**What Is IoT**

    IoT stands for Internet of Things. It refers to the interconnectedness of physical devices, such as appliances and vehicles that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

**Internet of Things (IoT)** is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a very few of the categorical examples where IoT is strongly established.

***IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.***

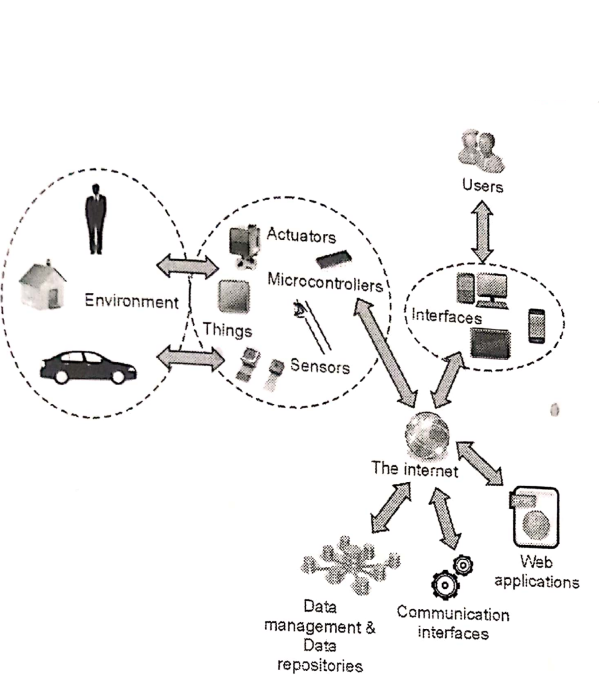
**Main components used in IoT:**

* **Low-power embedded systems:**Less battery consumption, high performance are the inverse factors that play a significant role during the design of electronic systems.
* **Sensors :**Sensors are the major part of any IoT applications. It is a physical device that measures and detect certain physical quantity and convert it into   signal which can be provide as an input to processing or control unit for analysis purpose.

1. Different types of Sensors :
2. Temperature Sensors
3. Image Sensors
4. Gyro Sensors
5. Obstacle Sensors
6. RF Sensor
7. IR Sensor
8. MQ-02/05 Gas Sensor
9. LDR Sensor
10. Ultrasonic Distance Sensor

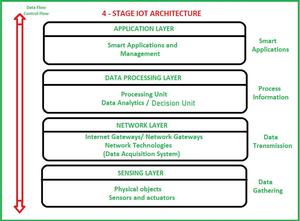
* **Control Units :** It is a unit of small computer on a single integrated circuit containing microprocessor or processing core, memory and programmable input/output devices/peripherals. It is responsible for major processing work of IoT devices and all logical operations are carried out here.
* **Cloud computing:**Data collected through IoT devices is massive and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system.
* **Availability of big data:**We know that IoT relies heavily on sensors, especially in real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.
* **Networking connection:**In order to communicate, internet connectivity is a must where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

**Working with IoT Devices :**



* *Collect and Transmit Data :*For this purpose sensors are widely used they are used as per requirements in different application areas.
* *Actuate device based on triggers produced by sensors or processing devices :*If certain condition is satisfied or according to user’s requirements if certain trigger is activated then which action to performed that is shown by Actuator devices.
* *Receive Information :*From network devices user or device can take certain information also for their analysis and processing purposes*.*
* *Communication Assistance :*Communication assistance is the phenomena of communication between 2 network or communication between 2 or more IoT devices of same or different Networks. This can be achieved by different communication protocols like : MQTT , Constrained Application Protocol, ZigBee, FTP, HTTP etc.

# Architecture of Internet of Things (IoT)



1. **Sensing Layer –**   
   The sensing layer is the first layer of the IoT architecture and is responsible for collecting data from different sources. This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters. These devices are connected to the network layer through wired or wireless communication protocols.
2. **Network Layer –**   
   The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system. It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet. Examples of network technologies that are commonly used in IoT include WiFi, Bluetooth, Zigbee, and cellular networks such as 4G and 5G. Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wider internet, and may also include security features such as encryption and authentication to protect against unauthorized access.
3. **Data processing Layer –**   
   The data processing layer of IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing, and interpreting data from IoT devices. This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action.The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms. These tools are used to extract meaningful insights from the data and make decisions based on that data.**Example** of a technology used in the data processing layer is a data lake, which is a centralized repository for storing raw data from IoT devices.
4. **Application Layer –**   
   The application layer of IoT architecture is the topmost layer that interacts directly with the end-user. It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices.This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure. It also includes middleware services that allow different IoT devices and systems to communicate and share data seamlessly.The application layer also includes analytics and processing capabilities that allow data to be analyzed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities.

**Characteristics of IoT:**

* Massively scalable and efficient
* IP-based addressing will no longer be suitable in the upcoming future.
* An abundance of physical objects is present that do not use IP, so IoT is made possible.
* Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
* A device that is connected to another device right now may not be connected in another instant of time.
* Intermittent connectivity – IoT devices aren’t always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

### Advantages of IoT :

1. Improved efficiency and automation of tasks.
2. Increased convenience and accessibility of information.
3. Better monitoring and control of devices and systems.
4. Greater ability to gather and analyze data.
5. Improved decision-making.
6. Cost savings.

### Disadvantages of IoT :

1. Security concerns and potential for hacking or data breaches.
2. Privacy issues related to the collection and use of personal data.
3. Dependence on technology and potential for system failures.
4. Limited standardization and interoperability among devices.
5. Complexity and increased maintenance requirements.
6. High initial investment costs.
7. Limited battery life on some devices.
8. Concerns about job displacement due to automation.
9. Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.

What is IoT platform?

An IoT platform is **a set of components that allows developers to spread out the applications, remotely collect data, secure connectivity, and execute sensor management**. An IoT platform manages the connectivity of the devices and allows developers to build new mobile software applications.

# Internet of Things (IoT) Development Platforms

### Google Cloud IoT Platform

The giant Techno company has used the IoT platforms for efficiency. According to Google, the Cloud Platform is the top part for encouraging IoT technology. Moreover, with the utmost security system, Google Cloud offers complete functioning effectively. Standing as one of the top Internet of Things Platforms, it offers various fascinating features. For example, robust A.I. aptitudes, Fast business procedures, Machine learning with vast capacity. Not only these, but the Google Cloud IoT also increases the work rate of the devices. This platform uses cloud amenities to lessen the cost and inspires location intelligence as well. They mainly focus on effective, fast, and efficient ways to run your business. In addition, the Google Cloud platform offers real-time understandings of devices used worldwide. This Google platform makes files maintenance and sharing easy. You can operate this IoT platform within any operating system without any problems.

### Amazon Web Services Platform for IoT

Another best Internet of Things Platform that is easily available currently. Amazon was the first and foremost company that uses the cloud as an IoT platform in the year 2004. Since that time, Amazon has put a lot of energy into building Amazon web services as the best IoT platform. This platform offers the most innovative and captivating features for its users. Also, they provide the most wide-ranging set of tools in the market. As it is easy and has a uniqueness in its properties, several companies use it throughout the world. Moreover, because of IoT device management, you can easily connect and extend your devices. Amazon authorities have examined its versatility and adaptability properly. Therefore, they assure that this platform is safe and secure for the users.

### Microsoft Azure IoT Platform

The Microsoft open-source Internet of Things platform allows you to build safe and mountable edge-to-cloud results rapidly. As per the companies’ desires, you can use this platform for developing your apps flexibly. It consists of the boosted Artificial Intelligence solutions. The Microsoft Azure IoT Platform offers ready-to-use tools, facilities, and models to develop the apps accordingly. Undoubtedly, this platform protects the data and files from the cloud. The Azure platform completely manages the databases safely. The best feature of this IoT development Platform is the Azure IoT Edge. It has the ability to function the apps even if you are offline. Moreover, this IoT is designed in such a way that different industrial sectors can easily use it. No matter, it is a manufacturing industry or transportation one.

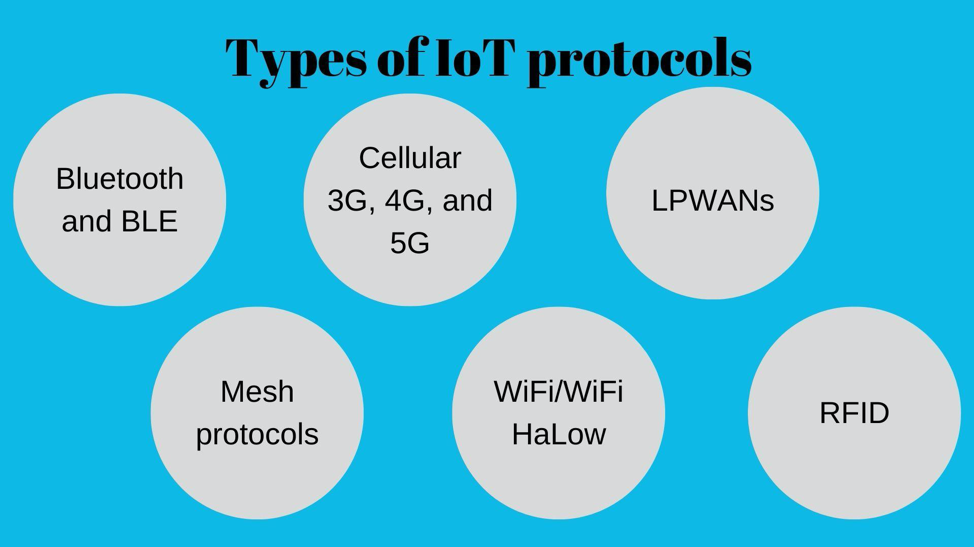
### Oracle IoT

Another notable and important Internet of Things Platform is Oracle. It is worldwide popular because of its stimulated planning for computing clouds and handling databases. The Oracle IoT platform connects the devices to the cloud without having any issues. Basically, the oracle permits the creation of IoT apps. Thereafter, it helps the devices to connect with JavaScript, Java, Android, iOS, etc. Furthermore, it enhances operational growth and improves work productivity. As Oracle is popular for its database handling services, it wires to produce a large amount of data. Due to the adaptable feature that develops business apps, several businesses opt for oracle. In addition, it offers exclusive digital individualities to devices that are connected. This enhances the faith between the apps and the devices.

### IBM Watson IoT

Last but not least, IBM Watson IoT offers various features related to IoT solutions. This offers a completely accomplished cloud service for device management. Also, it provides utmost scalability and flexibility to connected devices. The IBM Watson IoT platform helps you to collect data from several sources like assets, buildings, automobiles, and others things. Moreover, it possesses direct access to the newest data in the Cloudant NoSQL DB solution. IBM has other fine features like collecting raw data and understanding its patterns. This helps in taking out the treasured insights of the unstructured data. Also, IBM supports the easy transfer of data workload to the clouds. Moreover, this platform assists you to optimize the data and resources for your profit.

**IoT communication technologies**



### Bluetooth and BLE

Bluetooth is a 2.4GHz network for personal wireless network communication. 2.4GHz network is preferred for providing personal networks by network providers as it is cheaper and has a much better range than other networks. Bluetooth low energy (BLE) is the new and optimized version of Bluetooth for connections between IoT applications. BLE consumes lesser power than standard Bluetooth for communication. BLE-enabled devices are commonly used with electronic devices that can act as a hub for data transfer from IoT devices to the cloud. This makes BLE a perfect match for IoT wearables. BLE is widely integrated into health and fitness trackers, as well as some smart home devices like door locks. Data from BLE-enabled IoT wearables can be easily communicated to smartphones.

In the retail context, BLE can be used with [beacon technology to provide customer service](https://blog.hubspot.com/marketing/beacon-technology) like in-store navigation. Beacons are essentially small transmitters that use BLE to transmit signals to nearby IoT devices. By transmitting signals to nearby IoT devices, beacons can make location-based searching and navigation much easier and accurate.

### Cellular (3G, 4G, and 5G)

Cellular networks, as the name suggests, are well-established in the mobile consumer market. 2G is an “old school” cellular network that, along with [3G, is being phased out in most parts of the world](https://1ot.mobi/blog/2g-and-3g-networks-are-shutting-down-globally). But, the world is quickly embracing new high-speed cellular networks like 4G and 5G. Cellular networks provide high bandwidth and reliable broadband communication for voice calls or video streaming but with high operational costs and power consumption. Cellular networks cannot be used with most IoT devices due to their frequency, range, and security challenges. However, cellular networks can be viable options in some specific IoT devices like connected cars. Connected cars can use cellular networks for traffic routing with the help of GPS systems. GPS systems and cellular networks can help track road traffic in real-time as cellular networks can transfer high quantities of data over the network.

### LPWANs

LPWANs (Low Power Wide Area Networks) are new sets of protocols developed for IoT solutions but can also be used by other devices to communicate over a wide area. Even cellular networks can provide a wide-area communication network, but the cost of communication over cellular networks is high because of its high power consumption. LPWANs enable communications over wide area with the help of small and inexpensive batteries that can last for long-term making it a cost-saving option in comparison with cellular networks.

There are [different types](https://www.iotforall.com/iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/) of licensed (NB-IoT, LTE-M) and unlicensed (MIOTY, LoRa) LPWANs that are built differently for different purposes. While power consumption is one of the big challenges for licensed LPWANs, Quality of Service (QoS) and scalability are some challenges faced by unlicensed LPWANs.

Generally speaking, LPWANs can connect almost all types of sensors and enable data sharing among themselves and with the cloud. With the help of LPWANs, IoT sensors can facilitate numerous applications. For instance, sensors can allow remote monitoring of everything. However, LPWANs can send only small blocks of data over the network in a single instance, and it cannot send a large amount of data at a time.

### Mesh protocols

A mesh usually refers to a rich interconnection network of devices that are made up of devices organized in a mesh topology. [Mesh topology](https://www.link-labs.com/blog/what-is-mesh-topology) is a networking infrastructure in which all connected devices can cooperate to transfer and share data amongst each other.

ZigBee is one of the most popular mesh protocols used for IoT applications. It is a short-range, low-power protocol that is commonly deployed to extend communication over multiple IoT devices. When compared with LPWANs, ZigBee provides large data transfer at a single instance but with much less power-efficiency due to mesh infrastructure.

Due to its short physical range, ZigBee and other similar mesh protocols are best suited for medium-range IoT devices that are distributed within small areas. For instance, ZigBee protocols can be best suited for smart home sensor networks like smart lighting.

### WiFi/WiFi HaLOW

Everyone would know what WiFi is because of its pervasiveness in both industrial and home environments. However, WiFi is not used with most of the IoT devices. Except for a few applications like digital signages and security cameras, WiFi does not provide a feasible option for IoT connectivity. The use of the WiFi network is limited in IoT devices, mainly because of its low range, high power consumption, and low scalability. A lesser-known derivative of WiFi known as WiFi HaLow is introduced for IoT devices. WiFi HaLow offers increased range and improved power efficiency. However, the use of WiFi HaLow has received less support from industries as the network [offers low security](https://www.pindrop.com/blog/new-wifi-halow-protocol-could-bring-old-security-issues/).

### RFID

RFID (Radio-frequency identification) uses radio waves to transfer small data packets over the network within small areas. It is easy to embed an RFID chip in IoT devices. RFID readers can then read the tags and give information about the product that is attached to tags. One of the common applications of RFID is inventory management. By attaching RFID tags to all products and connecting it to IoT devices, businesses can keep track of the number of products available in stock. Thus RFID can help in better stock planning leading to an optimized supply chain management. RFID tags can also help smart home IoT devices. For instance, a smart washing machine that can read RFID tags can be controlled.

The use of IoT devices is increasing globally. According to an estimate, there will be [41.6 billion IoT devices generating 79.4ZB (zettabytes)](https://www.idc.com/getdoc.jsp?containerId=prUS45213219) of data in 2025. Simultaneously the chances of cyber-attacks on data may also increase. With the increased use of IoT devices and vulnerability to cyber-attacks, it is time for businesses and other stakeholders to know and choose IoT protocols and standards that can potentially keep the possibilities of cyber breaches at bay. To choose the best IoT protocol for businesses means accurately weighing the criteria of range, power consumption, bandwidth, latency, QoS, and security.

# Cloud Computing Overview

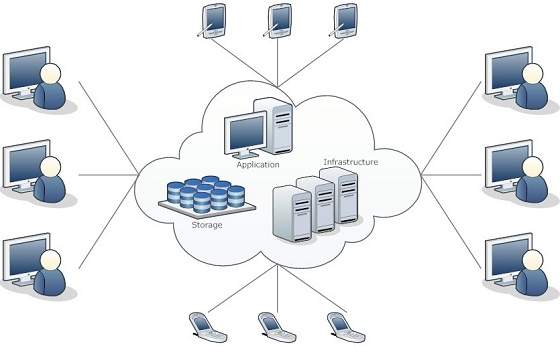
Cloud Computing provides us means of accessing the applications as utilities over the Internet. It allows us to create, configure, and customize the applications online.

## 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 public and private networks, i.e., WAN, LAN or VPN.

Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

## What is Cloud Computing?



Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

Cloud Computing refers to **manipulating, configuring,** and **accessing** the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

### CLOUD COMPUTING GUIDEBOOK - PART 3 : THE CLOUD COMPUTING REFERENCE MODEL

## Cloud computing layers

### Physical Layer

* Foundation layer of the cloud infrastructure.
* Specifies entities that operate at this layer : Compute systems, network devices and storage devices. Operating environment, protocol, tools and processes.
* Functions of physical layer : Executes requests generated by the virtualization and control layer.

### Virtual Layer

* Deployed on the physical layer.
* Specifies entities that operate at this layer : Virtualization software, resource pools, virtual resources.
* Functions of virtual layer : Abstracts physical resources and makes them appear as virtual resources (enables multitenant environment). Executes the requests generated by control layer.

### Control Layer

* Deployed either on virtual layer or on physical layer
* Specifies entities that operate at this layer : control software
* Functions of control layer : Enables resource configuration, resource pool configuration and resource provisioning. Executes requests generated by service layer. Exposes resources to and supports the service layer. Collaborates with the virtualization software and enables resource pooling and creating virtual resources, dynamic allocation and optimizing utilization of resources.

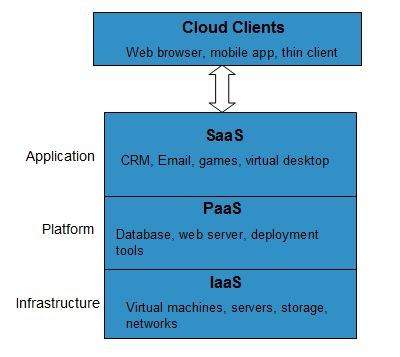
### Service Orchestration Layer

* Specifies the entities that operate at this layer : Orchestration software.
* Functions of orchestration layer : Provides workflows for executing automated tasks. Interacts with various entities to invoke provisioning tasks.

### Service Layer

* Consumers interact and consume cloud resources via this layer.
* Specifies the entities that operate at this layer : Service catalog and self-service portal.
* Functions of service layer : Store information about cloud services in service catalog and presents them to the consumers. Enables consumers to access and manage cloud services via a self-service portal.

### Service Models



Cloud computing is based on service models. These are categorized into three basic service models which are -

* Infrastructure-as–a-Service (IaaS)
* Platform-as-a-Service (PaaS)
* Software-as-a-Service (SaaS)

The **Infrastructure-as-a-Service (IaaS)** is the most basic level of service. Each of the service models inherit the security and management mechanism from the underlying model

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

#### Platform-as-a-Service (PaaS)

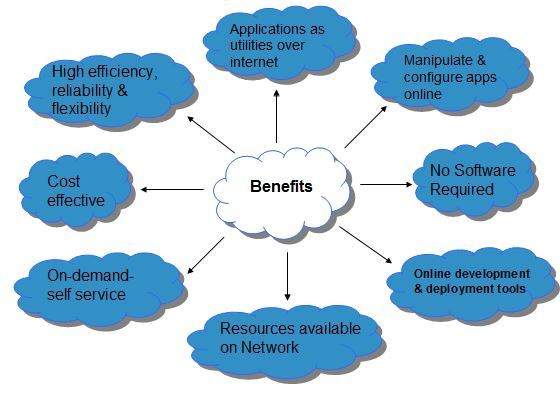
**PaaS** provides the runtime environment for applications, development and deployment tools, etc.

#### Software-as-a-Service (SaaS)

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

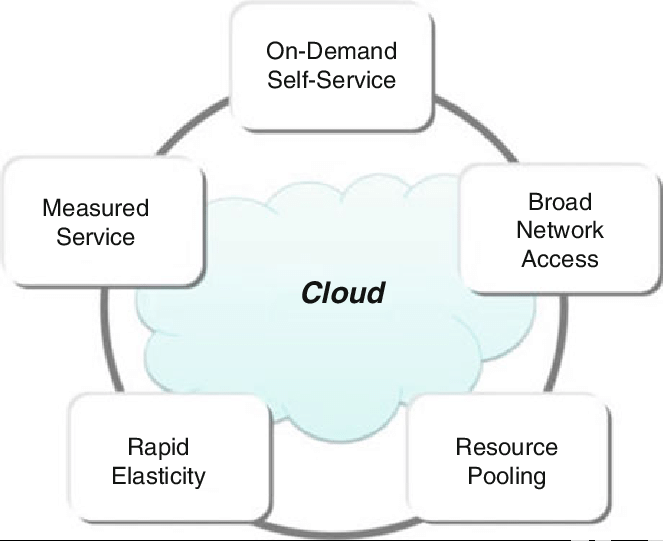
## Benefits

Cloud Computing has numerous advantages. Some of them are listed below -



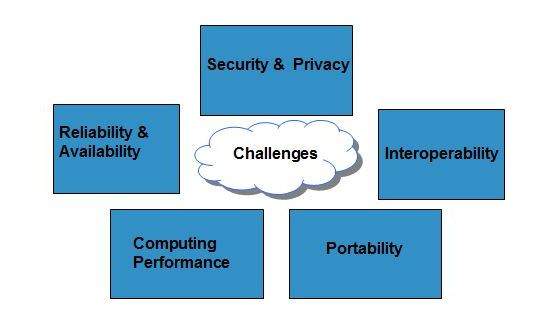
* One can access applications as utilities, over the Internet.
* One can manipulate and configure the applications online at any time.
* It does not require to install a software to access or manipulate cloud application.
* Cloud Computing offers online development and deployment tools, programming runtime environment through **PaaS model.**
* Cloud resources are available over the network in a manner that provide platform independent access to any type of clients.
* Cloud Computing offers **on-demand self-service.** The resources can be used without interaction with cloud service provider.
* Cloud Computing is highly cost effective because it operates at high efficiency with optimum utilization. It just requires an Internet connection
* Cloud Computing offers load balancing that makes it more reliable.

# Characteristics of Cloud Computing



1. **On-demand self-services:** The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.
2. **Broad network access:** The Computing services are generally provided over standard networks and heterogeneous devices.
3. **Rapid elasticity:** The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.
4. **Resource pooling:** The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.
5. **Measured service:** The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.
6. **Multi-tenancy:** Cloud computing providers can support multiple tenants (users or organizations) on a single set of shared resources.
7. **Virtualization:** Cloud computing providers use virtualization technology to abstract underlying hardware resources and present them as logical resources to users.
8. **Resilient computing:**Cloud computing services are typically designed with redundancy and fault tolerance in mind, which ensures high availability and reliability.
9. **Flexible pricing models:**Cloud providers offer a variety of pricing models, including pay-per-use, subscription-based, and spot pricing, allowing users to choose the option that best suits their needs.
10. **Security:** Cloud providers invest heavily in security measures to protect their users’ data and ensure the privacy of sensitive information.
11. **Automation:** Cloud computing services are often highly automated, allowing users to deploy and manage resources with minimal manual intervention.
12. **Sustainability:** Cloud providers are increasingly focused on sustainable practices, such as energy-efficient data centers and the use of renewable energy sources, to reduce their environmental impact.

# Cloud Computing Challenges



## Security and Privacy

Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

## Portability

This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There must not be vendor lock-in. However, it is not yet made possible because each of the cloud provider uses different standard languages for their platforms.

## Interoperability

It means the application on one platform should be able to incorporate services from the other platforms. It is made possible via web services, but developing such web services is very complex.

## Computing Performance

Data intensive applications on cloud requires high network bandwidth, which results in high cost. Low bandwidth does not meet the desired computing performance of cloud application.

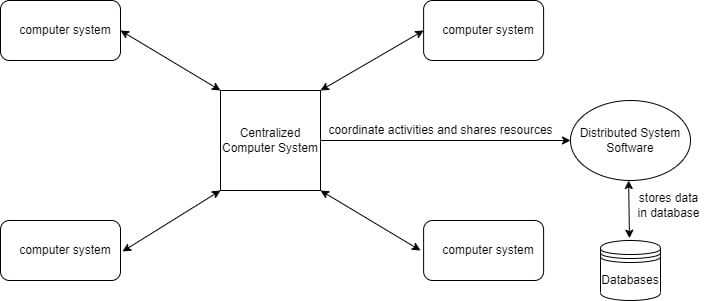
## Reliability and Availability

It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

# Distributed System

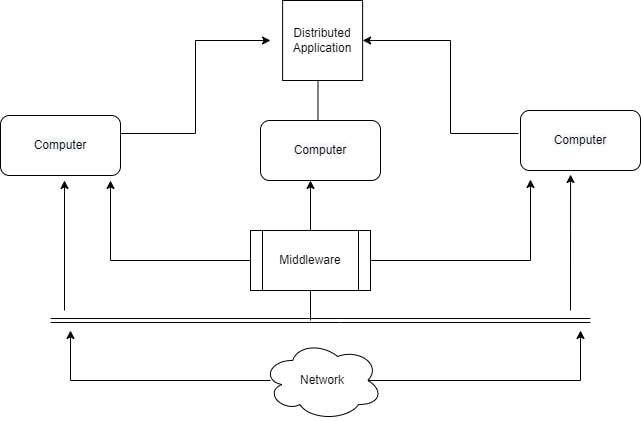
Distributed System is a collection of autonomous computer systems that are physically separated but are connected by a centralized computer network that is equipped with distributed system software. The autonomous computers will communicate among each system by sharing resources and files and performing the tasks assigned to them.

**Example of Distributed System:**



Any Social Media can have its Centralized Computer Network as its Headquarters and computer systems that can be accessed by any user and using their services will be the Autonomous Systems in the Distributed System Architecture.

* **Distributed System Software:**This Software enables computers to coordinate their activities and to share the resources such as Hardware, Software, Data, etc.
* **Database:**It is used to store the processed data that are processed by each Node/System of the Distributed systems that are connected to the                      Centralized network.



* As we can see that each Autonomous System has a common Application that can have its own data that is shared by the Centralized Database System.
* To Transfer the Data to Autonomous Systems, Centralized System should be having a Middleware Service and should be connected to a Network.
* Middleware Services enable some services which are not present in the local systems or centralized system default by acting as an interface between the Centralized System and the local systems. By using components of Middleware Services systems communicate and manage data.
* The Data which is been transferred through the database will be divided into segments or modules and shared with Autonomous systems for processing.
* The Data will be processed and then will be transferred to the Centralized system through the network and will be stored in the database.

### ****Characteristics of Distributed System:****

* **Resource Sharing:**It is the ability to use any Hardware, Software, or Data anywhere in the System.
* **Openness:** It is concerned with Extensions and improvements in the system (i.e., How openly the software is developed and shared with                                others)
* **Concurrency:**It is naturally present in Distributed Systems, that deal with the same activity or functionality that can be performed by separate users who are in remote locations. Every local system has its independent Operating Systems and Resources.
* **Scalability:** It increases the scale of the system as a number of processors communicate with more users by accommodating to improve the responsiveness of the system.
* **Fault tolerance:** It cares about the reliability of the system if there is a failure in Hardware or Software, the system continues to operate properly without degrading the performance the system.
* **Transparency:**It hides the complexity of the Distributed Systems to the Users and Application programs as there should be privacy in every system.
* **Heterogeneity:**Networks, computer hardware, operating systems, programming languages, and developer implementations can all vary and differ among dispersed system components.

### ****Advantages of Distributed System:****

* Applications in Distributed Systems are Inherently Distributed Applications.
* Information in Distributed Systems is shared among geographically distributed users.
* Resource Sharing (Autonomous systems can share resources from remote locations).
* It has a better price performance ratio and flexibility.
* It has shorter response time and higher throughput.
* It has higher reliability and availability against component failure.
* It has extensibility so that systems can be extended in more remote locations and also incremental growth.

### ****Disadvantages of Distributed System:****

* Relevant Software for Distributed systems does not exist currently.
* Security possess a problem due to easy access to data as the resources are shared to multiple systems.
* Networking Saturation may cause a hurdle in data transfer i.e., if there is a lag in the network then the user will face a problem accessing data.
* In comparison to a single user system, the database associated with distributed systems is much more complex and challenging to manage.
* If every node in a distributed system tries to send data at once, the network may become overloaded.

# Virtualization in Cloud Computing

**Virtualization** is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

## concept behind the Virtualization

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**

## Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

### Hardware Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

**Usage:**

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

### Operating System Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization.

**Usage:**

Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

### Server Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

**Usage:**

Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

### Storage Virtualization:

Storage virtualization is the *process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device*.

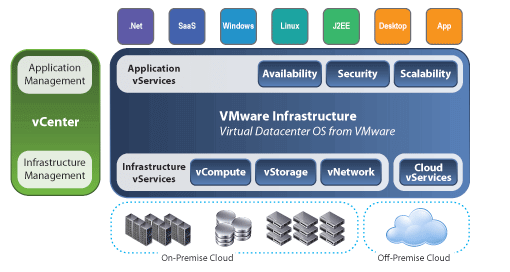
Storage virtualization is also implemented by using software applications.

**Usage:**

Storage virtualization is mainly done for back-up and recovery purposes.

**usage of Virtualization Technology**

**Virtualization** plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like application etc, but actually with the help of virtualization users shares the Infrastructure.



The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.

To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.