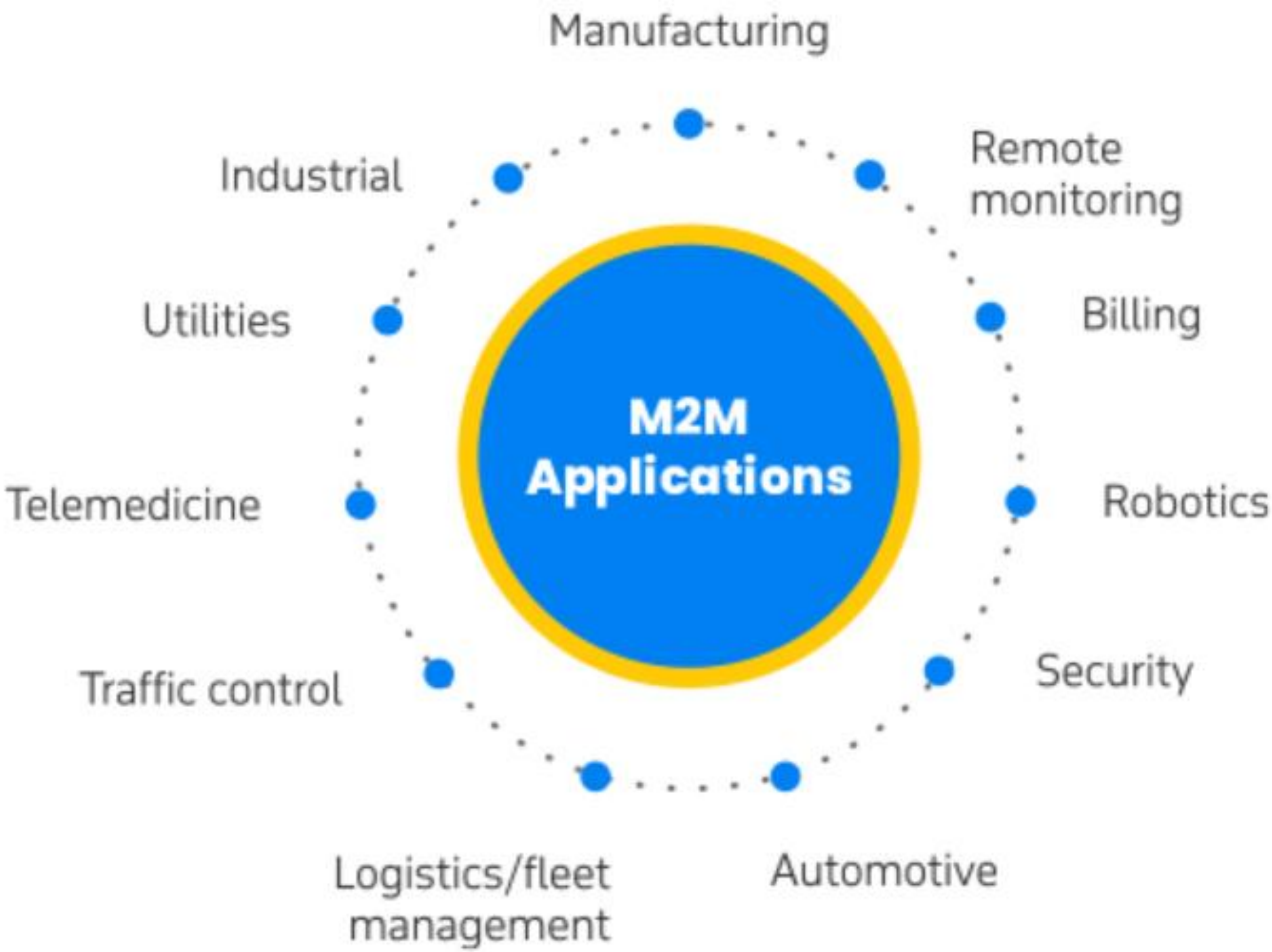
Here are the best things about M2M:

- Saves money by keeping gadgets in good shape and not having to fix them often.
- Helps businesses make more money by finding new ways to take care of their assets.
- Makes customer service better by checking and fixing things before they break or when needed.

Now Let's Look at a Few Popular Applications & Examples of M2M

- Machine-to-machine communication is often used for checking things from far away. For example, a vending machine can send a message to get more items when it's running low. Also, M2M helps watch over things like warehouse items and how things move from one place to another.

- Presently, many utility companies are really relying on M2M gadgets. As a result, they use them to get energy like oil and gas, send bills using smart meters, and see how things are going at work sites, like pressure, heat, and if the equipment is okay.


Manufacturing
Remote monitoring
Billing
Robotics
Security
Automotive
Logistics/fleet management
Traffic control
Telemedicine
Utilities
Industrial
M2M Applications

- Today, M2M tools are doing many big things in telemedicine. They watch over patients in real-time, give medicine by themselves, and track medical stuff. Great, isn’t it?

- Moreover, today the blend of IoT, AI, and ML is reshaping mobile payments, evident in systems like Google Wallet and Apple Pay. As a result, M2M financial operations are becoming increasingly popular.

- Furthermore, modern smart homes utilize M2M to manage devices and communicate over long distances remotely.

- Moreover, M2M plays a crucial role in various other domains, including the manufacturing industry, remote control of objects through software, robots, and traffic systems, ensuring safety, repositioning items, managing fleets of vehicles, and automotive applications

The Bottom Line

- In the world of technology, IoT and M2M are like magic threads weaving a tapestry of connectivity. It means smoother operations, better decisions, and satisfied customers for businesses, and people can enjoy smarter homes, healthier lives, and seamless experiences. But this is just the beginning. Imagine cities getting smarter, healthcare becoming handier, and industries evolving seamlessly. With IoT and machine-to-machine communication, the future holds a promise of a more connected and efficient world where innovation touches every aspect of our lives.

- **Why is machine-to-machine communication important?**
- Machine-to-machine communication decreases time, conserves bandwidth, and enables machines to act independently. Moreover, the goal is to minimize human involvement and tasks.

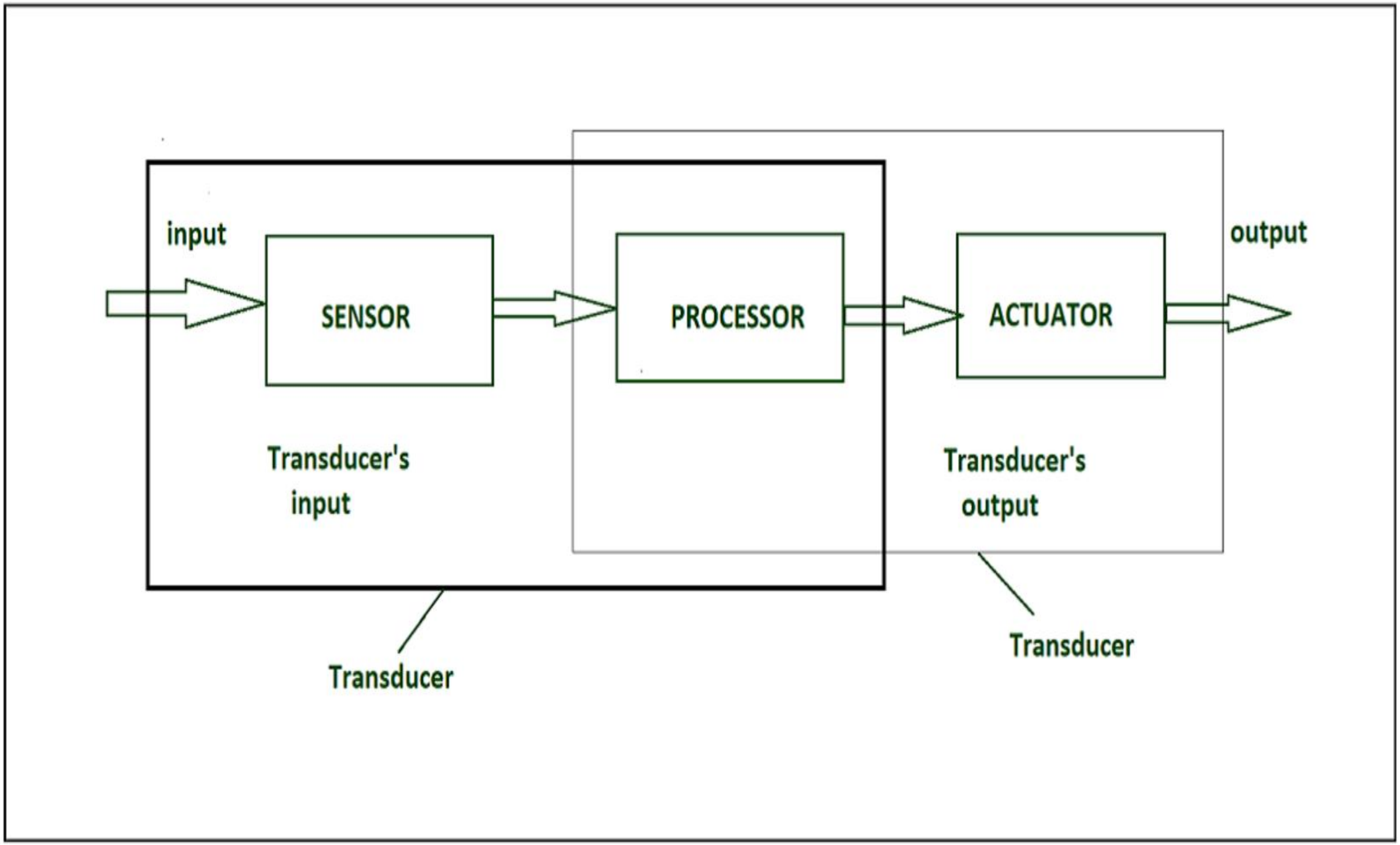
- **Why is machine-to-machine communication important in IoT?**
- M2M communication is crucial in IoT because it enables real-time operation and remote interaction of devices. Moreover, it enhances remote control, robotics, security, traffic, logistics, fleet management, and automotive functions.

- **What is an example of machine-to-machine communication?**
- An example of machine-to-machine communication is when a smart thermostat adjusts room temperature based on data from your phone’s location and weather forecasts. ATMs are also examples of machine-to-machine, as they notify the authorities when they are running low on cash.

- **What are the types of machine-to-machine communication?**
- There are primarily two types of machine-to-machine communication technology: wired and wireless (non-wired).

Introduction to Sensor Technology

- Generally, sensors are used in the architecture of IOT devices.
- **Sensors** are used for sensing things and devices etc.
- A device that provides a usable output in response to a specified measurement.
  The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity.
  The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance, etc.


input
SENSOR
PROCESSOR
ACTUATOR
output
Transducer's
input
Transducer's
output
Transducer
Transducer

- **Transducer :**
- A transducer converts a signal from one physical structure to another.
- It converts one type of energy into another type.
- It might be used as actuator in various systems.

- **Sensors characteristics :**
- Static
- Dynamic
- **1. Static characteristics :**
  It is about how the output of a sensor changes in response to an input change after steady state condition.
- **Accuracy:** Accuracy is the capability of measuring instruments to give a result close to the true value of the measured quantity. It measures errors. It is measured by absolute and relative errors. Express the correctness of the output compared to a higher prior system. Absolute error = Measured value – True value
  Relative error = Measured value/True value

- **Range:** Gives the highest and the lowest value of the physical quantity within which the sensor can actually sense. Beyond these values, there is no sense or no kind of response.
  e.g. RTD for measurement of temperature has a range of -200`c to 800`c.

- **Resolution:** Resolution is an important specification for selection of sensors. The higher the resolution, better the precision. When the accretion is zero to, it is called the threshold. Provide the smallest changes in the input that a sensor is able to sense.

- **Precision:** It is the capacity of a measuring instrument to give the same reading when repetitively measuring the same quantity under the same prescribed conditions.
- It implies agreement between successive readings, NOT closeness to the true value.
  It is related to the variance of a set of measurements.
  It is a necessary but not sufficient condition for accuracy.

- **Sensitivity:** Sensitivity indicates the ratio of incremental change in the response of the system with respect to incremental change in input parameters. It can be found from the slope of the output characteristics curve of a sensor. It is the smallest amount of difference in quantity that will change the instrument’s reading.

- **Linearity:** The deviation of the sensor value curve from a particularly straight line. Linearity is determined by the calibration curve. The static calibration curve plots the output amplitude versus the input amplitude under static conditions. A curve’s slope resemblance to a straight line describes linearity.

- **Drift:** The difference in the measurement of the sensor from a specific reading when kept at that value for a long period of time.

- **Repeatability:** The deviation between measurements in a sequence under the same conditions. The measurements have to be made under a short enough time duration so as not to allow significant long-term drift.

- **Dynamic Characteristics :**
  Properties of the systems
- **Zero-order system:** The output shows a response to the input signal with no delay. It does not include energy-storing elements.
  Ex. potentiometer measure, linear and rotary displacements.
- **First-order system:** When the output approaches its final value gradually.
  Consists of an energy storage and dissipation element.
- **Second-order system:** Complex output response. The output response of the sensor oscillates before steady state.

- **Sensor Classification :**
- Passive & Active
- Analog & digital
- Scalar & vector

- **Passive Sensor –**
  Can not independently sense the input. Ex- Accelerometer, soil moisture, water level and temperature sensors.
- **Active Sensor –**
  Independently sense the input. Example- Radar, sounder and laser altimeter sensors.
- **Analog Sensor –**
  The response or output of the sensor is some continuous function of its input parameter. Ex- Temperature sensor, LDR, analog pressure sensor and analog hall effect.

- **Digital sensor –**
  Response in binary nature. Design to overcome the disadvantages of analog sensors. Along with the analog sensor, it also comprises extra electronics for bit conversion. Example – Passive infrared (PIR) sensor and digital temperature sensor(DS1620).

- **Scalar sensor –**
  Detects the input parameter only based on its magnitude. The answer for the sensor is a function of magnitude of some input parameter. Not affected by the direction of input parameters. Example – temperature, gas, strain, color and smoke sensor.

-
- **Vector sensor –**
  The response of the sensor depends on the magnitude of the direction and orientation of input parameter. Example – Accelerometer, gyroscope, magnetic field and motion detector sensors.

Types of sensors

- **Electrical sensor :**
- Electrical proximity sensors may be contact or non contact.
- Simple contact sensors operate by making the sensor and the component complete an electrical circuit.
- Non- contact electrical proximity sensors rely on the electrical principles of either induction for detecting metals or capacitance for detecting non metals as well.

- **Light sensor:**

- Light sensor is also known as photo sensors and one of the important sensor.
- Light dependent resistor or LDR is a simple light sensor available today.
- The property of LDR is that its resistance is inversely proportional to the intensity of the ambient light i.e when the intensity of light increases, it’s resistance decreases and vise versa.

- **Touch sensor:**
- Detection of something like a touch of finger or a stylus is known as touch sensor.
- It’s name suggests that detection of something.
- They are classified into two types:
- Resistive type
- Capacitive type
- Today almost all modern touch sensors are of capacitive types.
- Because they are more accurate and have better signal to noise ratio.

- **Range sensing:**
- Range sensing concerns detecting how near or far a component is from the sensing position, although they can also be used as proximity sensors.
- Distance or range sensors use non-contact analog techniques. Short range sensing, between a few millimetres and a few hundred millimetres is carried out using electrical capacitance, inductance and magnetic technique.
- Longer range sensing is carried out using transmitted energy waves of various types eg radio waves, sound waves and lasers.

- **Mechanical sensor:**
- Any suitable mechanical / electrical switch may be adopted but because a certain amount of force is required to operate a mechanical switch it is common to use micro-switches.

- **Pneumatic sensor:**
- These proximity sensors operate by breaking or disturbing an air flow.
- The pneumatic proximity sensor is an example of a contact type sensor. These cannot be used where light components may be blown away.

- **Optical sensor:**
- In there simplest form, optical proximity sensors operate by breaking a light beam which falls onto a light sensitive device such as a photocell. These are examples of non contact sensors. Care must be exercised with the lighting environment of these sensors for example optical sensors can be blinded by flashes from arc welding processes, airborne dust and smoke clouds may impede light transmission etc.

- **Speed Sensor:**
- Sensor used for detecting the speed of any object or vehicle which is in motion is known as speed sensor .For example – Wind Speed Sensors, Speedometer ,UDAR ,Ground Speed Radar .

- **Temperature Sensor:**
- Devices which monitors and tracks the temperature and gives temperature’s measurement as an electrical signal are termed as temperature sensors .These electrical signals will be in the form of voltage and is directly proportional to the temperature measurement .

- **PIR Sensor:**
- PIR stands for passive infrared sensor and it is an electronic sensor that is used for the tracking and measurement of infrared (IR) light radiating from objects in its field of view and is also known as Pyroelectric sensor .It is mainly used for detecting human motion and movement detection .

- **Ultrasonic Sensor:**
- The principle of ultrasonic sensor is similar to the working principle of SONAR or RADAR in which the interpretation of echoes from radio or sound waves to evaluate the attributes of a target by generating the high frequency sound waves .

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 day some 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 media known as the internet **or Iot** is an ecosystem of connected physical object that are accessible through internet. Iot means anything which can be connected to internet and can be controlled or monitored using internet from smart devices or PC.

- **2. Machine to Machine :** This is commonly known as Machine to machine communication. It is a concept where two or 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.
- **M2M** is also named as Machine Type Communication (MTC) in 3GPP (3rd Generation Partnership Project).
- **M2M** is communication could carried over mobile networks, for ex- GSM-GPRS, CDMA EVDO Networks .

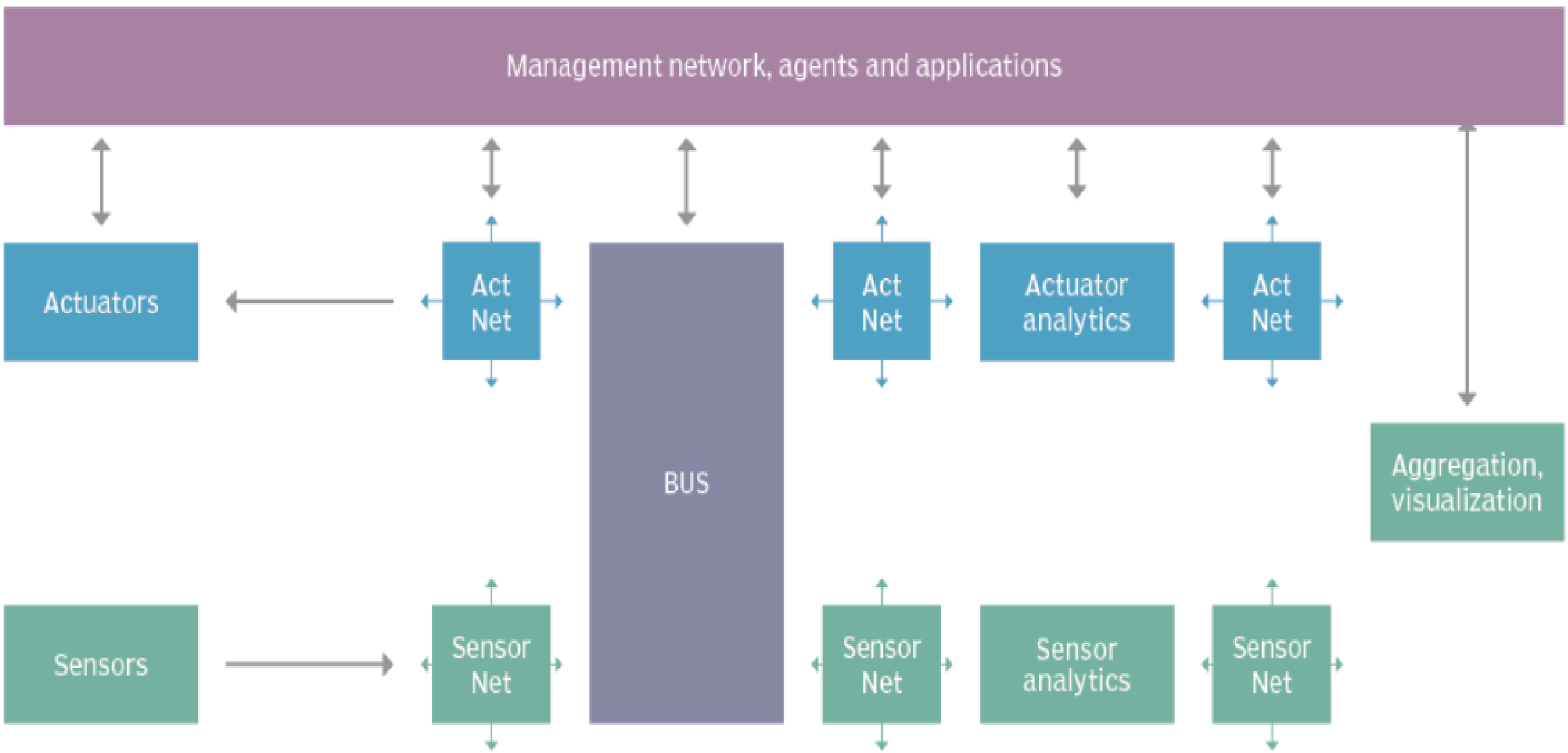
Basis of	IoT	M2M
Abbreviation	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this.
Connection type used	The connection is via Network and using various communication types.	The connection is a 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 wearables, Big Data and Cloud, etc.	Sensors, Data and Information, etc.

IoT security architecture components



- Securing Internet of Things (IoT) devices is crucial to protect against potential threats and vulnerabilities. IoT security involves safeguarding the entire ecosystem, including devices, networks, and the data they generate. Here are some key considerations for ensuring security in IoT:

- **Device Authentication and Authorization:**
- **Unique Credentials:** Each IoT device should have unique, strong credentials such as passwords or cryptographic keys.
- **Authentication Protocols:** Use secure authentication protocols like OAuth or JWT to ensure that only authorized devices can access the network

- **Encryption:**
  - **Data Encryption:** Employ end-to-end encryption to protect data both in transit and at rest.
  - **Secure Communication Protocols:** Use protocols like TLS/SSL for secure communication between devices and servers.

- **Device Management:**
  - **Regular Updates:** Keep devices updated with the latest security patches to address vulnerabilities.
  - **Remote Monitoring and Control:** Implement mechanisms for remote monitoring and management of devices to address security issues promptly.

- **Network Security:**
  - **Firewalls and Intrusion Detection Systems (IDS):** Deploy firewalls and IDS to monitor and protect the network from unauthorized access and attacks.
  - **Segmentation:** Segment the network to limit the impact of a breach and prevent lateral movement of attackers.

- **Physical Security:**
  - **Tamper Detection:** Implement mechanisms to detect physical tampering with devices.
  - **Restricted Access:** Restrict physical access to IoT devices to authorized personnel only.

- **Secure Boot and Firmware Integrity:**
  - **Secure Boot:** Ensure that only signed and authenticated firmware is allowed to run on the device.
  - **Firmware Updates:** Implement secure methods for updating firmware to prevent tampering.

- **Privacy Protection:**
  - **Data Minimization:** Collect only the necessary data and avoid unnecessary information.
  - **User Consent:** Obtain explicit user consent for collecting and processing data.

- **API Security:**
  - **Secure APIs:** Implement secure APIs with proper authentication and authorization mechanisms.
  - **API Rate Limiting:** Use rate limiting to protect against API abuse and denial-of-service attacks.

- **Monitoring and Logging:**
  - **Real-time Monitoring:** Implement real-time monitoring to detect and respond to security incidents promptly.
  - **Audit Logs:** Keep detailed logs for auditing and forensic analysis in case of a security breach.

- **Regulatory Compliance:**
  - **Adherence to Standards:** Ensure compliance with relevant security standards and regulations (e.g., GDPR, HIPAA).

- **Vendor Security Assessment:**
  - **Thorough Evaluation:** Assess the security practices of IoT device vendors before procurement.
  - **Security Certifications:** Prefer devices with security certifications to ensure a certain level of security.

- **Incident Response Plan:**
  - **Preparedness:** Develop and regularly update an incident response plan to address security breaches effectively.

- Implementing a comprehensive security strategy requires collaboration among device manufacturers, network providers, and end-users to create a secure and resilient IoT ecosystem. Regular security audits and ongoing vigilance are essential to adapt to evolving threats and maintain a high level of IoT security.

THE END