**PBR VISVODAYA INSTITUTE OF TECHNOLOGY AND SCIENCE**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IOT)**

# (20A05703b)
# INDUSTRIAL & MoT

**CSE(IoT) - IV. B. Tech SEM – I**

**by**

**Dr G Vijay Kumar**

# UNIT-I

# OVERVIEW OF INTERNET OF THINGS (IIOT)

# UNIT-I SYLLABUS

## OVERVIEW OF INTERNET OF THINGS

Introduction, IOT Architecture, Application–based IOT protocols, Cloud Computing, Fog Computing, Sensor Cloud, Big Data.

Overview of Industry 4.0 and Industrial Internet of Things: IIoT- Prerequisites of IIOT, Basics of CPS, CPS and IIOT, Applications of IIoT.

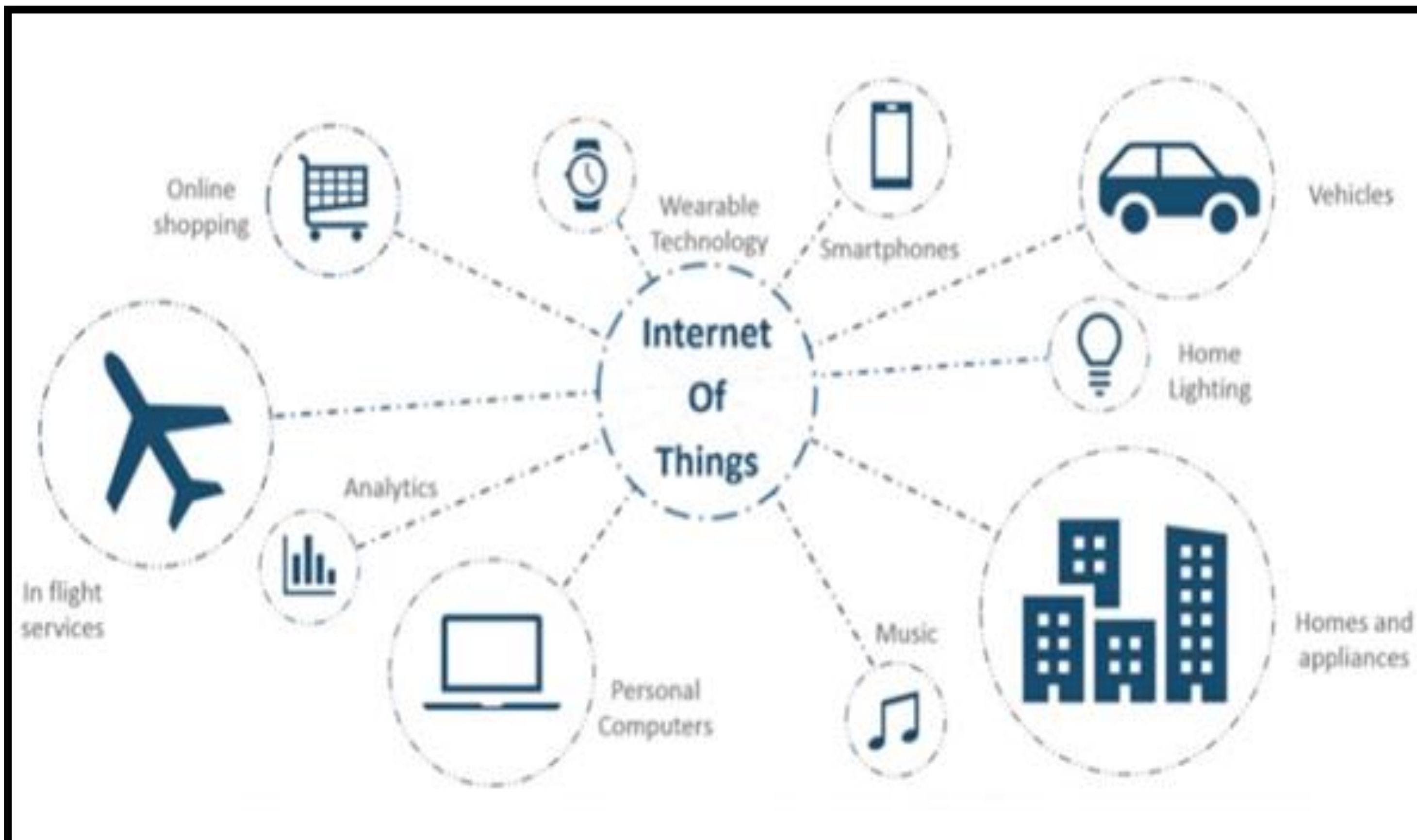
## Introduction of IOT:

The Internet of Things (IoT) refers to the network of interconnected physical objects or "things" that are embedded with sensors, software, and other technologies to collect and exchange data over the internet or other communication networks.

These objects can range from everyday devices such as smart phones, wearable devices, and household appliances to more specialized items like industrial machinery, environmental sensors, and even vehicles.

The concept of IoT revolves around enabling these objects to communicate, share information, and collaborate without requiring direct human intervention.

This connectivity and data exchange offer a wide range of benefits and opportunities across various industries and aspects of life, leading to enhanced efficiency, convenience, and insights. Here are some key aspects of IoT:



**Sensors and Data Collection:**

IoT devices are equipped with various sensors that can measure different attributes such as temperature, humidity, pressure, light, motion, and more. These sensors gather data from the physical world and convert it into digital information.

**Connectivity:**

IoT devices connect to the internet or local networks using various communication protocols such as Wi-Fi, Bluetooth, cellular networks, Zigbee, LoRaWAN, and more. This connectivity enables seamless data transmission and remote control.

**Data Processing and Analysis:**

The data collected by IoT devices can be processed and analyzed either locally on the device or in the cloud. Advanced analytics and machine learning techniques can derive valuable insights from the collected data, enabling informed decision-making.

## Automation and Control:

IoT enables automation by allowing devices to perform actions based on predefined rules or real-time data. For instance, a smart thermostat can adjust the temperature based on occupancy and ambient conditions.

## Interconnectivity:

IoT devices often work in conjunction with other devices and systems, creating interconnected ecosystems. This interconnectedness allows for complex and collaborative applications. For example, a smart home system might integrate security cameras, door locks, and lighting controls.

## Applications:

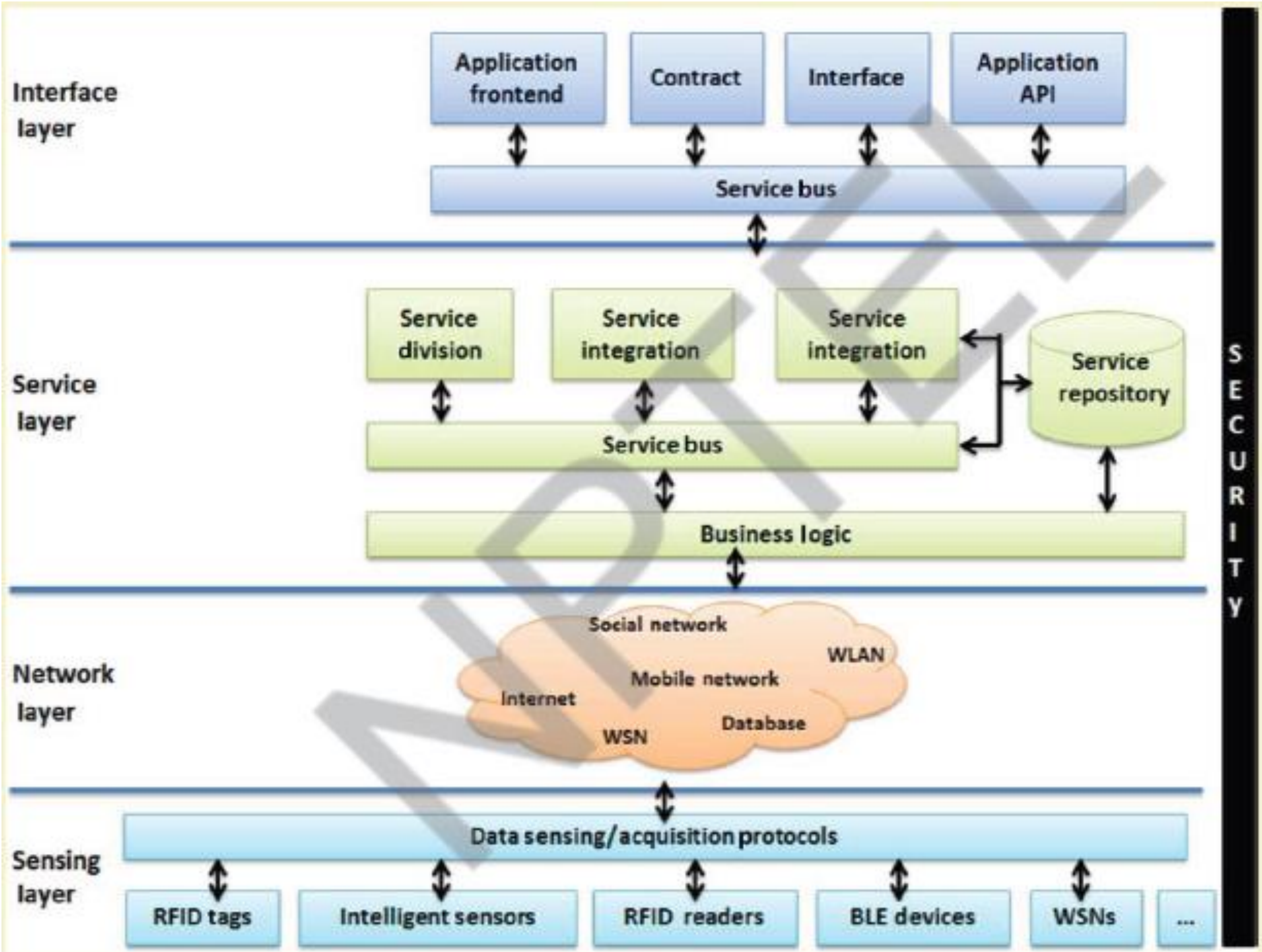
IoT has a wide range of applications across industries such as healthcare, agriculture, manufacturing, transportation, smart cities, energy management, and more. For instance, in healthcare, IoT devices can monitor patients' vital signs remotely and alert medical professionals in case of emergencies.

**Challenges:** The rapid proliferation of IoT devices has also brought about challenges, including data security and privacy concerns, interoperability issues, and the need for efficient data management and processing.

## IOT Architecture:

Internet of Things (IoT) architecture refers to the structure or framework that defines how IoT devices, sensors, networks, and applications interact with each other to collect, process, and exchange data.

A well-designed IoT architecture is crucial for the successful deployment of IoT solutions. There are various IoT architecture models, but a typical IoT architecture can be divided into several layers:


Interface layer
Application frontend
Contract
Interface
Application API
Service bus
Service layer
Service division
Service integration
Service integration
Service repository
Service bus
Business logic
Network layer
Social network
WLAN
Mobile network
Internet
WSN
Database
Sensing layer
Data sensing/acquisition protocols
RFID tags
Intelligent sensors
RFID readers
BLE devices
WSNs
...
SECURITY

## 1. Device Layer:

**IoT Devices/Sensors**: These are physical devices that collect data from the environment. Ex: temperature sensors, cameras, RFID tags, and smart appliances.

**Edge Devices/Gateways**: In some cases, edge devices or gateways are used to preprocess and filter data locally before sending it to the cloud. They also often manage device communication protocols and security.

## 2. Communication Layer:

**Connectivity**: This layer deals with the protocols and technologies used to connect IoT devices to the network. Common connectivity options include Wi-Fi, cellular, Bluetooth, Zigbee, LoRa, and MQTT.

**IoT Protocols**: MQTT, CoAP, HTTP, and other protocols enable devices to send data to the cloud or other devices.

## 3. Cloud/Fog Layer:

**Cloud Services**: IoT data is typically sent to the cloud for storage, processing, and analysis. Cloud services include IoT platforms, databases, and data analytics tools.

**Edge/Fog Computing**: In some cases, data processing occurs closer to the devices (at the edge or fog) to reduce latency and improve real-time processing.

## 4. Middleware Layer:

**IoT Middleware**: This layer provides services such as device management, data normalization, security, and authentication. It often acts as a bridge between devices and applications.

## 5. Application Layer:

**IoT Applications**: These are the end-user applications and services that leverage IoT data to provide value. Examples include home automation, industrial automation, smart cities, and healthcare applications.

**User Interface (UI):** Dashboards, mobile apps, and web interfaces allow users to interact with and control IoT devices and access data insights.

## 6. Security and Privacy Layer:

**Authentication and Authorization**: Ensuring that only authorized devices and users can access and control IoT resources.

**Data Encryption**: Encrypting data in transit and at rest to protect it from unauthorized access.

**Security Updates and Patch Management**: Keeping IoT devices and software up-to-date to address vulnerabilities.

**Privacy Controls**: Managing user consent and data handling to comply with privacy regulations.

## 7. Business Layer:

**Business Logic**: Defining the rules and logic that govern IoT operations.

**Monetization Strategies**: Determining how the IoT system generates revenue, such as through subscription models or data monetization.

## 8. Analytics and Insights Layer:

**Data Analytics**: Using machine learning and data analysis techniques to derive insights from IoT data.

**Predictive Maintenance**: Identifying patterns and anomalies to predict when devices need maintenance or replacement.

## 9. Device Management:

**Lifecycle Management**: Tracking and managing devices from provisioning to decommissioning.

**Over-the-Air (OTA) Updates**: Updating device firmware and software remotely.

IoT architectures can vary greatly depending on the specific use case, industry, and technology choices.

**IOT Applications:**

The Internet of Things (IoT) has a wide range of applications across various industries and sectors. Those are

1. **Smart Home Automation**: Thermostats, lighting, security cameras, and appliances.

2. **Industrial IoT (IIoT)**: In manufacturing and industrial settings, IoT devices can monitor equipment performance, track inventory, and optimize production processes.

3. **Healthcare:** IoT devices are used in healthcare for remote patient monitoring, tracking vital signs, and managing medical equipment.

4. **Smart Cities**: Urban infrastructure - traffic management, waste management, and energy consumption.

5. **Agriculture**: IoT sensors can monitor soil conditions, weather, and crop health.

6. **Transportation**: IoT is used for tracking and managing vehicles, optimizing routes, and providing real-time information to travelers.

7. **Environmental Monitoring**: IoT devices can monitor air quality, water quality, and environmental conditions.

8. **Energy Management**: IoT is used to monitor and control energy consumption in buildings and industrial facilities.

9. **Smart Grids**: IoT is used to create smart grids that can better distribute electricity, manage peak loads, and integrate renewable energy sources.

## IoT protocols:

IoT protocols aim to connect devices to IoT devices over a seamless and secure connection.

The IoT protocols operate on four pillars - device, connectivity, data, and analytics.

Their defense-in-depth security strategy shields the data transmission layer by layer.

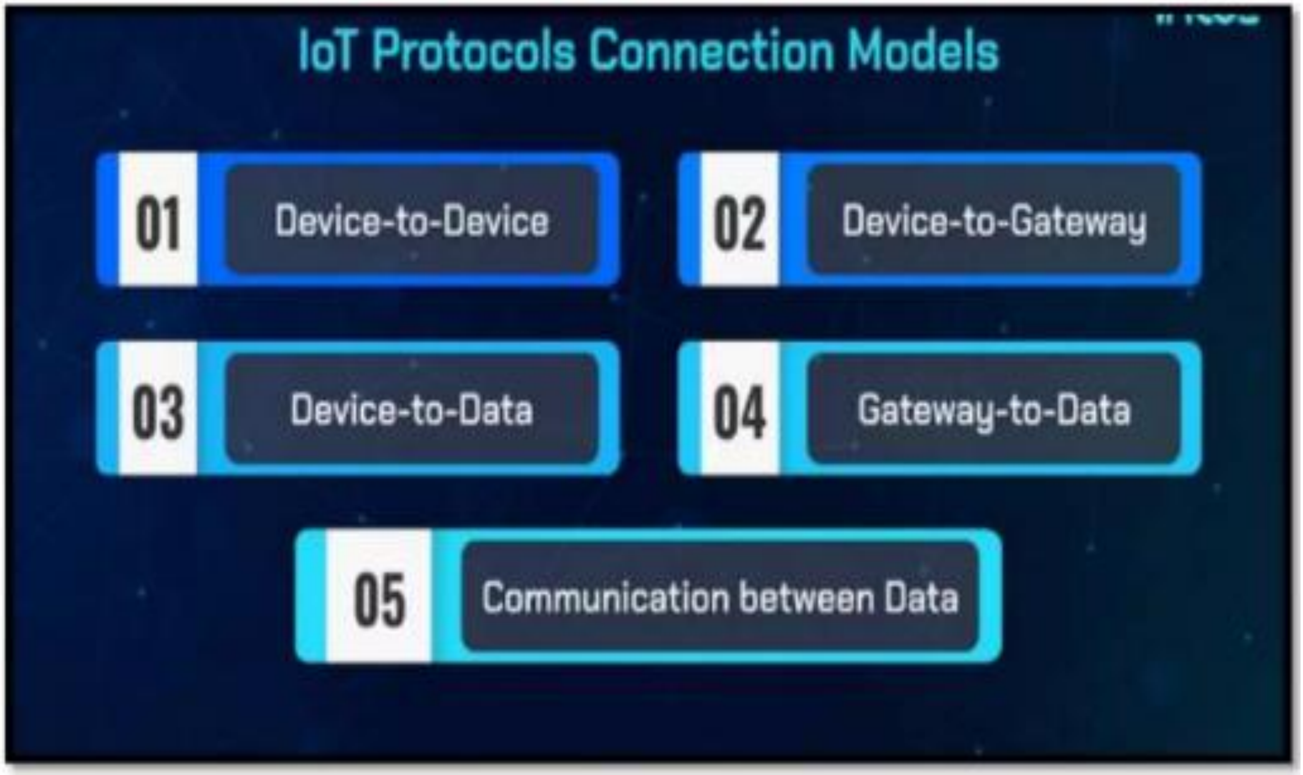
The device layer comprises combination of sensors, a hardware, actuators, software, and gateways, constituting a device that connects and interacts with a network.

The data layer involves the data collected, processed, stored, and analyzed in business contexts.

## IoT protocols connection models:

There is no set pattern for data routing, and the communication is highly dependent on the network topology.

However, the fundamental models are used either as standalone or in combinations for IoT deployments, including:



## 1. Device-to-device

It enables communication between nearby devices (proximity) using IoT Protocols like Bluetooth, ZigBee, Z-Wave, 4G, 5G, and WiFi.

## 2. Device-to-gateway

In this model, the devices communicate with the data system using a mediator platform, such as LPWAN, Wi-Fi, and/or Ethernet IoT protocols.

The core functions of device-to-gateway are combining data from sensors, analyzing it, and routing it to the destination data system (data center or cloud).

Also, in case of any problem, the connection model sends back the data to the source device.

## 3. Device-to-data

It works on edge computing, allowing devices to connect directly with the data source. A few popular device-to-data connection models include BLE, LoRaWAN, and Z-Wave.

## 4. Gateway-to-data

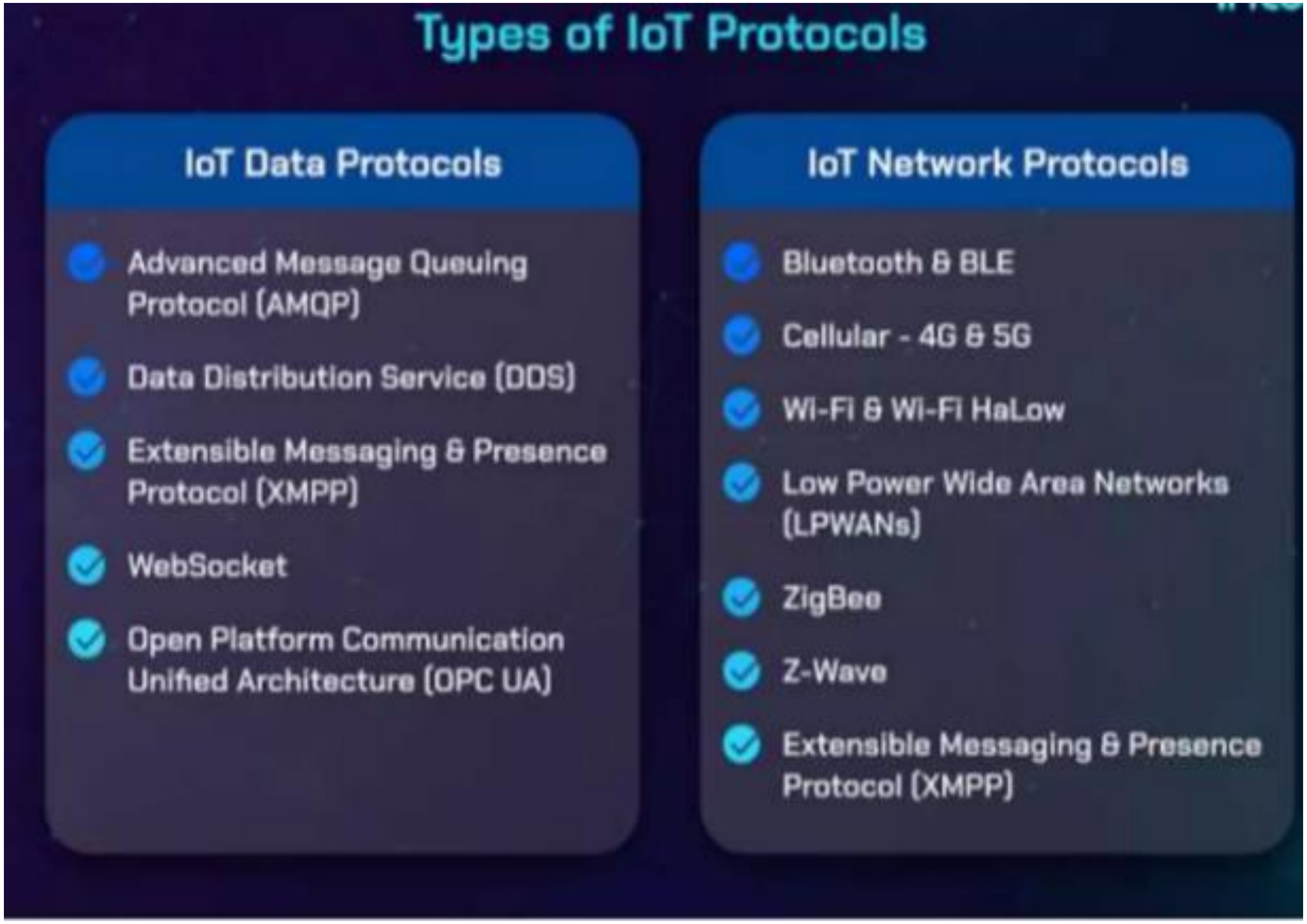
It is the simple communication between the mediator platform or central hubs and the data center or cloud. Open Automation Software (OAS) and Universal Data Connector are the best examples of robust IoT Gateways.

## 5. Communication between data

This protocol connection model allows data transmission between the data center and the cloud. It includes IoT Data protocols like MQTT, HTTP, REST, etc.

# Types of IoT protocols

IoT protocols and standards are broadly classified into two separate categories, including IoT data protocols that have presentation or application layers and network protocols for IoT comprising



## Cloud Computing:

### What is Cloud?

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location.

Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud.

### What is Cloud Computing?

Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application.

Cloud Computing is both a combination of software and hardware based computing resources delivered as a network service.

# Cloud Computing Architecture

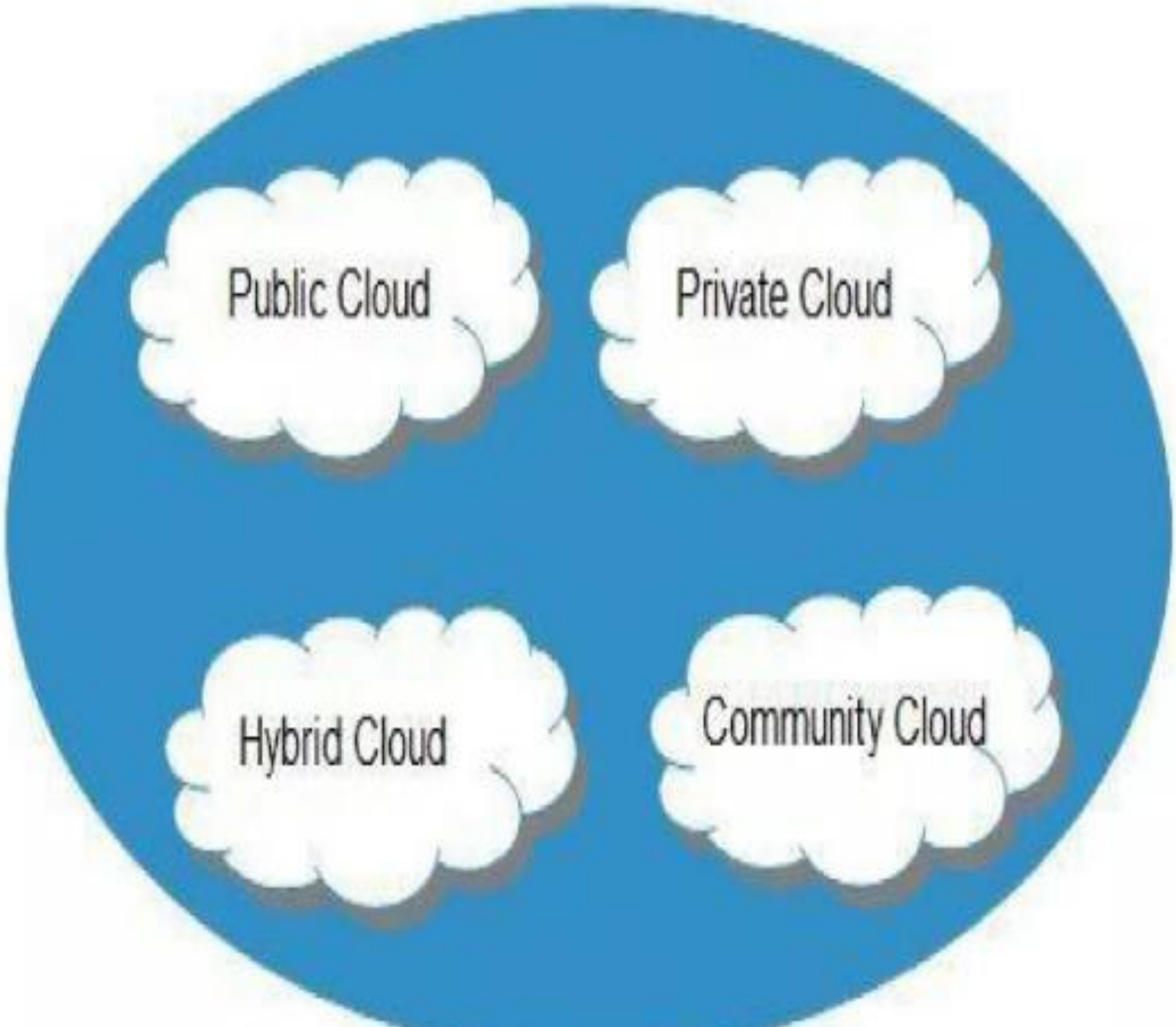
## Basic Concepts:

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. Following are the working models for cloud computing:

1. Deployment Models
2. Service Models

## 1. Deployment Models

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community.


Public Cloud
Private Cloud
Hybrid Cloud
Community Cloud

## PUBLIC CLOUD:

The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

## PRIVATE CLOUD:

The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

## COMMUNITY CLOUD:

The Community Cloud allows systems and services to be accessible by group of organizations.

## HYBRID CLOUD:

The Hybrid Cloud is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

## 2. Service Models

Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

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

IaaS is the delivery of technology infrastructure as an on demand scalable service.

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

- Usually billed based on usage
- Usually multi tenant virtualized environment
- Can be coupled with Managed Services for OS and application support

## IaaS Examples

**Platform as a Service (PaaS):**

PaaS provides the runtime environment for applications, development & deployment tools, etc.

PaaS provides all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely from the Internet.

Typically applications
1. Multi tenant environments
2. Highly scalable multi tier architecture

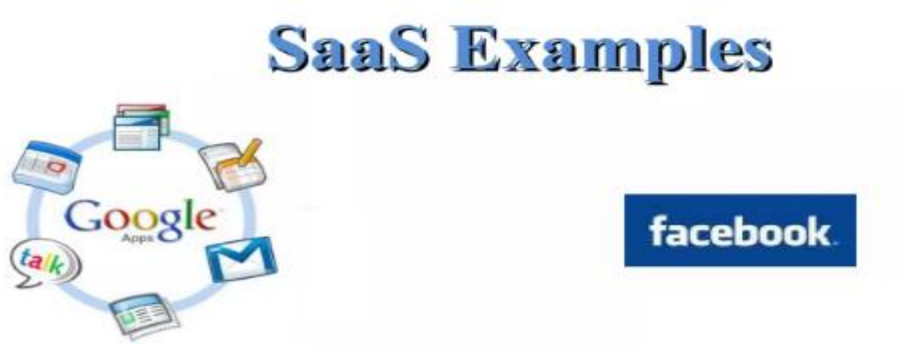
**PaaS Examples**

## Software as a Service (SaaS)

SaaS model allows to use software applications as a service to end users.

SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service.

- Usually billed based on usage
- Usually multi tenant environment
- Highly scalable architecture



# Fog Computing:

## What is Fog:

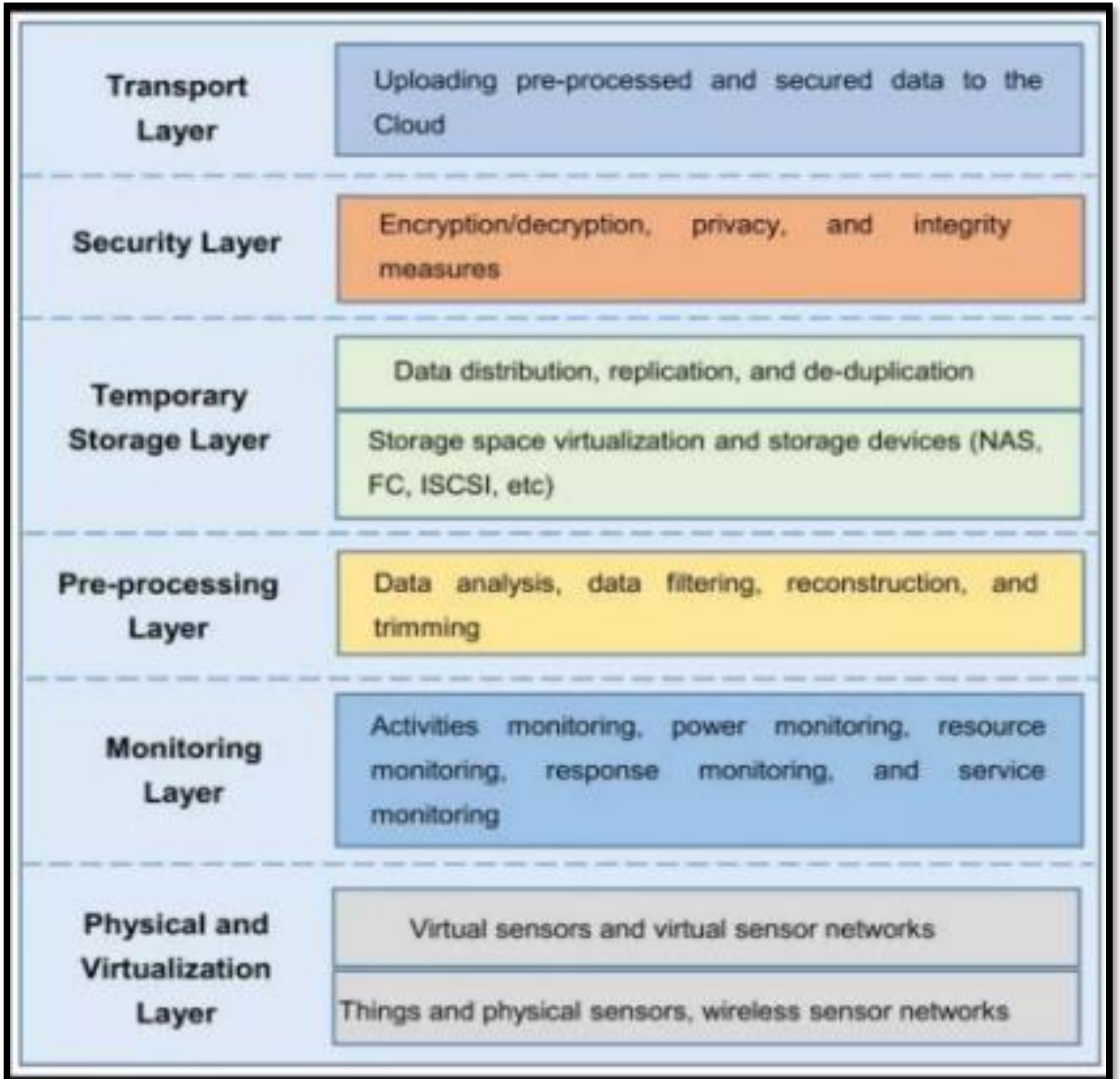
Fog is the extension of cloud computing that consists of multiple edge nodes directly connected.

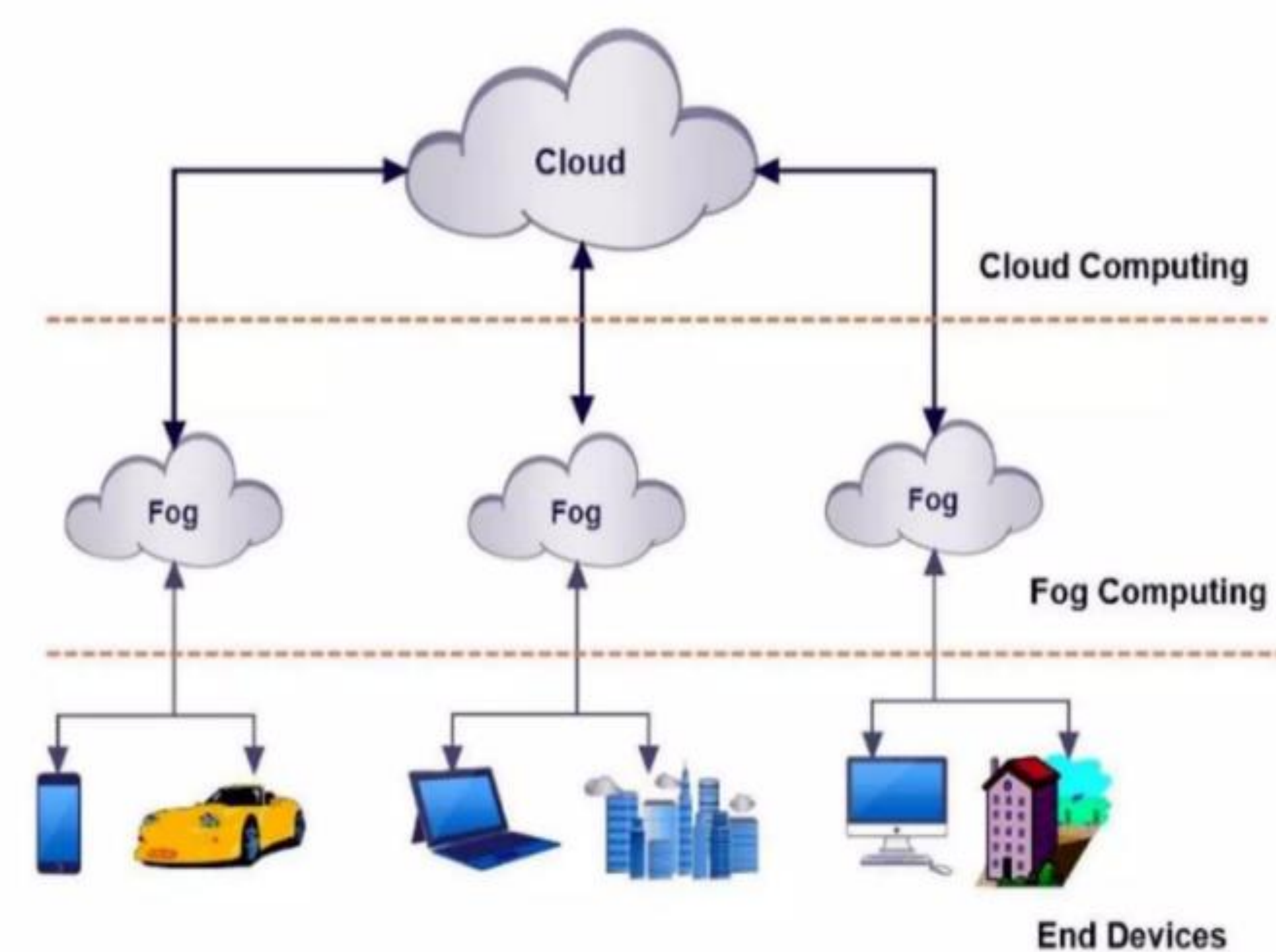
## What is Fog Computing:

Fog computing is a term for technology that extends cloud computing and services to the edge of an enterprise's network. It allows data, applications, and other resources to be moved closer to, or even on top of, end users.

Such nodes are physically much closer to devices if compared to centralized data centers, which is why they are able to provide instant connections.

# Fog Architecture:




Cloud
Cloud Computing
Fog
Fog
Fog
Fog Computing
End Devices

**Transporting data through fog computing has the following steps:**

- Signals from IoT devices are wired to an automation controller which then executes a control system program to automate the devices.

- The control system program sends data through to an OPC server or protocol gateway.

- The data is then converted into a protocol that can be more easily understood by internet-based services (Typically this is a protocol like HTTP or MQTT).

- Finally, the data is sent to a fog node or IoT gate way which collects the data for further analysis. This will filter the data and in some cases save it to hand over to the cloud later.

## Applications of fog computing:

**Linked vehicles:** Self-driven or self-driven vehicles are producing a significant volume of data, such as traffic, driving conditions, environment, etc. All this information is processed quickly with the aid of fog computing.

**Smart Grids and Smart Cities:** Energy networks use real-time data for the efficient management of systems. Fog computing is constructed in such a manner that all problems can be sorted.

**Real-time analytics:** Data can be transferred using fog computing deployments from the location where it is produced to different locations. Fog computing is used for real-time analytics that passes data to financial institutions that use real-time data from production networks.

## Sensor Cloud:

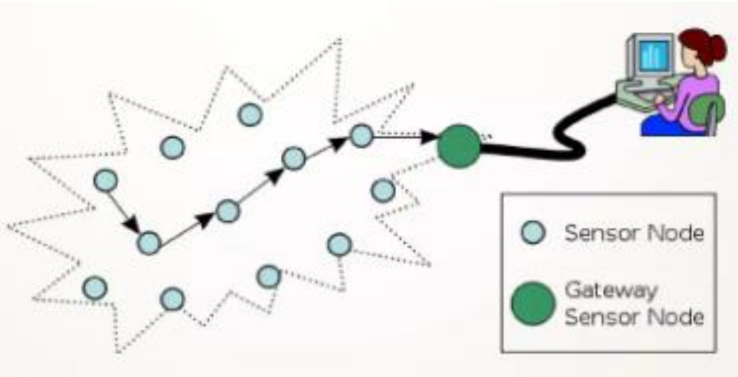
A sensor-cloud is the combination of WSNs and cloud computing and controls sensor networks through a cloud for information collection, processing, and storage

## Wireless Sensor Network:

- A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions.

- Monitors temperature, sound, pressure, etc.

- Used in healthcare, military, critical infrastructure monitoring, environment monitoring, and manufacturing.



## Why Sensor Cloud?

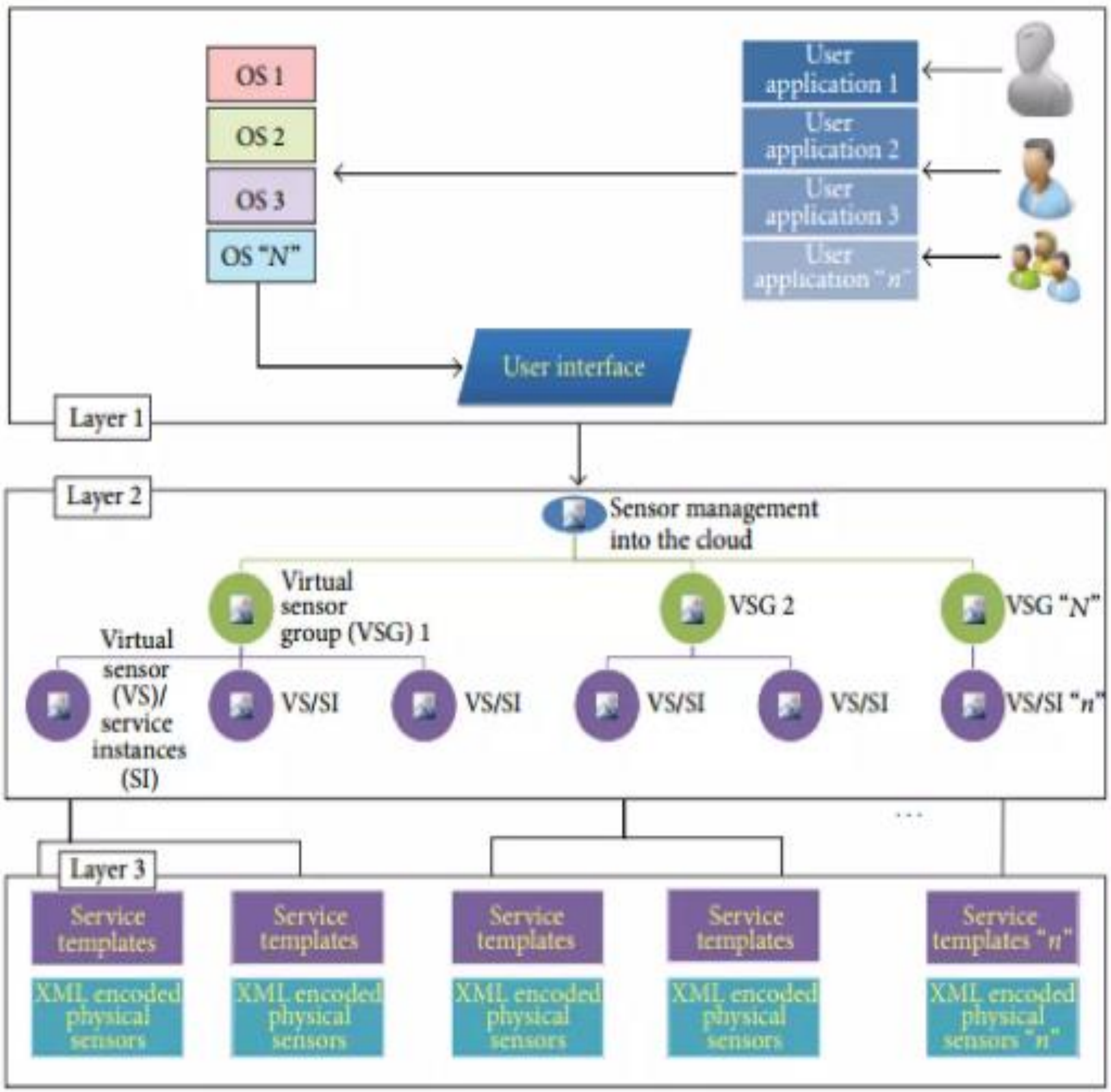
Sensors are limited in energy, processing power, memory, and communication band width.

WSNs have been designed to support a specific application service in mind.

Sensor data used for specific applications cannot be easily shared among different groups of users.

Cloud computing platform dynamically provisions, configures, and reconfigures the servers when needed by users.

# Architecture of Sensor Cloud:




1. User and application layers

2. Sensor-Cloud and virtualization layers,

3. Template creation and tangible sensors layers

16-01-2017

# Design Considerations:

## 1. Virtualization

- Each virtual sensor is created from one or more physical sensors which is dependent on the user application area.

- A virtual sensor group is created from one or more virtual sensors.

- Users can create virtual sensor groups and freely use the virtual sensors included the groups as if they owned sensors.

- Users can activate or inactivate their virtual sensors, check their status, and set the frequency of data collection from them.

## 2. Standardization & Automation:

- Each physical sensor provides its own functions for control and data collection.

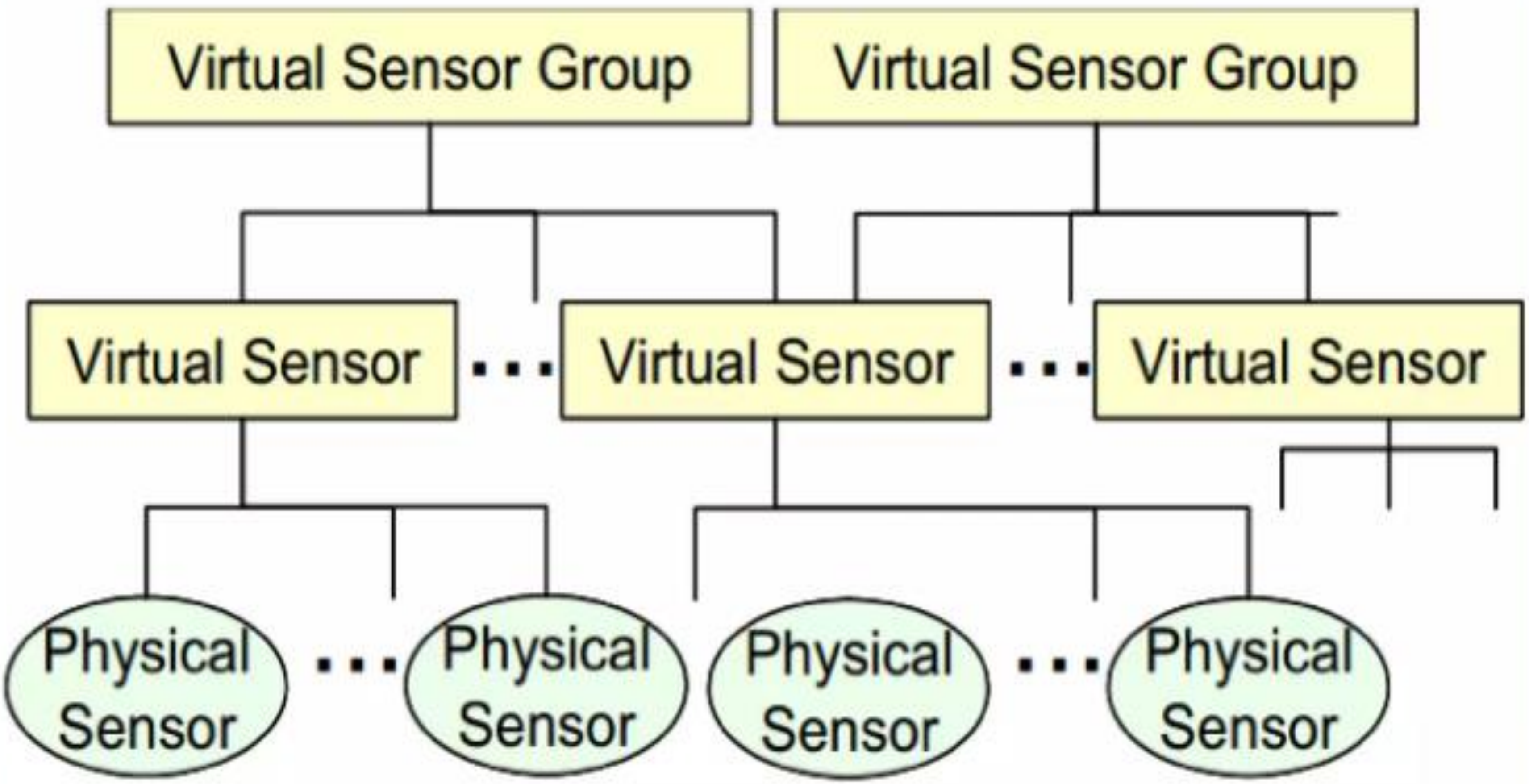
- Standard like Sensor Model Language/SML mechanism enables users to access sensors without concern for the differences among the physical sensors.

- Sensor-Cloud infrastructure translates the standard functions for the virtual sensors into specific functions for the different kinds of physical sensors.

- Automation (in terms of response of data). improves the service delivery time and reduces the cost.

- Sensor-Cloud infrastructure is an on demand service delivery and supports the full lifecycle of service delivery from the registration of physical sensors through creating templates, requesting of virtual sensors, provisioning, starting and finishing to use virtual sensors, and deleting the physical sensors.

# Design Considerations



## Applications:

### 1. Transport Monitoring

Transport monitoring system includes basic management systems like traffic signal control. navigation, emergency vehicle notification, etc.

### 2. Military Use

Sensor networks are used in the military for monitoring friendly forces, equipment and ammunition, Battlefield surveillance, Reconnaissance of opposing forces, Targeting etc.

### 3.Weather Forecasting

Weather forecasting is the application to predict the state of the atmosphere for a future time and a given location.

### 4.Health Care

Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital.

# BIG DATA:

## DATA:

The quantities, characters, or symbols on which operations are performed by a computer, which maybe stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

## BIG DATA:

Big data is a combination of structured, semi structured and unstructured data collected by organizations that can be mined for information and used in machine learning projects, predictive modeling and other advanced analytics applications.

## Importance of Big data:

Companies use big data in their systems to improve operations, provide better customer service, create personalized marketing campaigns and take other actions that, ultimately, can increase revenue and profits.

Businesses that use it effectively hold a potential competitive advantage over those that don't be cause they are able to make faster and more informed business decisions.

Both historical and real-time data can be analyzed to assess the evolving preferences of consumers or corporate buyers, enabling businesses to become more responsive to customer wants and needs.

**Types of Big Data:**

Following are the types of Big Data:

1. Structured
2. Unstructured
3. Semi-structured

## 1. Structured

Any data that can be stored, accessed and processed in the form of fixed format is termed as a structured data. However, nowadays, we are foreseeing issues when a size of such data grows to a huge extent, typical sizes are being in the rage of multiple zetta bytes.

## Examples of Structured Data

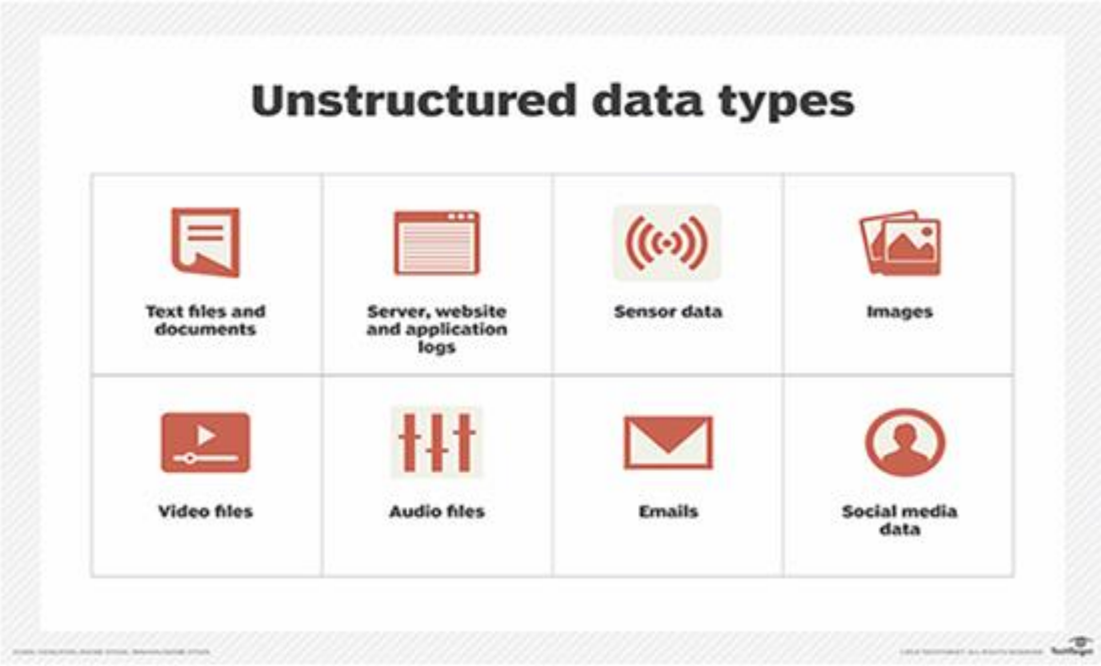
An 'Employee‘ table in a data base is an example of Structured Data

| Employee ID | Employee Name | Gender | Department | Salary In lacs |
|---|---|---|---|---|
| 2365 | Rajesh Kulkarni | Male | Finance | 650000 |
| 3398 | Pratibha Joshi | Female | Admin | 650000 |
| 7465 | Shushil Roy | Male | Admin | 500000 |
| 7500 | Shubhojit Das | Male | Finance | 500000 |
| 7699 | Priya Sane | Female | Finance | 550000 |

## Unstructured

Any data with unknown form or the structure is classified as unstructured data. In addition to the size being huge, un-structured data poses multiple challenges in terms of its processing for deriving value out of it.

A typical example of unstructured data is a heterogeneous data source containing a combination of simple text files, images, videos etc.



## Semi-structured

Semi-structured data can contain both the forms of data. We can see semi-structured data as a structured in form but it is actually not defined with e.g. a table definition in relational DBMS.

Example of semi-structured data is a data represented in an XML file.

## Characteristics of Big Data:

Big data can be described by the following characteristics:

- Volume
- Variety
- Velocity
- Variability

**Volume** – The name Big Data itself is related to a size which is enormous. Size of data plays a very crucial role in determining value out of data. Hence, 'Volume' is one characteristic which needs to be considered while dealing with Big Data solutions.

**Variety** – The next aspect of Big Data is its variety. Variety refers to heterogeneous sources and the nature of data, both structured and unstructured. Nowadays, data in the form of emails, photos, videos, monitoring devices, PDFs, audio, etc.

**Velocity** – The term 'velocity' refers to the speed of generation of data. Big Data Velocity deals with the speed at which data flows in from sources like business processes, application logs, networks, and social media sites, sensors, Mobile devices, etc.

**Variability** – This refers to the inconsistency which can be shown by the data at times, thus hampering the process of being able to handle and manage the data effectively.

## Types of data that comes under big data.

1. Black box data: The black box of aeroplane, jets, Helicopter
2. Social media data: Different social media websites
3. Stock exchange data: Buy and sell shares
4. Transport data: The transport model, capacity, distance
5. Search engine data: Retrieve data from different data base.

## Advantages of Big Data Processing

Ability to process Big Data in DBMS brings in multiple benefits, such as

- Businesses can utilize outside intelligence while taking decisions
- Improved customer service
- Early identification of risk to the product/services, ifany
- Better operational efficiency

# Overview of Industry 4.0 and Industrial Internet of Things:

# Thank you

# Thanks!

Contact us:


A. Bhaktha Vatsala
**Associate Professor**
**Department of EEE**
**PBR VITS**
**Kavali - 524201**

E-Mail: bhaktha1000@gmail.com

Mobile: **+91 9848651775**