MODULE - 1

What is IoT?

★ IoT

- History: 1969: Internet emerges
  1982: TCP/IP takes shape
  1990: A thing was born (First connected device: Toaster)
  1999: The IoT gets a name (Kevin Ashton)
  2005: Getting Global Attention (UN)
  2008: connections count
  2011: IPv6 launches
- Definition - International Tele communication Union (ITU)

"A network that is available anywhere, anytime, by anything and anyone"

Any time connection, Any place connection, Any thing connection } on the move, indoors, outdoors, day, night, at the PC, between PCs, human-to-human, human-to-thing, thing to thing

- Concept:

Things
sensors/actuators with IP address that can be connected to Internet

→

Local Network
can be wired or wireless
LAN, BAN, PAN, CAN.

→

Cloud services
Data either sent to or received from cloud

Global Network
connecting bridge between the local network, cloud services and connected consumer devices

Connected Consumer Electronics
smart phones, devices, cars wearables which are connected to the things.

The age of IoT started between 2008 and 2009, with more "things" connected to the internet than people.

★ IoT and digitalization:

It encompasses the connection of "things" with the data they generate and the business insights that result.

Ex: In a shopping mall where Wi-Fi location tracking is used.

Digitalization is the conversion of information into a digital format. It may include the video rental industry and transportation also.

★ IoT Impact:

IoT Impact is the rapid growth in the number of devices connected to the Internet.

- Connected Roadways: Intersection movement assist warns the drivers if it is not safe to enter an intersection
  Wireless router - entertainment, mapping, safety
  connected sensors - fuel efficiency, collision avoidance
  Urban connectivity - reduced congestion.
- Connected Factory: Accelerating new product and service introductions to meet customer, increasing plant production, quality and decreasing cost, mitigating unplanned downtime, securing factories from cyber threats and increasing worker productivity and safety.

Industry 4.0: IoT Integration (Today)

Sensors with a new level of interconnectivity are integrated

- Smart Connected Buildings: control the heating, ventilation and air conditioning - BMS's (Building Management systems)
  communication protocol for building automation is called BACnet (Building Automation and Control Network)
  Ethernet based communication between building devices such as lighting, access control and fire detection systems.

- Digital ceiling: lighting, sensors, video surveillance, wifi access point.
- Smart creatures: "Connected cow": Dutch company developed a sensor placed in a cow's ear which monitors various health aspects of the cow as well as its location, by transmitting data wirelessly for analysis by the farmer.
  IoT enabled Roach can assist in finding survivors after a disaster.

* Convergence of IT and OT:

- Information technology supports connections to the Internet along with related data and technology systems and it focuses on the secure flow of data across an organization.
- Operation technology monitors and controls devices and processes on physical operational systems. They include assembly lines, utility distribution networks, production facilities, roadway systems and many more.

IT organization is responsible for the information systems of a business, such as email, file and print services, databases and so on whereas OT is responsible for the devices and processes acting on industrial equipment such as factory machines, meters, actuators, electrical distribution automation devices and so on.

Management of OT is crucial, for example, if the network connecting the machines in a factory fails, the machine cannot function and production may come to standstill impacting in the order of millions of dollars. On the other hand, if an IT fails, for example, if email server fails it may irritate people but it is unlikely to impact business.

Criterion	OT network	IT network
• Operational focus	– operating 24 x 7	– manage data and computers in secure way
• Priorities	– [1]Availability, [2]integrity, [3]security	– [1]security, [2]integrity, [3]availability
• Types of data	– monitoring, control, supervisory data	– voice, video, transactional, bulk data.
• Security	– controlled physical access to devices	– Devices and users authenticated to the network
• Implication of failure	– Directly impacts business	– Depends on industry
• Security vulnerability	– Low	– High

* IoT Challenges:

- Scale
- Security
- Privacy
- Big data and data analytics
- Interoperability
- various protocols and architectures are jockeying for market share and standardization within IoT.

IoT Network Architecture and Design

★ Drivers behind new Network Architectures:

Challenge	Description	IoT Architectural Change Required
Scale	The massive scale of IoT sensors is far beyond that of typical IT networks	The IPv4 address space has reached exhaustion and is unable to meet IoT's scalability requirements. Scale can be met only by using IPv6. IT networks continue to use IPv4 through features like Network Address Translation (NAT).
security	IoT devices, especially those on wireless sensor networks are often physically exposed to the world.	Security is required at every level of the IoT network. Every IoT endpoint node on the network must be part of the overall security strategy and must support device-level authentication and link encryption.
Devices and networks constrained by power, CPU, memory and link speed.	Due to the massive scale and longer distances the networks are often constrained, lossy and capable of supporting only minimal data rates.	New last mile wireless technologies are needed to support constrained IoT devices over long distances. The network is also constrained, meaning modifications need to be made to traditional network-layer transport mechanisms
The massive volume of data generated	The sensors generate a massive amount of data on a daily basis, causing network bottlenecks and slow analytics in the cloud	Data analytics capabilities need to be distributed throughout the IoT network, from the edge to the cloud. In traditional IT networks, analytics and applications typically run only in the cloud.

Support for legacy devices	An IoT network often comprises a collection of modern, IP capable endpoints as well as legacy, non-IP devices that rely on serial or proprietary protocols.	Digital transformation is a long process that may take many years, and IoT networks need to support protocol translation and/or tunneling mechanisms to support legacy protocols over standards-based protocols such as Ethernet and IP.
The need for data to be analyzed in real time.	whereas traditional IT networks perform scheduled batch processing of data, IoT data needs to be analyzed and responded to in real-time.	Analytics software needs to be positioned closer to the edge and should support real-time streaming analytics. Traditional IP analytics software are better suited to batch-level analytics that occur after the fact.

★ Comparing IoT Architectures:

- M2M:

ETSI (European Telecommunications Standards Institute) created the M2M Technical committee in 2008

2012: ETSI and 13 other members launched oneM2M as a global initiative designed to promote efficient M2M communication systems and IoT.

Goal: To create a common services layer which can be readily embedded in field devices to allow communication with application servers.

OneM2M's framework focuses on IoT services, applications and platforms. These include smart metering applications, smart grid, smart city automation, e-health and connected vehicles.

Application Layer:

This domain includes the application layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models and thus they are shown as vertical entities.

Service Layer:

This layer is shown as a horizontal framework across the vertical industry applications. One of the stated goals of oneM2M is to develop technical specifications which address the need for a common M2M service layer that can be readily embedded

Network Layer:

It includes the devices themselves and the communications network that links them. Infrastructure include wireless mesh technologies such as IEEE 802.15.4 and wireless point-to-multipoint systems such as IEEE 801.11ah.

- IoT World Forum (IoTWF):

It decomposes the IoT problem into smaller parts, identify different technologies at each layer and how they relate to one another. It defines a system in which different parts can be provided by different vendors. They have a process of defining interfaces that leads to interoperability and define a tiered security model that is enforced at the transition points between levels.

Layer 1 - Physical Devices and controllers layer:

This layer is home to the "things". Their primary function is generating data and being capable of being queried and controlled

over a network.

Layer 2: connectivity Layer:

It is responsible for timely transmission of data. It encompasses all the networking elements and does not distinguish between the last-mile network gateway and backhaul networks.

Functions: - communication between layer 1 devices.
- Reliable delivery of information across the network
- Switching and Routing
- Translation between protocols
- Network level security

Layer 3: Edge Computing Layer:

It is often refered to as "fog". It emphasises on data reduction and converting network data flows into information that is ready for storage and processing by higher layers.

Functions: - Evaluate and reformat data for processing at higher levels
- Filter data to reduce traffic at higher level processing
- Access data for alerting, notification and other actions

Layer 4: Data Accumulation Layer:

Functions: - Captures data and stores it so it is usable by applications when necessary.
- converts event-based data to query-based processing

Layer 5: Data Abstraction Layer:

It reconciles multiple data formats and ensures semantics from various sources are consistent. It confirms that the data set is complete and consolidates data into one place or multiple data stores using virtualization.

Layer 6: Applications Layer:

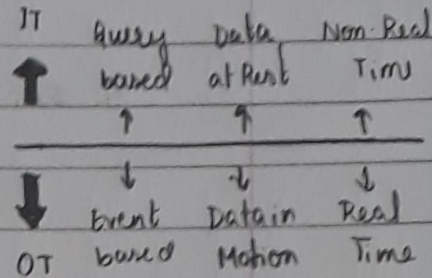
Interprets data using software applications which may be used to monitor, control and provide reports based on the analysis of data.

Layer 7: collaboration and Processes Layer:

It consumes and shares the application information. This layer can change business processes and deliver the benefits of IoT

Levels

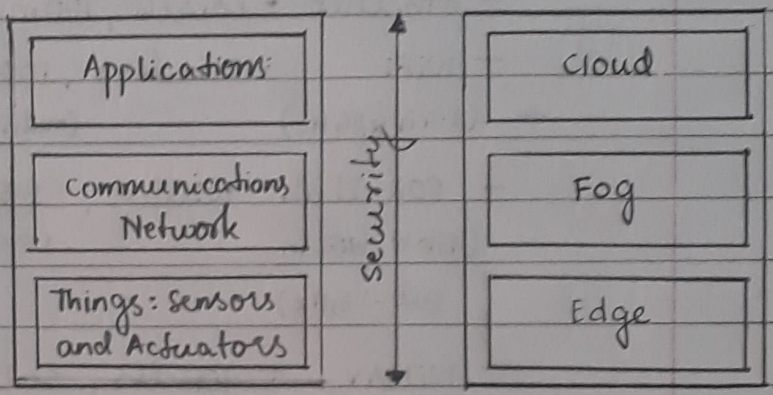
7	Collaboration and Process layer
6	Applications Layer
5	Data Abstraction Layer
4	Data Accumulation Layer
3	Edge computing Layer
2	Connectivity Layer
1	Physical devices and controllers layer



★ **A Simplified IoT Architecture:**

This framework is represented as two parallel stacks:

1. The core IoT Functional Stack
2. The IoT Data Management and compute stack.



Core IoT Functional stack

IoT Data Management and compute stack

– **The Core IoT Functional Stack**

Layer 1: Things: Sensors and Actuators Layer

1. Battery powered or power connected
2. Mobile or static
3. Low or high reporting frequency
4. Simple or rich data
5. Report range
6. object density per cell

Layer 2: Communication Network Layer

1. PAN: Personal Area Network (Bluetooth)
   Scale of a few meters. Personal space around a person.
2. HAN: Home Area Network (ZigBee and Bluetooth Low energy BLE)
   Scale of a few ten meters.

3. NAN : Neighbourhood Area Network
Scale of a few hundred meters. For a group of house units from which data is connected.

4. FAN : Field Area Network
Scale of several tens of meters to several hundreds of meters. An outdoor area larger than a single group of house units.

5. LAN : Local Area Network
Scale of up to 100 m.

Technologies
- Ethernet : wired, 100m max
- WiFi : wireless, 100 m - few kilometers
(2.4 GHz, 5 GHz) (multipoint) (point to point)
- 802.11ah : wireless, 1.5km - 10 km
(HaloW, WiFi in sub-1 GHz) (multipoint) (point to point)
- WiMAX : wireless, several kilometers - 50 km
(802.16) (last mile) (backhaul)
- Cellular : wireless, several kilometers.
(LTE)

Layer 3 : Applications and Analytics Layer :
Analytics Application : It collects data from multiple smart objects, processes the collected data and displays information resulting from the data that was processed.
Control Application : It controls the behavior of the smart object or the behavior of an object related to the smart object. Ex: a pressure sensor may be connected to a pump and a control application increases the pump speed when the connected sensor detects a drop in pressure.