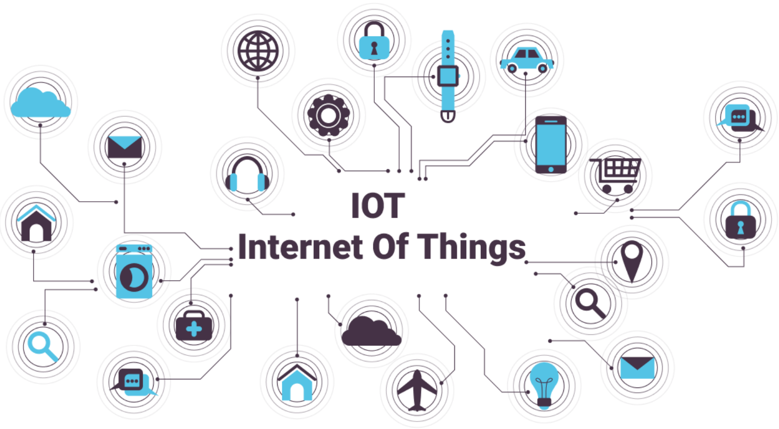
Computer Networks & Internet of Things
Module
Introduction to Internet of Things (IoT)

Jaypee Institute of Information Technology, Noida

Overview

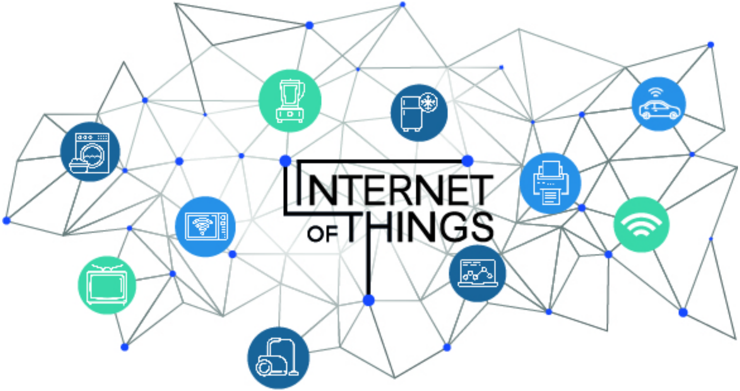
1. Introduction to Internet of Things
2. Internet of Things Reference Model
3. Internet of Things Reference Architecture
4. Machine to Machine Communication Architecture
5. Internet of Things Devices


IOT
Internet Of Things

Introduction to IoT

Definition

IoT is the network of physical objects or things embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.



IoT Components

"**Things**" or **objects** are designed in such a way that they can engage in communication without human intervention. IoT consists of the following components:

- Physical Object (Controller, Sensor and Actuators)
- Connectivity (Internet)

Controller

is a hardware device or a software program that manages or directs the flow of data between two entities. In computing, controllers may be cards, microchips, or separate hardware devices for the control of a peripheral device.

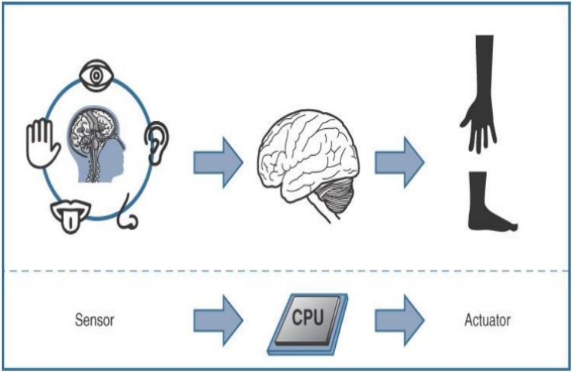
Sensor

The sensors basically sense the physical phenomena occurred near by to the sensor. Moreover, sensors or devices help in collecting very minute data from the surrounding environment.

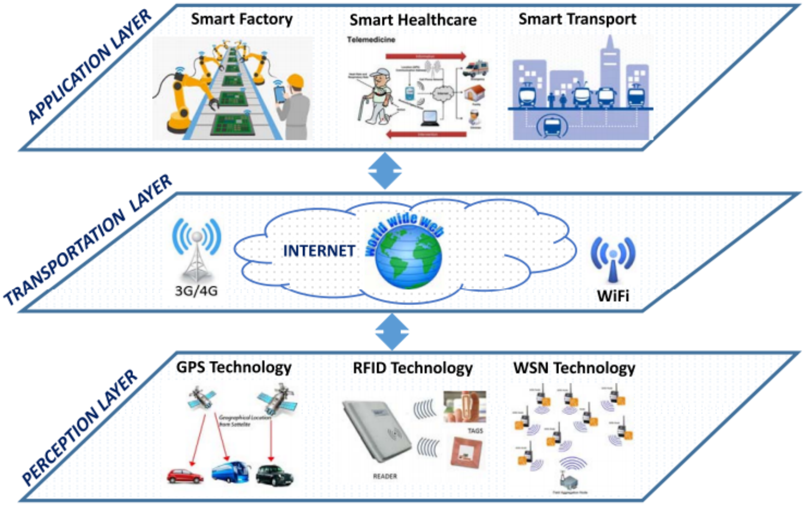
IoT Components

Actuators

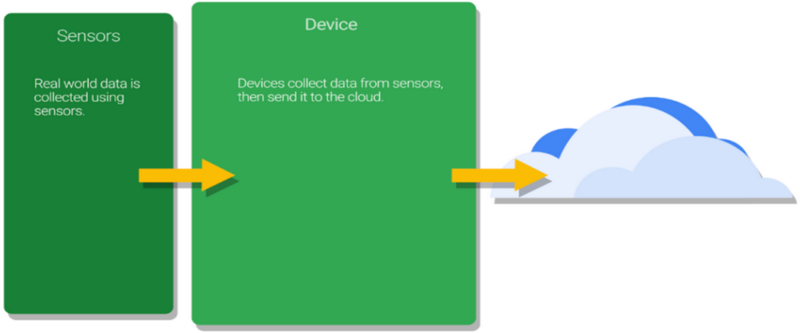
the actuators basically based on the sensed information. Actuators, performs operation in physical environment. Moreover, we can say that actuator performs operation, which is based on the sensed information.



IoT : Layered Architecture



IoT : Working


Sensors
Real world data is collected using sensors.
Device
Devices collect data from sensors, then send it to the cloud.

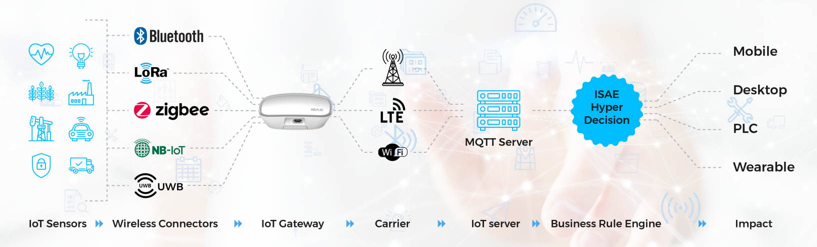
Sensor closely monitor the environmental changes and forward the information to its base station device, which is further transferred ot the cloud or processing centre.

IoT : Working

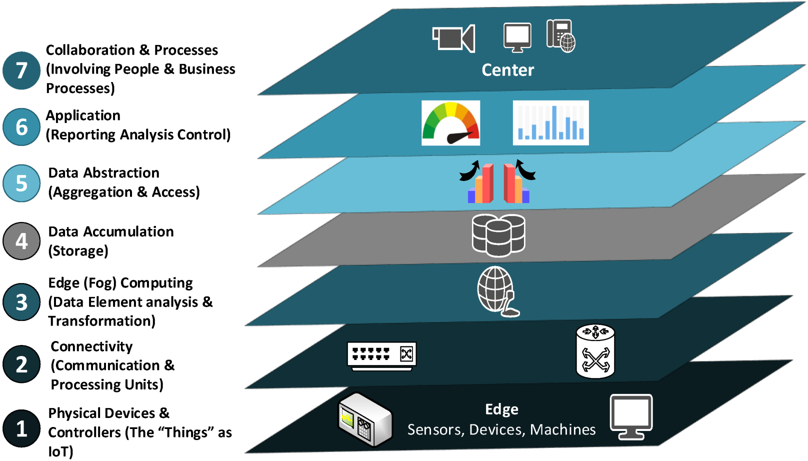
Connectivity

- Sensor or Device can use short range communication interface according to the need. We have a wide variety of communication interface such as **RFID, NFC, Wi-Fi, Bluetooth(BLE), and Zigbee**.
- Sensors can also use long range communication interface such as **GSM, GPRS, 3/4G, and LTE**

IoT : Working Together



IoT Reference Model


7
Collaboration & Processes (Involving People & Business Processes)
6
Application (Reporting Analysis Control)
5
Data Abstraction (Aggregation & Access)
4
Data Accumulation (Storage)
3
Edge (Fog) Computing (Data Element analysis & Transformation)
2
Connectivity (Communication & Processing Units)
1
Physical Devices & Controllers (The "Things" as IoT)
Center
Edge
Sensors, Devices, Machines

IoT world Forum proposed a reference model to provide the introductory walk through to develop the IoT APPLICATIONS.

IoT Reference Model

- **Physical Devices and Controllers:**
  - This layer represent the “things” in the Internet of Things.
  - Although, this layer is a little ambiguous. On the one hand, the “things” are the assets being managed. From a system design perspective, the “things” are the sensors and devices that are directly managed by the IoT architecture.
- **Connectivity:**
  - This layer spans from the the “middle” of an Edge Node device up through transport to the cloud.
  - Many alternatives can be used for communications and this layer includes the mapping of field data to the logical and physical technologies used as well as the backhaul to the on premise or cloud and the next layer, Edge Computing.

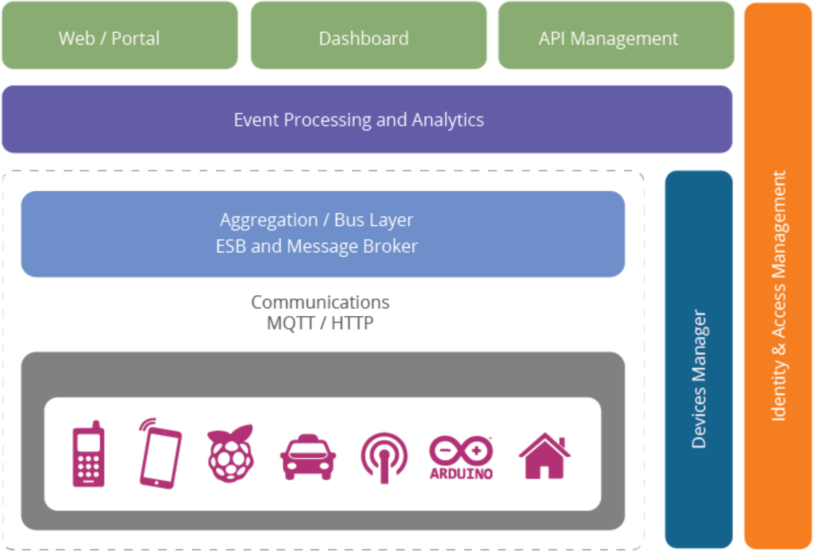
IoT Reference Model

- **Edge Computing:**
  - The next layer in the World Forum Model architecture is Edge Computing, or more properly "Cloud Edge" or "Cloud Gateway" computing.
  - Protocol conversion, routing to higher layer software functions and even fast path logic for low latency decision making will be implemented at this layer.
- **Data Accumulation:**
  - Given the Velocity, Volume and Variety that IoT systems can provide it is essential to provide incoming data storage for subsequent processing, normalization, integration, and preparation for upstream applications.
  - This layer may be implemented in simple SQL or may require more sophisticated Hadoop & Hadoop File System, Mongo, Cassandra, Spark or other NoSQL solutions.

IoT Reference Model

- **Data Abstraction :**
  - Data abstraction layer we “make sense” of the data, collecting “like” information from multiple IoT sensors or measurements, expedite high priority traffic or alarms, and organize incoming data from the data lake into appropriate schema and flows for upstream processing.
- **Application Layer:**
  - This layer is self explanatory and is where control plane and data plane application logic is executed. Monitoring, process optimization, alarm management, statistical analysis, control logic, logistics, consumer patterns, are just a few examples of IoT applications.
- **Collaboration and Processes :**
  - At this layer, application processing is presented to users, and data processed at lower layers is integrated in to business applications.
  - This layer is about human interaction with all of the layers of the IoT system and where economic value is delivered.

IoT Reference Architecture



IoT Reference Architecture

The reference architecture consists of a set of components. Layers can be realized by means of specific technologies, and we will discuss options for realizing each component. There are also some cross-cutting/vertical layers such as access/identity management.

The layers are

- Client/external communications - Web/Portal, Dashboard, APIs
- Event processing and analytics (including data storage)
- Aggregation/bus layer ESB and message broker
- Relevant transports - MQTT/HTTP/XMPP/CoAP/AMQP, etc.
- Devices

The cross-cutting layers are

- Device manager
- Identity and access management

IoT Reference Architecture : The Device Layer

- The bottom layer of the architecture is the device layer.
- Devices can be of various types, but in order to be considered as IoT devices, they must have some communications that either indirectly or directly attaches to the Internet.
- Examples of direct connections : Arduino with Arduino Ethernet connection, Raspberry Pi connected via Ethernet or Wi-Fi
- Each device typically needs an identity.
  - A unique identifier (UUID) burnt into the device (typically part of the System-on-Chip, or provided by a secondary chip)

The specification is based on HTTP; however, (as we will discuss in the communications section) the reference architecture also supports these flows over MQTT.

IoT Reference Architecture : The Communications Lay

The communication layer supports the connectivity of the devices. There are multiple potential protocols for communication between the devices and the cloud. The most wellknown three potential protocols are

- HTTP/HTTPS (and RESTful approaches on those)
- MQTT 3.1/3.1.1
- Constrained application protocol (CoAP)

IoT Reference Architecture : The Aggregation/Bus Lay

An important layer of the architecture is the layer that aggregates and brokers communications. This is an important layer for three reasons:

- The ability to support an HTTP server and/or an MQTT broker to talk to the devices;
- The ability to aggregate and combine communications from different devices and to route communications to a specific device (possibly via a gateway)
- The ability to bridge and transform between different protocols, e.g. to offer HTTPbased APIs that are mediated into an MQTT message going to the device.

The aggregation/bus layer provides these capabilities as well as adapting into legacy protocols. The bus layer may also provide some simple correlation and mapping from different correlation models (e.g. mapping a device ID into an owners ID or vice-versa).

The Event Processing and Analytics Layer

This layer takes the events from the bus and provides the ability to process and act upon these events. A core capability here is the requirement to store the data into a database.

This may happen in three forms:

- Traditional model or server side processing model such as JAS-RS application backed with database
- Big data analytic platform and cloud-scalable platform like Apache Hadoop
- Near real-time complex event processing

Client/External Communications Layer

The reference architecture needs to provide a way for these devices to communicate outside of the device-oriented system.

This includes three main approaches:

- we need the ability to create web-based front-ends and portals that interact with devices and with the event-processing layer.
- we need the ability to create dashboards that offer views into analytics and event processing.
- we need to be able to interact with systems outside this network using machine-to-machine communications (APIs). These APIs need to be managed and controlled and this happens in an API management system.

The recommended approach to building the web front end is to utilize a modular front-end architecture, such as a portal, which allows simple fast composition of useful UIs.

Device Management

Device management (DM) is handled by two components.

- **Server side device management**
    - It communicates with devices via various protocols and provides both individual and bulk control of devices.
- **Remotely Software based device managemtn**
    - It also remotely manages software and applications deployed on the device. It can lock and/or wipe the device if necessary.
    - The device manager works in conjunction with the device management agents. There are multiple different agents for different platforms and device types.
- The device manager also needs to maintain the list of device identities and map these into owners.
- It must also work with the identity and access management layer to manage access controls over devices (e.g. who else can manage the device apart from the owner, how much control does the owner have vs. the administrator, etc.)

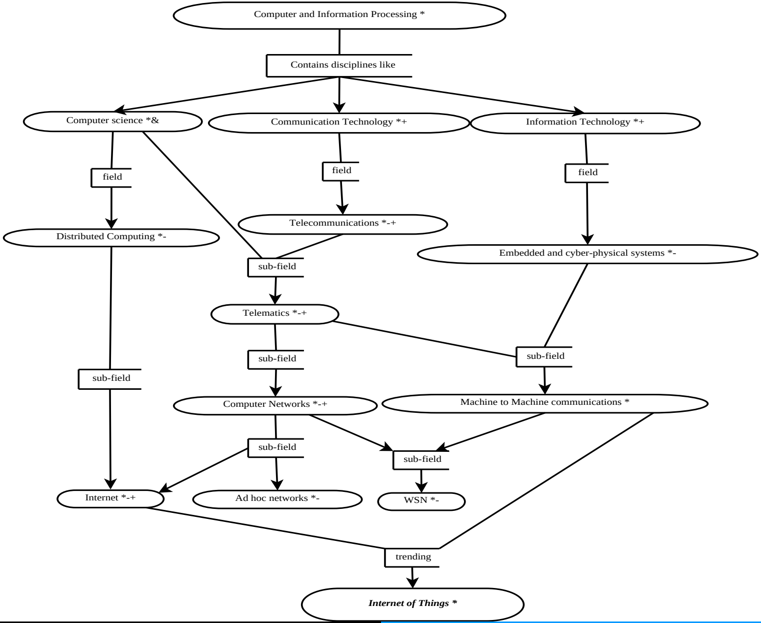
Identity and Access Management

The final layer is the identity and access management layer. This layer needs to provide the following services:

- OAuth2 token issuing and validation
- Other identity services including SAML2 SSO and OpenID Connect support for identifying inbound requests from the Web layer
- XACML PDP
- Directory of users (e.g. LDAP)
- Policy management for access control (policy control point)

The identity layer may of course have other requirements specific to the other identity and access management for a given instantiation of the reference architecture.

Thesaurus Relation Between IoT, WSN, M2M, and CN



Machine to Machine Communication

Definition

Machine-to-machine (M2M) communications means the largely automated exchange of information between technical devices themselves, for example, machines, vending machines, vehicles, or measuring equipment (e.g. electricity, gas and water meters), or between the devices and a central data processing unit.

- M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type.
- 4 basic stages that are common to just about every M2M application.
    1. Collection of data
    2. Transmission of selected data through a communication network
    3. Assessment of the data
    4. Response to the available information

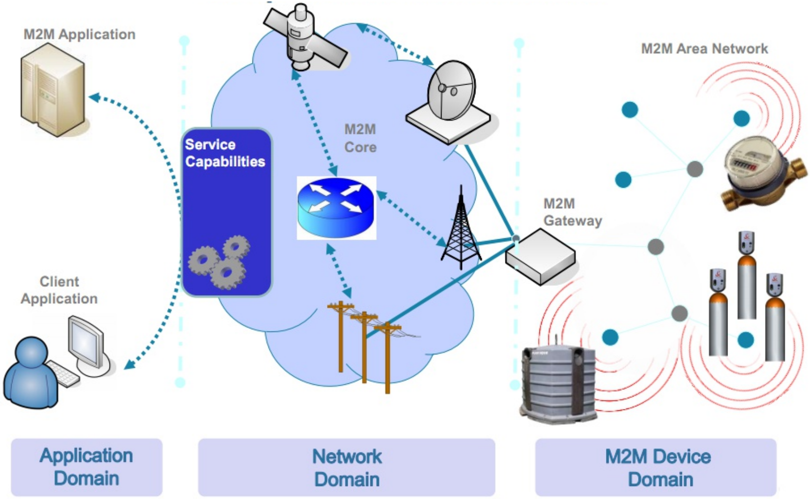
Machine to Machine : Application

- **Security :** Surveillances, Alarm systems, Access control, Car/driver security
- **Tracking & Tracing :** Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering
- **Payment :** Point of sales, Vending machines, Gaming machines
- **Health :** Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics
- **Remote Maintenance/Control :** Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics
- **Metering :** Power, Gas, Water, Heating, Grid control, Industrial metering
- **Manufacturing :** Production chain monitoring and automation
- **Facility Management :** Home / building / campus automation

Machine to Machine : Features

- **Low Mobility :** M2M Devices do not move, move infrequently, or move only within a certain region
- **Time Controlled :** Send or receive data only at certain pre-defined periods
- **Time Tolerant :** Data transfer can be delayed
- **Packet Switched :** Network operator to provide packet switched service with or without an MSISDN
- **Online small Data Transmissions:** MTC Devices frequently send or receive small amounts of data.
- **Monitoring :** Not intend to prevent theft or vandalism but provide functionality to detect the events
- **Low Power Consumption :** To improve the ability of the system to efficiently service M2M applications
- **Location Specific Trigger :** Intending to trigger M2M device in a particular area e.g. wake up the device

Machine to Machine : Architecture



Machine to Machine : Device

- Device capable of replying to request for data contained within those devices or capable of transmitting data autonomously.
- Sensors and communication devices are the endpoints of M2M applications.
- The data endpoint is the system containing the data to be transmitted or monitored. A DEP can be a vending machine that sends inventory information to a central office, an instrument that records weather data, or a medical device that transmits patient health data.
- Data endpoints are microcomputer systems, meaning transmitters that are linked to a receiver.

Device Domain

Provide connectivity between M2M Devices and M2M Gateways, e.g. personal area network.

Machine to Machine : Gateway

- Equipment that uses M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.
- 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. Thus, the task of gateways and routers are twofold.
- Firstly, they have to ensure that the devices of the capillary network may be reached from outside and vice versa.
- Secondly, there may be the need to map bulky internet protocols to their lightweight counterpart in low-power sensor networks.

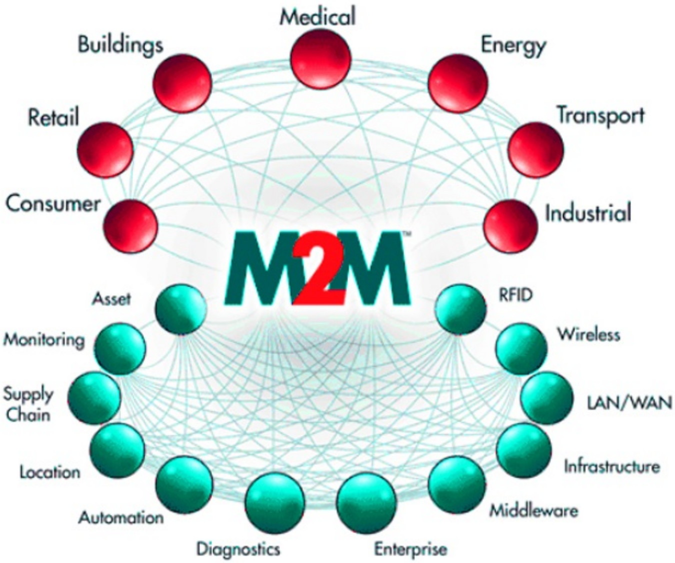
Machine to Machine : Network Domain

- It covers the communications between the M2M Gateway(s) and M2M application(s), e.g. xDSL, LTE, WiMAX, and WLAN.
- There are different types of communication networks for transferring data from one machine to another.
- These include the **cellular networks and wireless or wired Internet connections** that we use every day. However, there are other short range communication technology, which are used for IoT application like:
  - RFID
  - NFC *Bluetooth*

Machine to Machine : Applications

- It contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.
- M2M applications will be based on the infrastructural assets (e.g., access enablers) that are provided by the operator.

Machine to Machine : Applications



M2M vs. IoT

Machine to Machine	**Internet of Things**
M2M is subset of IoT	IoT is super set of M2M. It is a vast network of connected devices that may or may not include human interaction.
Point to point communication usually embedded within hardware at the customer site. Ex (Tap to pay, NFC). The service in Samsung taps to pay without using card. You just need to bring your mobile near the swipe machine. Using your ID card to open or close the door.	Multipoint Communication. Ex: By showing the ID card then your attendance will be registered. Monitoring the health parameters through the help of android app or web app.
It uses cellular or wired network.	It uses wireless network.
The devices used are homogeneous type within an M2M area network.	The devices used are heterogeneous type such as fire alarms, door alarms, lighting control devices, etc..
It is more hardware based.	It is more software based.

M2M vs. IoT

Machine to Machine	**Internet of Things**
On premises applications. (i.e software and technology i.e located within the physical confines of an enterprise or companys data centre.) Ex. Diagnosis applications, Service management applications and on- premises enterprises applications.	It uses cloud based application such as analytic applications, enterprise applications, and remote diagnosis and management applications.
Data collection and analysis is done in on premises storage infrastructure.	Data collection and analysis is done in cloud mostly.
Non IP based communication.	IP based communication.
M2M protocols include ZigBee, Bluetooth, ModBus, M-Bus, Wireless M-Bus, Power Line communication (PLC), 6LoWPAN, IEEE 802.15.4, Z-wave. These protocols work below the network layer.	IoT protocols include HTTP, CoAP, Web Socket, MQTT, XMPP, DDS, AMQP etc.. The protocols work above the network layer.
Do not necessarily require internet connection.	Majority of cases require Internet connection.

IoT Devices

Definition

IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks. They can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more.

The following characteristic should be provided by the IoT devices:

- Intelligence and Identity
- Connectivity
- Dynamic Nature of self adaptance
- Enormous Scale
- Sensing
- Heterogeneity
- Safety & Security

Why IoT Devices ?

Increasingly, IoT devices are using AI and machine learning to bring intelligence and autonomy to systems and processes, such as autonomous driving, industrial smart manufacturing, medical equipment, and home automation.

- Many of these devices are small, power and cost constrained microcontroller-based systems.
- Network bandwidth and consumer expectations around data privacy and user experience continue to demand more on-device processing, where data is processed on the IoT endpoint, rather than using cloud-based approaches.

IoT Devices

- IoT i.e Internet of things, where things refer to the IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities (ex: combination of sensors, actuators, Arduino, relay, non IoT devices).
- The IoT devices can share information with as well as collect information from other connected devices and applications (directly and indirectly).
- They can process the data locally or in the cloud to find greater insights and put them into action based on temporal and space constraints (i.e space memory, processing capabilities, communication latencies and speeds and deadlines).
- IoT devices can be of varied types. For ex: wearable sensors, smart watches, LED lights, automobiles and industrial machines.

Type of IoT Devices

IoT devices depends on the application, where device is actually used, such as:

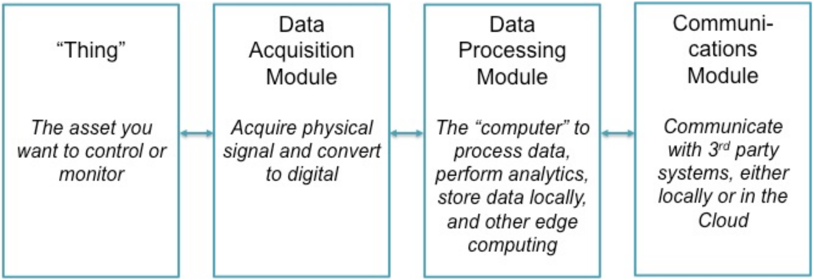
- **Consumer IoT** - Primarily for everyday use. Eg: home appliances, voice assistance, and light fixtures.
- **Commercial IoT** - Primarily used in the healthcare and transport industries. Eg: smart pacemakers and monitoring systems.
- **Military Things (IoMT)** - Primarily used for the application of IoT technologies in the military field. Eg: surveillance robots and human-wearable biometrics for combat.
- **Industrial Internet of Things (IIoT)** - Primarily used with industrial applications, such as in the manufacturing and energy sectors. Eg: Digital control systems, smart agriculture and industrial big data.
- **Infrastructure IoT** - Primarily used for connectivity in smart cities. Eg: infrastructure sensors and management systems.

Top Most IoT Device in 2021

1. Google Home Voice Controller (provide voice enabling services)
2. Amazon Echo Plus Voice Controller (Provide voice enabling services)
3. August Doorbell Cam (Door management facility)
4. August Smart Lock (Security from remote location)
5. Foobot (Measure the indoor pollution)

How IoT Device Work ?

Working of IoT device depends on 4 building blocks.



"Thing"

The asset you want to control or monitor

Data Acquisition Module

Acquire physical signal and convert to digital

Data Processing Module

The "computer" to process data, perform analytics, store data locally, and other edge computing

Communi-cations Module

Communicate with 3^{rd} party systems, either locally or in the Cloud

Building Block 1 : Thing

I define “thing” as the asset you want to control or monitor.

- Many IoT devices integrate the “thing” into the smart device itself. For example, think of products like a smart water pump or an autonomous vehicle. These products control and monitor themselves. In this case, your product includes all four building blocks in a single package as shown below.
- But there are many other applications where the “thing” stands alone as a “dumb” device, and a separate product is connected to it to make it a smart device. In this case, your product only includes the three modules in blue below.

Building Block 2 : Data Acquisition

The data acquisition module focuses on acquiring physical signals from the thing and converting them into digital signals that can be manipulated by a computer.

- The data acquisition module includes more than sensors though. It also contains the necessary hardware to convert the sensor signal into digital information for the computer to use. It includes signal conditioning, analog-to-digital conversion, scaling, and interpretation.

Building Block 3: Data Processing

The third building block of an IoT device is the data processing module. This is the "computer" that processes the data, performs local analytics, stores data locally, and performs any other computing operations at the edge.

- Processing power (i.e., how much processing will you do at the edge?)
- Amount of local data storage (i.e., hard drive size how much data will you need to store at the edge?)

Building Block 4: Communications

The last building block of your device's hardware is the communications module. This is the circuitry that enables communications with your Cloud Platform, and with 3rd party systems either locally or in the Cloud.

- This module may include communication ports such as USB, serial (232/485), CAN, or Modbus, to name a few. It may also include the radio technology for wireless communications such as Wi-Fi, LoRA, ZigBee, 3G, 5G, etc.
- The communications module can be included in the same device as your other modules, or it could be a separate device that is specifically for communications. This approach is often referred to as a "gateway architecture".

IoT Device : Conclusion

- IoT device consists of embedded framework with other technology.
- Nowadays, we have one device to do all work, which is called as smart device.
- We can call it as edge device or end device.
- IoT device can monitor the environment in real-time and can provide the prescriptive measures in fly mode.

If you think that the internet has changed your life, think again. The IoT is about to change it all over again!

Thank You!!!