Subject : Internet Of Things Technology.

Subject code : 15CS81

Module-1

What is IOT?

- IOT - Internet Of Things, extends Internet connectivity beyond traditional device like desktop and laptop computers, smartphones and tablets to a diverse range and wellday things that utilize embedded technology to communicate and interact with the external environment, all via the INTERNET

The basic premise and goal of IOT is to "connect the unconnected". This means that objects that are not currently joined to a computer network, namely the Internet, will connect so that they can communicate and interact with people and other objects.

IOT is a technology transition in which devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.

* Genesis Of IOT:-

- IOT has been started between the year 2008 and 2009. During this time period, the number of devices connected to the Internet eclipsed the world's population
- The person credited with the creation of the term "Internet of Things" is Kevin Ashton while working for Procter and Gamble in 1999, Kevin used this phrase to explain a new idea related to linking the company's supply chain to Internet

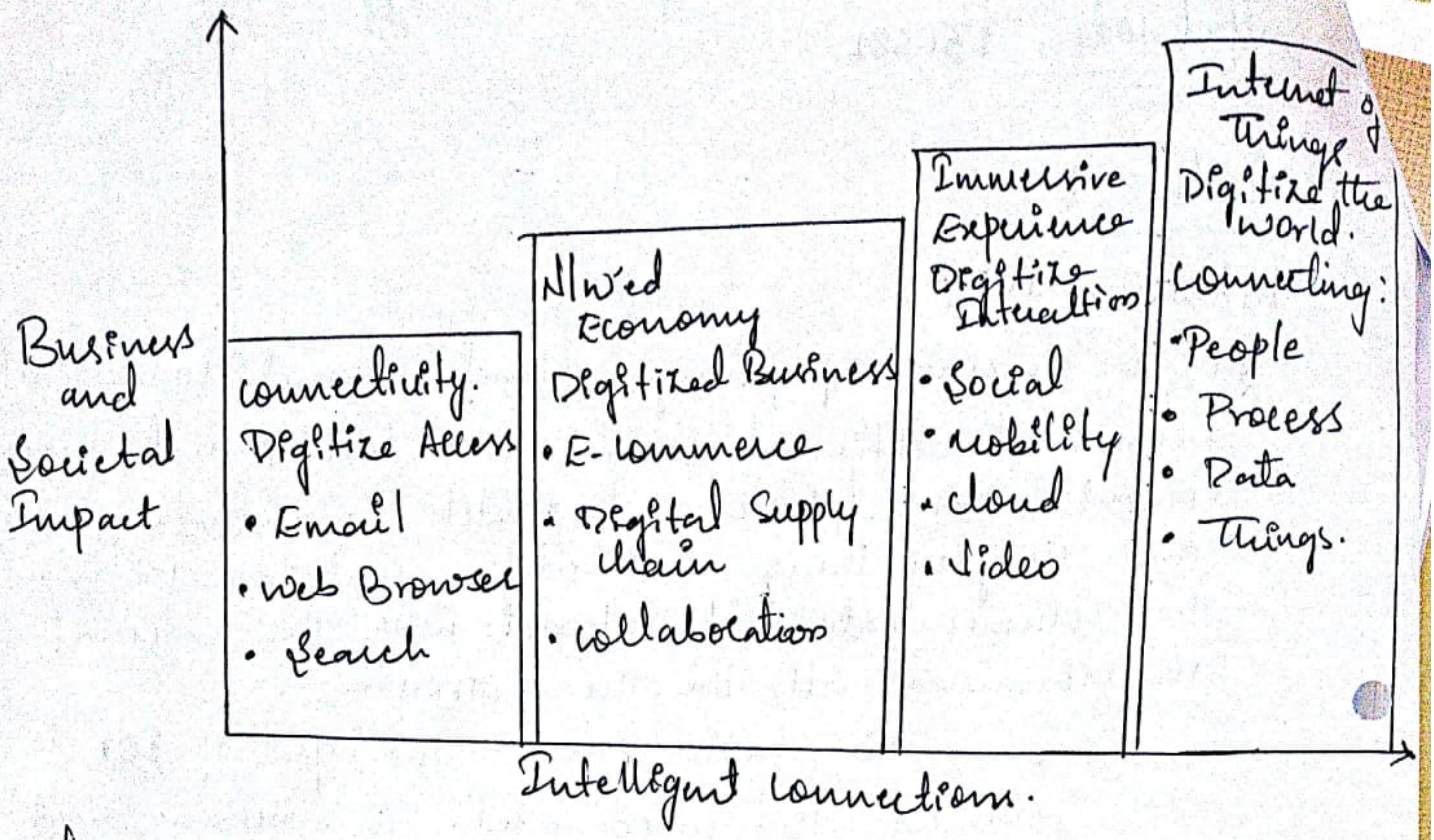


Figure 1-1 : Evolutionary Phases of the Internet.

As shown in the figure, the evolution of the Internet can be categorized in four phases.

Each of these evolutionary phases builds on the previous one. With each subsequent phase, more value become available for businesses, governments and society in general.

- The first phase :- [Connectivity], began in the mid-1990's. This phase connected people to email, web services and search so that information is easily accessed.

Even though connectivity and its speed continued to improve, a saturation point was reached where connectivity was no longer then major challenge.

Second Phase :- The beginning of the second phase of Internet evolution, called the Networked Economy. This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes

- with the Networked Economy, e-commerce and digitally connected supply chains became the rage, and this caused one of the major disruption of the past 100 years!
- The economy itself became more digitally intertwined as suppliers, vendors, and consumer all became more directly connected.

Third Phase :- Immersive Experience [Digitize Internet]

Immersive Experience is characterized by the emergence of social media, collaboration and widespread mobility on a variety of devices.

- This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.

fourth phase :- Internet of Things [Digitize the world]

This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences & connecting the unconnected.

IOT and Digitization :—

IOT and Digitization are terms that are often used interchangeably, but there are key differences to be aware of.

- IOT focuses on connecting "things", such as objects and machines, to a computer network, such as the Internet.
- On the other hand, digitization can mean different things to different people but generally encompasses the connection of "things" with the data they generate and the business insights that result.
- Digitization, as defined in its simplest form, is the conversion of information into digital format. Digitization has been happening in one form or another for several decades.
- In context to IOT, digitization brings together things, data and business process to make networked connections more relevant and valuable

IOT Impact :—

Projections on the potential impact of IOT are impressive. About 14 billion, or just 0.06% of "things" are connected to the Internet today.

- Connected Roadways :- People have been fantasizing about the self-driving car, or autonomous vehicle, in literature and film for decades.

While this fantasy is now becoming a reality with well-known projects like Google's self-driving car, IOT is also a necessary component for implementing a fully connected transportation infrastructure.

* Current challenges Being Addressed by Connected Roadways.

Challenges	Supporting Data
- Safety →	According to the US Department of Transportation, 5.6 million crashes were reported in 2012 alone, resulting in more than 33,000 fatalities.
- Mobility →	More than a billion cars are on the roads worldwide. Connected vehicle mobility applications can enable system operators and drivers to make more informed decisions, which can, in turn, reduce travel delay.
- Environment →	According to the American Public Transportation Association, each year transit systems can collectively reduce carbon dioxide (CO_2) emission by 16.2 million metric tons by reducing private vehicle miles.

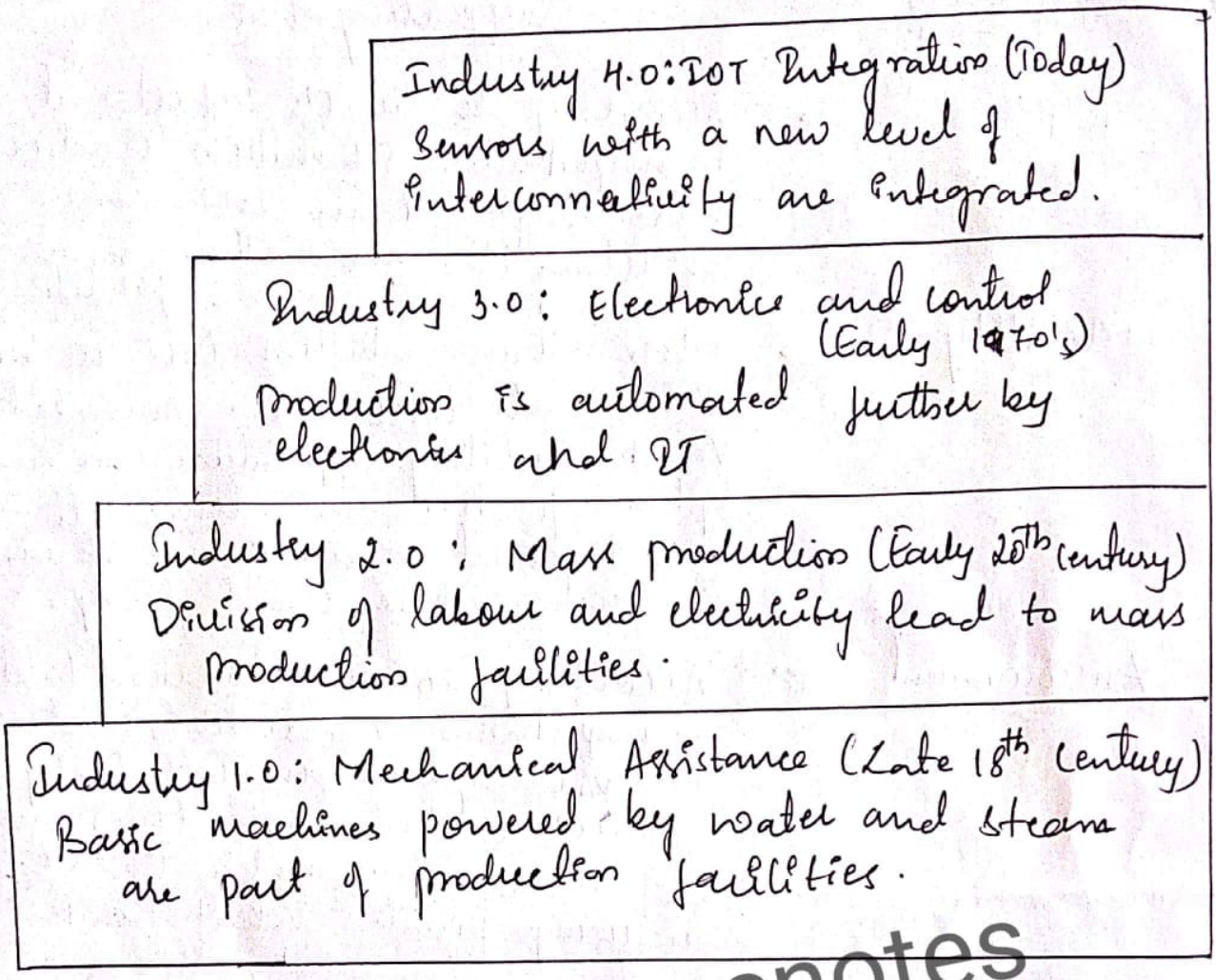
- Connected factory :-

For years, traditional factories have been operating at a disadvantage, impeded by production environments that are "disconnected", or, at the very last, "strictly gated" to corporate business systems, supply chains and customers and partners.

- We look to tend to look at IOT as an evolution of the Internet, it is also sparking an evolution of Industry.

- In 2016 the World Economic Forum referred to the evolution of Internet and the Impact of IOT as the "fourth Industrial Revolution".

Figure: The fourth Industrial Revolution



IOT Challenges :-

The following are the few of the most significant challenges and problems that IOT is currently facing.

- IOT Challenges :-

Challenges	Description
- Scale	While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger.
- Security	With more "things" becoming connected with other "things" and people, security is an increasingly complex issue for IOT. The network is already expanding and if the device gets hacked, its connectivity is a major concern

- Privacy ⟶ As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities

- Big data and data analytics ⟶ IOT and its large number of sensors is going to trigger a deluge of data that must be handled. This data will provide critical information and insights if it can be processed in an efficient manner.

- Interoperability ⟶ As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IOT.

*

CHAPTER-2

IOT Network Architecture and Design

To successfully complete a construction project, time and effort are required to design each phase, from the foundation to the roof.

- Failure to carefully architect a network according to sound design principles will likely result in something that is difficult to scale, manage, adapt to organization changes, and worst of all, troubleshoot when things go wrong.

Drivers Behind New Network Architectures :-

IOT Architectural Drivers.

Challenge	Description	IOT Architectural change Required.
Scale	The massive scale of IOT endpoints is far beyond that of typical IT nlw	The IPv4 address space has reached exhaustion and is unable to meet IOT's scalability requirements.
Security	IOT devices, especially those on wireless sensor nlw (WSN), are often physically exposed to the world.	Security is required at every level of the IOT endpoint node on the network must be part of the overall security
Devices and nlw: constrained by power, CPU memory & link speed	Due to the massive scale and longer distance, the nlw are often constrained, lossy, and capable of supporting only minimal data rates	New last-mile wireless technologies are needed to support constrained IOT device over long distance
The massive volume of data generated	The sensors generate a massive amount of data on a daily basis, causing nlw bottlenecks and slow analytics in the cloud.	Data analytics capabilities need to be distributed throughout the IOT device from the edge to the cloud.
Support for Legacy devices	An IOT network often comprises a collection of modern, IP-capable endpoints as well as legacy, non-IP device that rely on serial or proprietary protocols	Digital transformation is a long process that may take many years and IOT net works need to support protocol translation and/or tunneling mechanisms

* Scale :-

The Scale of a typical IT network is on the order of several thousand devices - typically printers, mobile wireless devices, laptops, servers and so on.

- The kind of scale has only previously been seen by the Tier-1 service providers. IOT introduces a model where an average-sized utility, factory transportation system, or city could easily be asked to support a network of this scale. Based on scale requirements of this order, IPv6 is the natural foundation for the IOT network layer.

* Security :-

Traditional models of IT security are simply not designed for the new attack vectors introduced by highly dispersed IOT systems. IOT systems require consistent mechanisms of authentication, encryption, and intrusion prevention techniques that understand the behavior of industrial protocols and can respond to attacks on critical infrastructure.

- For optimum security, IOT system must:
  * Be able to identify and authenticate all entities involves in the IOT service
  * Ensure that all user data shared b/w the endpoint device and back-end applications is encrypted.
  * Comply with local data protection legislation so that all data is protected and stored correctly
  * Utilize an IOT connectivity management platform and establish rules-based security policies so immediately action can be taken if anomalous behavior is detected from connected devices.
  * Take a holistic, network-level approach to security

* Constrained Devices and Networks :-

Most IOT Sensors are designed for a single job, and they are typically small and inexpensive. This means they often have limited power, CPU and memory and they transmit only when there is something important.

VLAN and are impacting performance, you can simply carve out a new VLAN and continue to scale as much as need.

* Data :-

IOT devices generate a mountain of data. In general, most IT shops dont really care much about the unstructured chatty data generated by devices on the network.

- In IOT data is like gold, as it is what enables business to deliver new IOT services that enhance that customer experience, reduce cost, and deliver new revenue opportunities.

Although most IOT-generated data is unstructured, the insights it provides through analytics can revolutionize processes and create new business models

IOT systems are designed to stagger data consumption throughout the architecture, both to filter and reduce unnecessary data going upstream and to provide the fastest possible response to devices when necessary.

* Legacy device support :-

Supporting legacy devices in an IT organization is not usually a big problem - If someone's computer or operating system is outdated, she/he simply upgrades.

As the IoT networks are deployed, they need to support the older devices already present on the network, as well as devices with new capabilities.

In many cases, legacy devices are so old that they don't even support IP. For example, a factory may replace machine only once every 20 years — or perhaps even longer! It does not want to upgrade multi-million-dollar machines just so it can connect them to a network for better visibility and control.

* Comparing IoT Architecture :—

The foundational concept in all these architectures is supporting data, process, and the functional that endpoint devices perform. The best known architectures are those supported by.

- One M2M
- IoT World Forum (IoTWF).

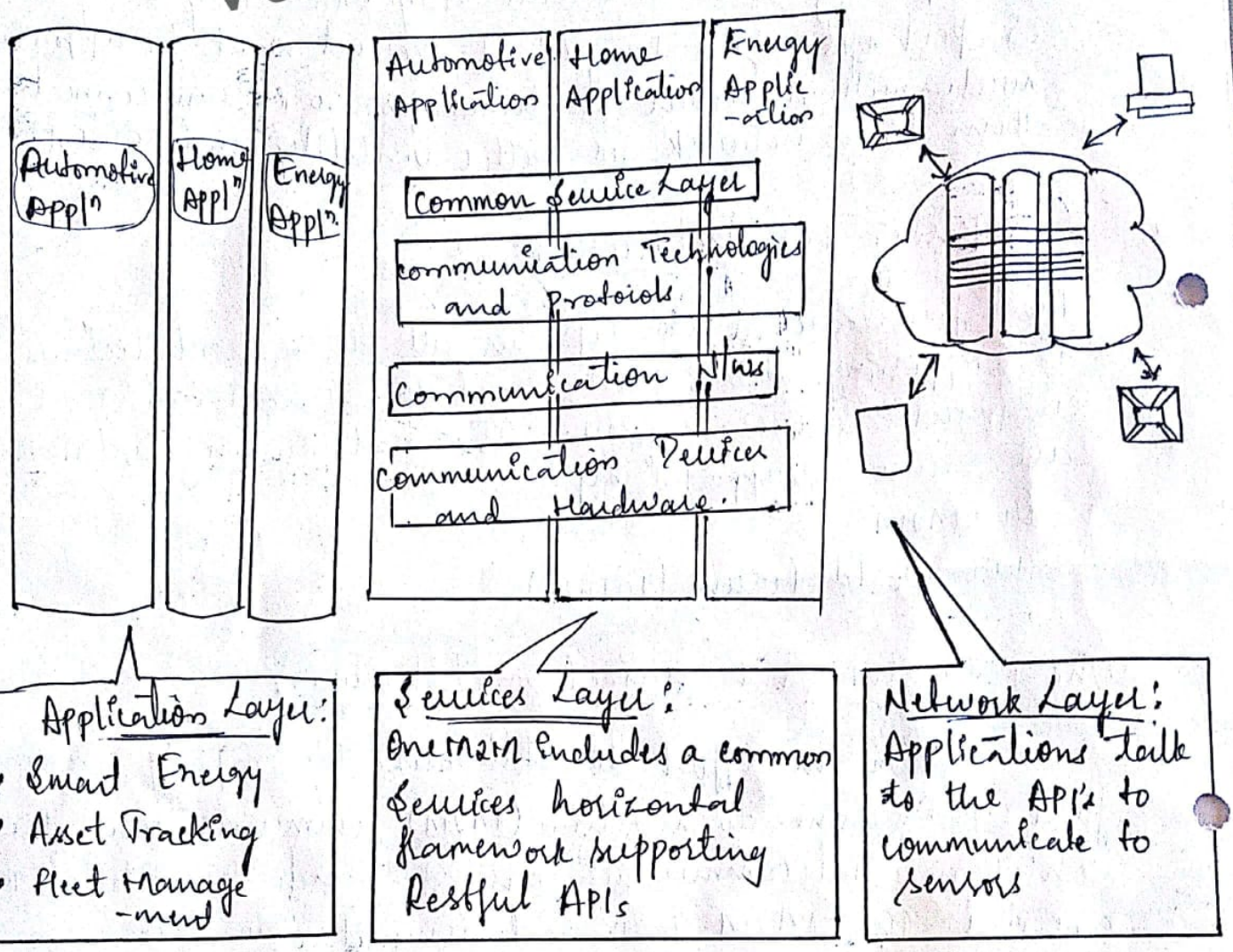
* One M2M IoT Standardized Architecture :—

In an effort to standardize the rapidly growing field of machine-to-machine (M2M) communications, the European Telecommunications Standards Institute (ETSI) created the M2M Technical committee in 2008.

The goal of this committee was to create a common architectural that would help accelerate the adoption of M2M applications and devices.

One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software and access methods. By developing a horizontal platform architecture, OneM2M is developing standards that allow interoperability at all levels of the IoT stack.

Figure :- The main elements of the oneM2M IoT Architecture.



The oneM2M architecture divides IoT functions into three major domains: the application layer, the service layer and the network layer. While this architecture may seem simple and somewhat generic at first glance, it is very rich and promotes interoperability through IP-friendly APIs and supports a wide range of IoT technologies

* Application Layer:

The One M2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application layer protocols and attempts to standardize API definitions for interactions with Business Intelligence (BI) systems.

* Service Layer:

This layer is shown as a horizontal framework across the vertical industry applications.

- At this layer, horizontal modules include the physical network that the IOT applications run on, the underlying management protocols, and the hardware.
  Eg- MPLS networks, VPNs etc.
- This conceptual layer adds APIs and middleware supporting third-party services and applications.
  One of the stated goals of One M2M is to "develop technical specification which address the need for a common M2M service layer that can be readily embedded within various hardware and software nodes, field area network to M2M application services, which typically reside in a cloud or data center".

* Network layer:-

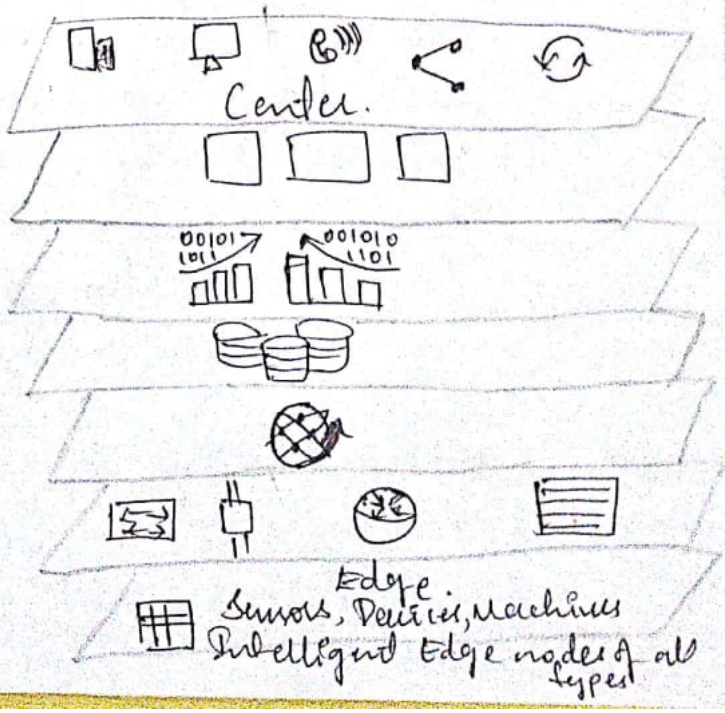
This is the communication domain for the IOT devices and end points.

- It includes the devices themselves and the communications network that links them.
- This communication infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and Wireless point-to-multipoint systems, such as IEEE 801.11ah. and wired device connections, such as IEEE 1901 power line communications.
- In some cases, machine-to-machine communi-cation is not necessary, and the device simply communicate through a field area Network (FAN) to use-case-specific appx in the IOT application domain.

The IOT World Forum (IOTWF) Standardized Architecture

In 2014 the IOTWF architectural committee has published a seven-layer IOT architectural reference model.

Figure : IOT Reference Model Published by the IOTWF.



7. Collaboration & processes
6. Application
5. Data Abstraction
4. Data Accumulation
3. Edge computing
2. Connectivity
1. Physical Devices and controllers.

The above figure, the IOT Reference Model defines a set of levels with control flowing from the center to edge, which includes sensors, devices, machines and other types of intelligent end nodes.

Using this reference model, we are able to achieve the following -

* Decompose the IOT problem into smaller parts
* Identify different technologies at each layer and how they relate to one another
* Define a system in which different parts can be provided by different vendors
* Have a process of defining interfaces that leads to interoperability
* Define a tiered security model that is enforced at the transition points between levels.

Layer 1 : Physical Devices and Controllers Layer :-

The first layer of the IOT Reference Model is the physical devices and controllers layer. This layer is home to the "things" in the Internet of Things, including the various endpoint devices and sensors that send and receive information.

Their primary function is generating data and being capable of being queried and/or controlled over a network.

Layer 2 : Connectivity Layer :-

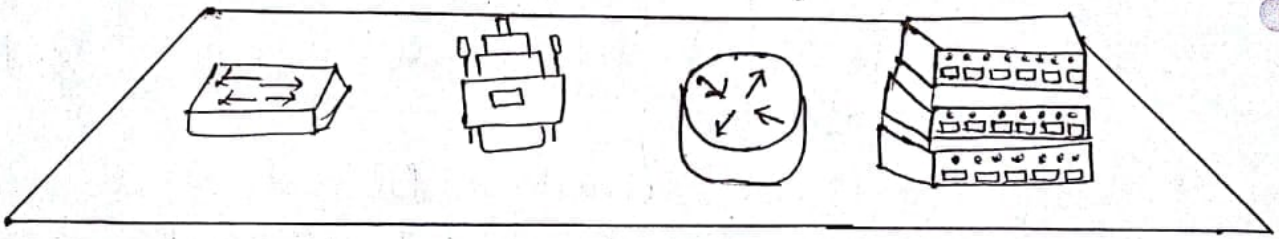
In the second layer of the IOT Reference Model, the focus is on connectivity. The most imp function of this IOT layer is the reliable and timely transmission data. This includes transmission b/w layer 1 devices and the b/w information processing that occurs at Layer 3.

Figure :- IOT Reference Model Connectivity Layer functions

② Connectivity.
(Communication and processing Units)

Layer 2 functions:

- Communications Between Layer 1 Devices
- Reliable Delivery of Information Across the Nw
- Switching and Routing
- Translation Between Protocols
- Network Level Security

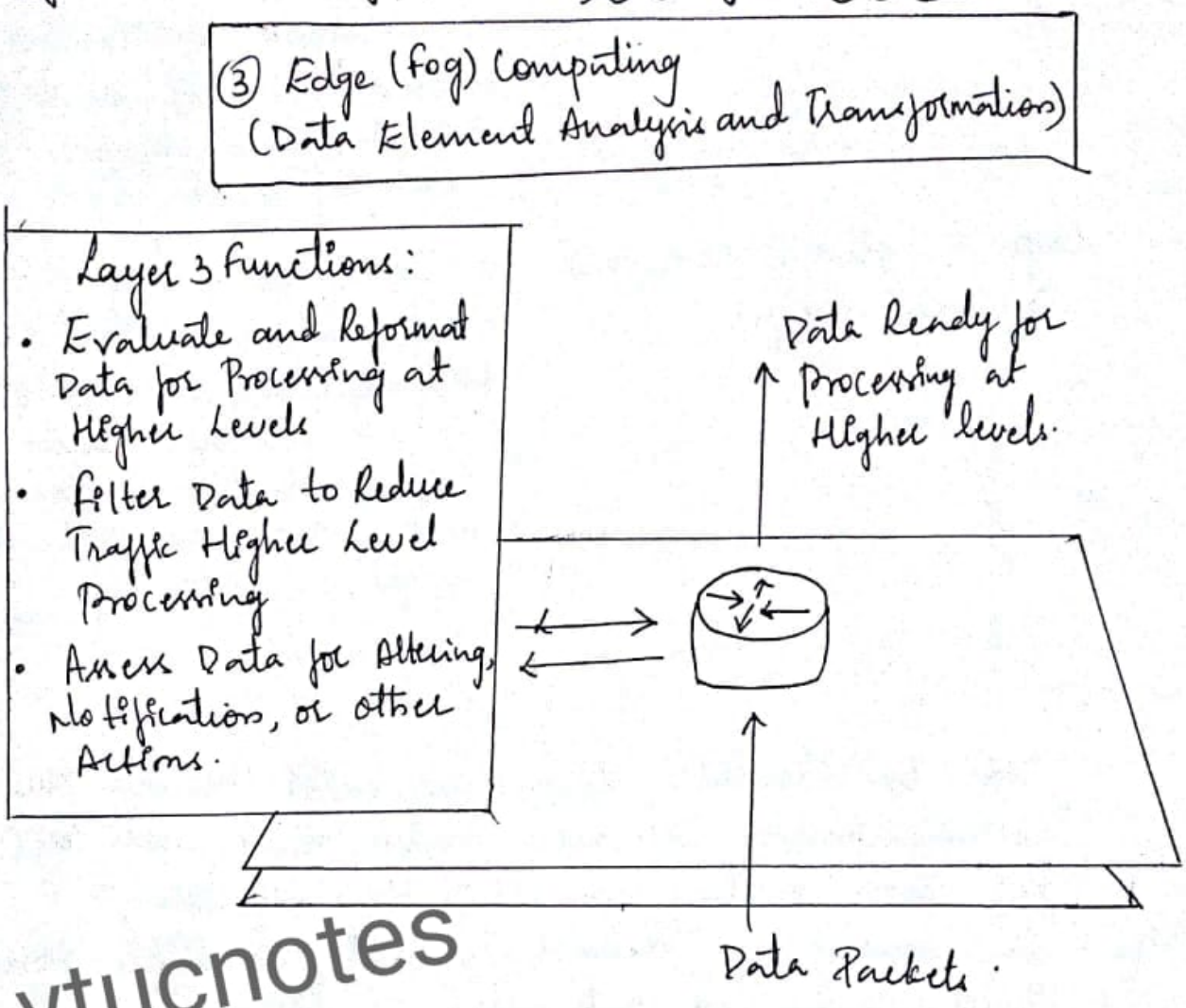


– Layer 3 : Edge Computing Layer.

Edge computing is the role of Layer 3. Edge computing is often referred to as the "fog" Layer.

- One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible.
- Another important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered or aggregated before being sent to a higher layer.
- This also allows for data to be reformatted or decoded, making additional processing by other system easier.

Figure: IOT Reference Model Layer 3 Functions



– Upper Layers: Layers 4-7

The upper layers deal with handling and processing the IOT data generated by the bottom layer. For the sake of completness, Layer 4-7 of the IOT Reference are:

IOT Reference Model Layer	Functions
* Layer 4: Data accumulation layer	→ 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	→ Reconcile multiple data formats and ensures consistent semantics from various sources.

- Layer 6 : Application layer → Interprets data using software applications. Applications may monitor, control, and provide reports based on the analysis of the data.

- Layer 7 : Collaboration and Processor layer → Consumes and shares the application informations. collaborating on and communicating IoT informations often requires multiple steps, and it is what makes IoT useful.

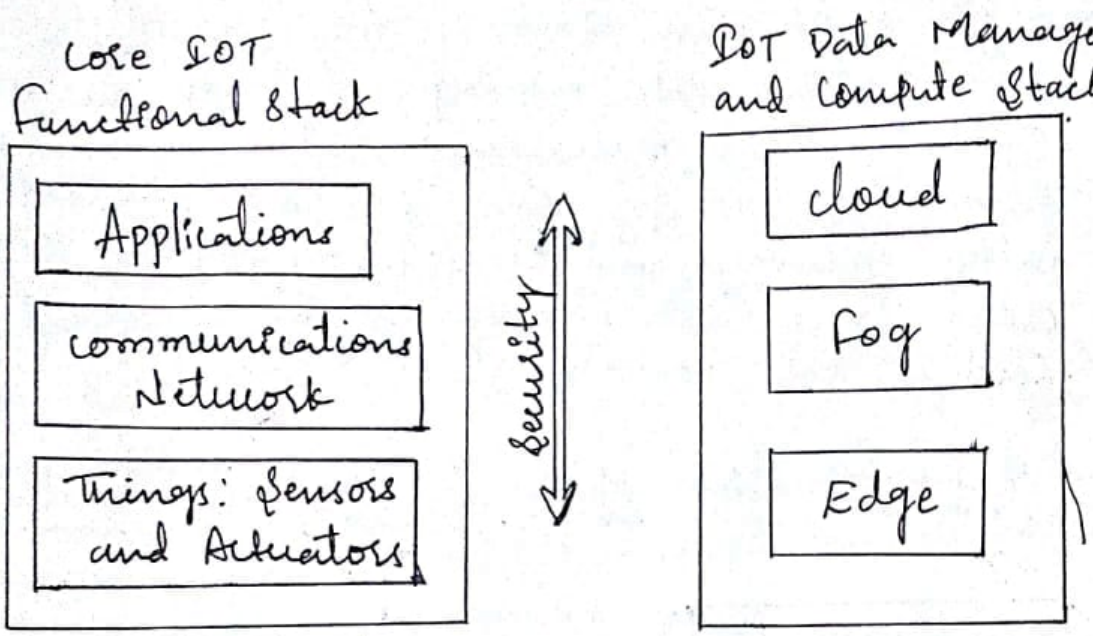
* A Simplified IoT Architecture :-

A considerable differences exist between the aforementioned reference models, they each approach IoT from a layered perspective, allowing development of technology and standards somewhat independently at each level or domain.

- An IoT framework that highlights the fundamental building blocks that are common to most IoT systems and which is intended to help you in designing an IoT network.
- The following framework is presented as two parallel stacks: the IoT Data Management and compute stack and the core IoT functional stack.
- Reducing the framework down to a pair of three-layer stacks in no way suggests that the model lacks the detail necessary to develop a sophisticated IoT strategy.

Prepared by Sandhya Rani BLDEC.

figure :- Simplified IOT Architecture



- In the above figure - it includes "things," a communication network and applications. The framework presented here separates the core IOT and data management into parallel and aligned stacks, allowing you to carefully examine the functions of both the network and the applications at each stage of a complex IOT system.
- The presentation of the core IOT functional stack in three layers is meant to simplify your understanding. The network communications layer of the IOT stack itself involves a significant amount of detail and incorporates a vast array of technologies.

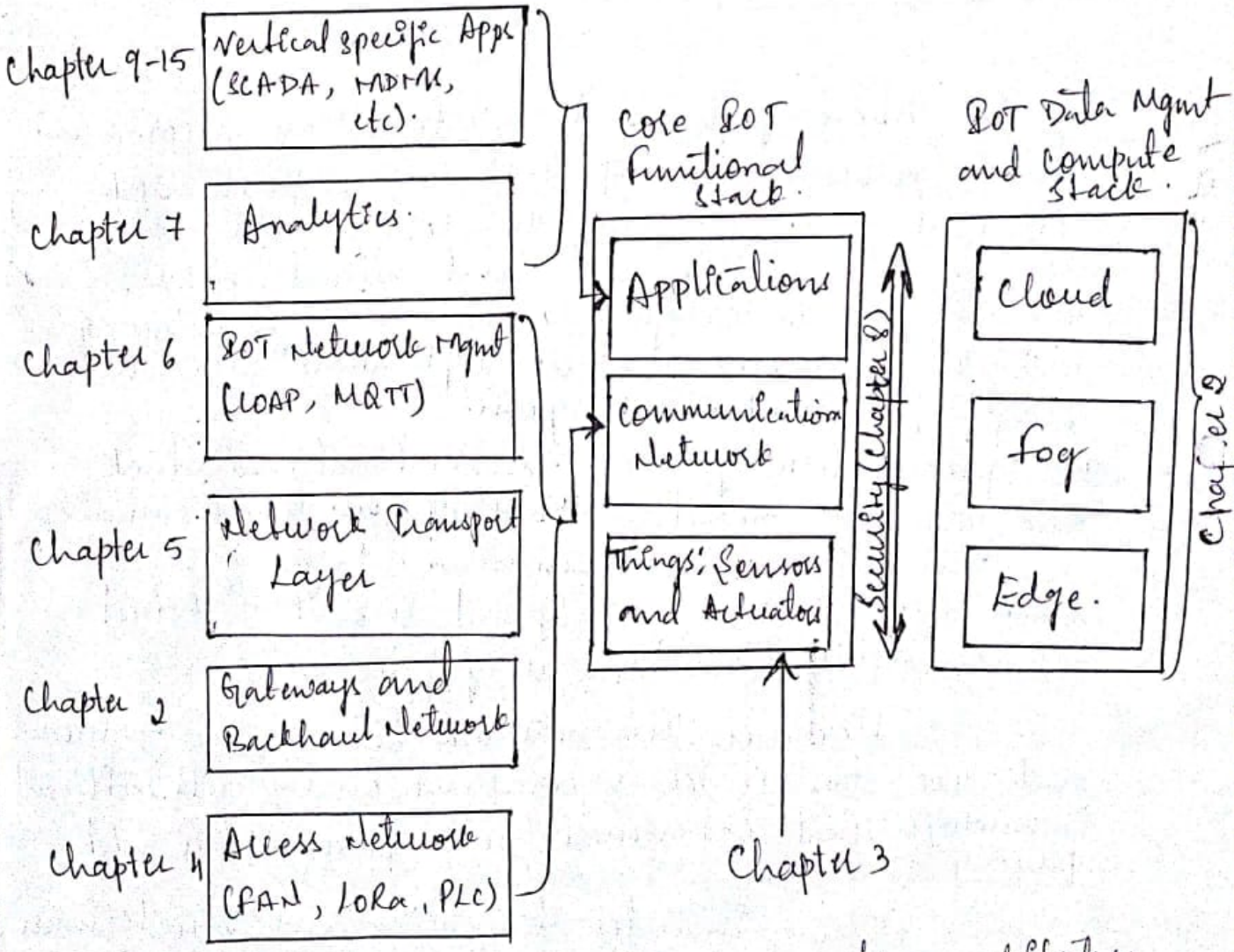
However, the network between the gateway and the data center is composed mostly of traditional technologies that experienced IT professionals would quickly recognize.

These include tunneling and VPN technologies, IP based quality of Service (QoS), conventional layer 3 routing protocols such as BGP and IP-PIM, security capabilities such as encryption, access control lists (ACLs) and firewalls.

In the above model presented, the data management is aligned with each of the three layers of the core IOT Functional Stack.

The three data management layers are the edge layer (data management within the sensors themselves), the fog layer (data management in the gateways and transit network), and the cloud layer (data management in the cloud or central data center).

Figure : Expanded view of the Simplified IOT Architecture



→ The Security is central to the entire architecture both from the network connectivity and data management.

- As shown in the figure, the core IoT functional stack can be expanded into sublayers containing greater detail and specific network functions.

  for example, the communications layer is broken down into four separate sublayers: the access networks, gateways and backhaul, IP transport and operations and management sublayers.

- The applications layer of IoT network is quite different from the application layer of a typical enterprise network. The security is central to the entire architecture, both from network connectivity and data management.

* The core IoT functional Stack:—

- IoT networks are built around the concept of "things" or smart objects performing functions and delivering new connected services.

  From an architectural standpoint, several components have to work together for an IoT network to be operational:—

→ "Things" Layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed.

→ Communications network layer: when smart objects are not self-contained, they need to communicate with an external system.

This layer has four sublayers:

* Access network sublayer: The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa.

* Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects.

* Network transport sublayer: For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use.

* IoT network management sublayer: Additional protocols must be in place to allow the headend applications to exchange data with the sensors.

→ Application and analytics layer: At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the "things" or other system.

- Layer 1: Things: Sensors and Actuators Layer:-
  Most IoT network start from the object, or "Thing" that need to be connected.
  - Battery-powered or Power-connected
  - Mobile or Static
  - Low or high reporting frequency
  - Simple or rich data
  - Report range
  - object density per cell

Prepared By Sandhya Rani BKEC.

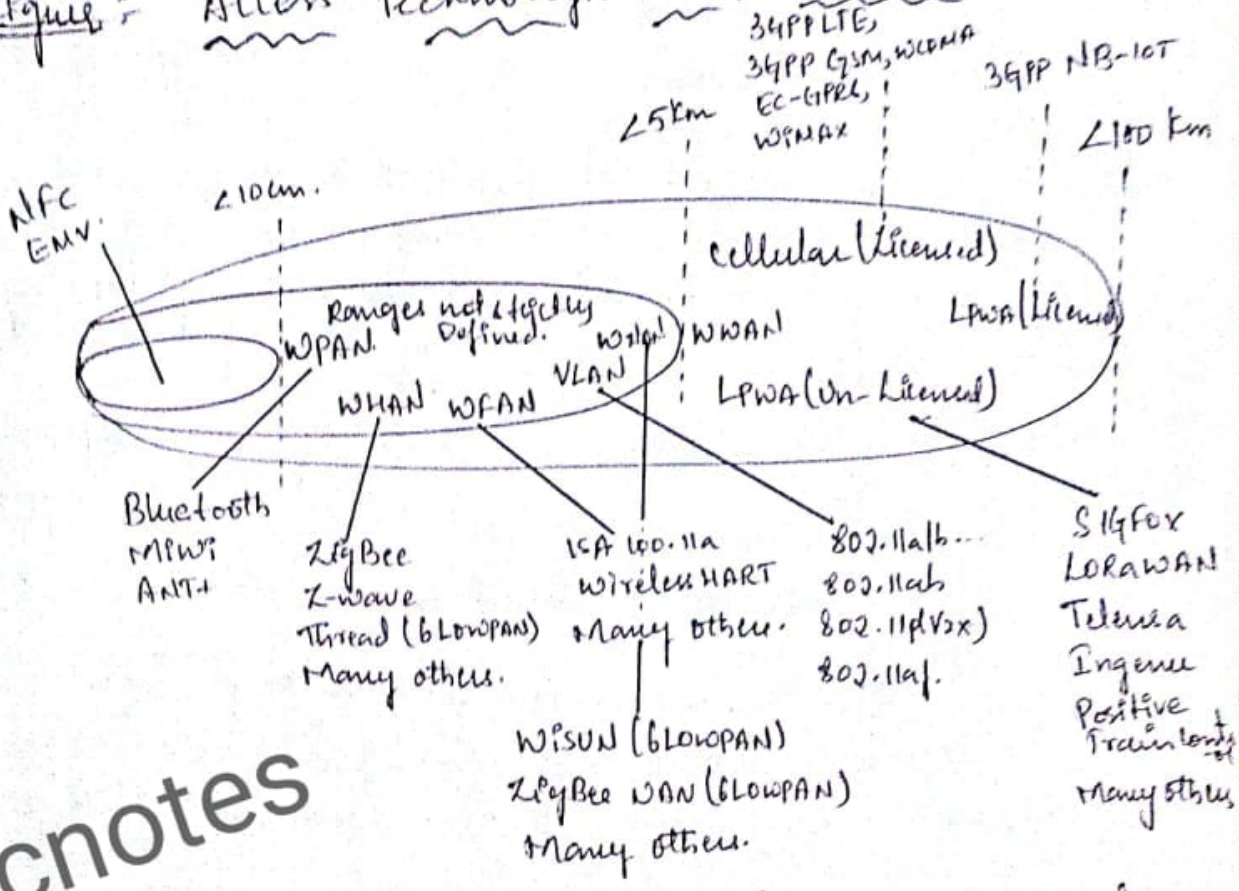
Layer 2: Communications Network layer

After determining the influence of the smart object from factor over the communication capabilities, we can connect object and communicate.

Access Network Sublayer

- There is a direct relationship between the IOT network technology, we choose and the type of connectivity topology this technology allows.

Figure: Access Technologies and Distance :—



- Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected.

- → PAN (Personal Area Network)
- → HAN (Home Area Network)
- → NAN (Neighborhood Area Network)
- → FAN (Field Area Network)
- → LAN (Local Area Network) -

→ Point-to-Point Topology

→ Point-to-Multipoint topology.

Layer 3: Applications and Analytics Layer

Once connected to a network, your smart objects exchange information with other systems.

- **Analytics Versus Control Applications**

  Multiple applications can help increase the efficiency of an IoT network. Each application collects data and provides a range of function based on analyzing the collected data.

  * **Analytics applications:** This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed.

    The important aspect is that the application processes the data to convey a view of the network that cannot be obtained from solely looking at the information displayed by a single smart object.

  * **Control Application :-** This type of application controls the behaviour of the smart object or the behaviour of an object related to the smart object.

    An example of control system architecture is SCADA. SCADA was developed as a universal method to remote systems and send instructions

- Many advanced IoT applications include both analytics and control modules. In most cases data is collected from the smart objects and processed in the analytics modules.

Prepared By Sandhya Rani BKBE.

Data versus Network Analytics :-

Analytics is a general term that describes processing information to make sense of collected data.

- Data analytics :- This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IOT system.

  In more complex case, temperature, pressure, wind, humidity and light levels collected from thousands of sensors may be combined and then processed to determine a storm and its possible path.

- Data analytics can also monitor the IOT system itself. for example, a machine or robot in a factory can report data about its own movements.

+ Network analytics :- Most IOT systems are built around oby smart objects connected to the network. A loss or degradation in connectivity is likely to affect the efficiency of the system. Such a loss can have dramatic effects.

- Loss of connectivity means that data stops being fed to your data analytics platform, and the system stops making intelligent analyses of the IOT system.

- Most of the analytics applications employs both data and network analytics modules. Network analytics is necessary for connected system.

  Data analytics is a wider space with a lager gray area than network analytics.

Data Analytics Versus Business Benefits :-

Data analytics is undoubtedly a field where the value of IoT is booming. Almost any object can be connected, and multiple types of sensors can be installed on a given object. Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

- **Smart Services :-**

The ability to use IoT to improve operations is often termed "smart services". This term is generic, and in many cases the term is used but its meaning is often stretched to include one form of service or another where an additional level of intelligence is provided.

- Smart services can also be used to measure the efficiency of machines by detecting machine output, speed, or other forms of usage evaluation.
- Smart services can be integrated into an IoT system. For example, sensors can be integrated in a light bulb. A sensor can turn a light on or off based on the presence of a human in the room.

Light bulbs are simple example. By connecting to other systems in the house, efficiencies can be coordinated.

Prepared By Sandhya Rani BREC.

IOT Data Management and Compute Stack :—

The data generated by IOT sensors is one of the single biggest challenges in building an IOT system.

— There are some new requirements :—

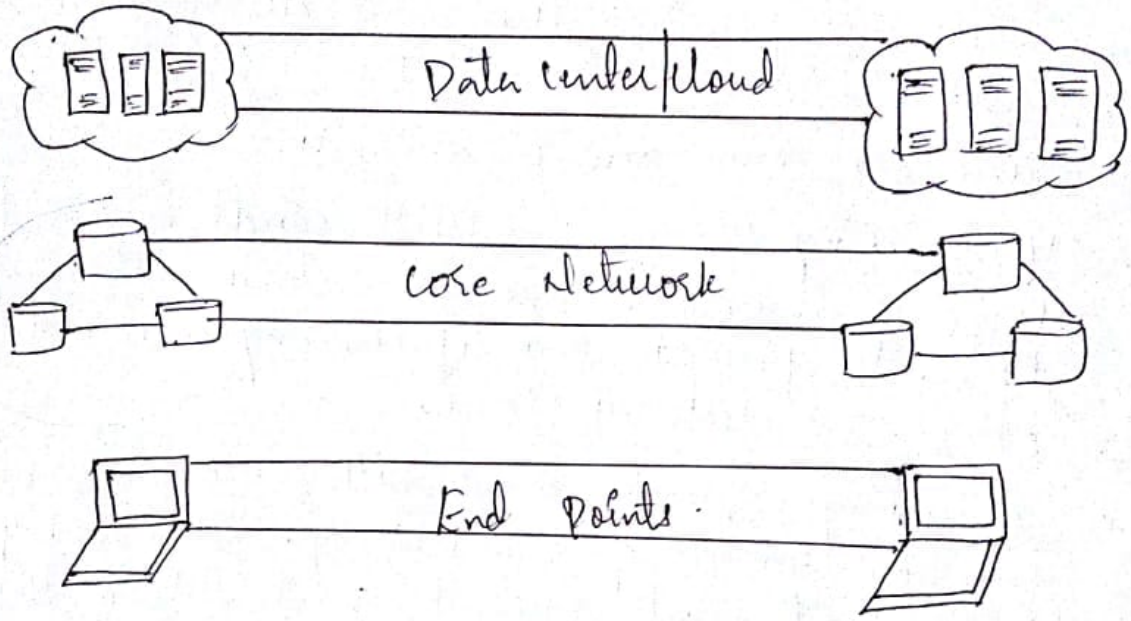
* Minimizing Latency :— Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdown or restore electrical service.

* Conserving network bandwidth :— Offshore oil rigs generate 500 GB of data weekly. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the clou

* Increasing local efficiency :— collecting and securing data across a wide geographic area with different environmental conditions may not be useful.

— In the figure— The traditional IT cloud computing model, data management in traditional IT systems is very simple.
The endpoints communicate over an IP core network t servers in the data center or cloud. Data is generat stored in the data center, and the physical links from access to core are typically high bandwidth, meaning access to IT data is quick.

Figure :- The traditional IT Cloud Computing Model



Fog computing :-

The defining characteristics of fog computing are as follows:

* Contextual location awareness and low latency :- The fog node sits as close to the IOT endpoint as possible to deliver distributed computing.
* Geographic distribution :- In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.
* Deployment near IOT endpoints : Fog nodes are typically deployed in the presence of a large number of IOT endpoints.
* Wireless communication between the fog and the IOT endpoint :- Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a larger number of endpoints.
* Use for interactions : Important fog applications involve real-time interactions rather than batch processing