What is Cloud Computing?

Cloud Computing is defined as storing and accessing of data and computing services over the internet. It doesn't store any data on your personal computer. It is the on-demand availability of computer services like servers, data storage, networking, databases, etc. The main purpose of cloud computing is to give access to data centers to many users. Users can also access data from a remote server.

Examples of Cloud Computing Services: AWS, Azure, Google

Types of Clouds

There are four different cloud models that you can subscribe according to business needs. Following are the different Types of Clouds:

1. **Private Cloud:** Here**,** computing resources are deployed for one particular organization. This method is more used for intra-business interactions. Where the computing resources can be governed, owned and operated by the same organization.
2. **Community Cloud:** Here**,** computing resources are provided for a community and organizations.
3. **Public Cloud:** This type of cloud is used usually for B2C (Business to Consumer) type interactions. Here the computing resource is owned, governed and operated by the government, an academic or business organization.
4. **Hybrid Cloud:** This type of cloud can be used for both types of interactions – B2B (Business to Business) or B2C (Business to Consumer). This deployment method is called hybrid cloud as the computing resources are bound together by different clouds.

Benefits of Cloud Computing

Characteristics of Cloud Computing

The characteristics of cloud computing are given below:

1) Agility

The cloud **works in a distributed computing environment**. It shares resources among users and works very fast.

2) High availability and reliability

The availability of servers is high and more reliable because the **chances of infrastructure failure are minimum**.

3) High Scalability

Cloud offers **"on-demand" provisioning of resources on a large scale**, without having engineers for peak loads.

4) Multi-Sharing

With the help of cloud computing, **multiple users and applications can work more efficiently** with cost reductions by sharing common infrastructure.

5) Device and Location Independence

Cloud computing enables the users to access systems using a web browser regardless of their location or what device they use e.g. PC, mobile phone, etc. **As infrastructure is off-site** (typically provided by a third-party) **and accessed via the Internet, users can connect from anywhere**.

6) Maintenance

Maintenance of cloud computing applications is easier, since they **do not need to be installed on each user's computer and can be accessed from different places**. So, it reduces the cost also.

7) Low Cost

By using cloud computing, the cost will be reduced because to take the services of cloud computing, **IT company need not to set its own infrastructure** and pay-as-per usage of resources.

8) Services in the pay-per-use mode

Application Programming Interfaces **(APIs) are provided to the users so that they can access services on the cloud** by using these APIs **and pay the charges as per the usage of services**.

Advantages of Cloud Computing

1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) IServices in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

Disadvantages of Cloud Computing

A list of the disadvantage of cloud computing is given below -

1) Internet Connectivity

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection. If you do not have good internet connectivity, you cannot access these data. However, we have no any other way to access data from the cloud.

2) Vendor lock-in

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.

3) Limited Control

As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastructure.

4) Security

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.

Cloud Computing Architecture

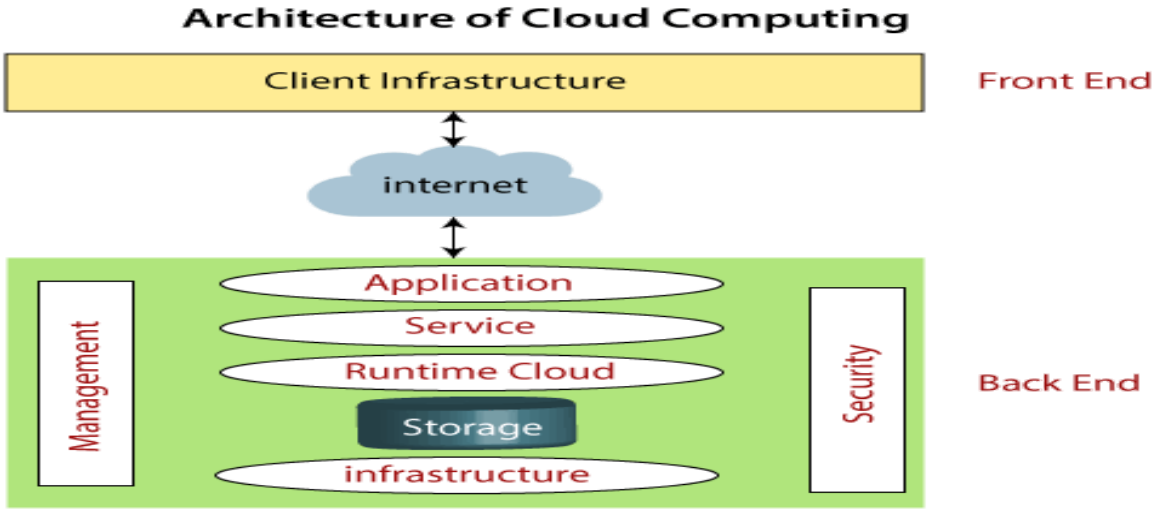
As we know, cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at anytime using the internet connection.

Cloud computing architecture is a combination of **service-oriented architecture** and **event-driven architecture**.

Cloud computing architecture is divided into the following two parts -

- Front End
- Back End

The below diagram shows the architecture of cloud computing -



Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc.

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

1. Client Infrastructure

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

2. Application

The application may be any software or platform that a client wants to access.

3. Service

A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

i. Software as a Service (SaaS) – It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. Some important example of SaaS is given below –

Example: Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

ii. Platform as a Service (PaaS) – It is also known as **cloud platform services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.

Example: Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

iii. Infrastructure as a Service (IaaS) – It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments.

Example: Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

4. Runtime Cloud

Runtime Cloud provides the **execution and runtime environment** to the virtual machines.

5. Storage

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

6. Infrastructure

It provides services on the **host level**, **application level**, and **network level**. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

7. Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

8. Security

Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

9. Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

Difference between cloud computing and grid computing:-

Cloud Computing	Grid Computing
Cloud Computing follows client-server computing architecture.	**Grid computing follows a distributed computing architecture.**
Scalability is high.	**Scalability is normal.**
Cloud Computing is more flexible than grid computing.	**Grid Computing is less flexible than cloud computing.**
Cloud operates as a centralized management system.	**Grid operates as a decentralized management system.**
In cloud computing, cloud servers are owned by infrastructure providers.	**In Grid computing, grids are owned and managed by the organization.**
Cloud computing uses services like Iaas, PaaS, and SaaS.	**Grid computing uses systems like distributed computing, distributed information, and distributed pervasive.**
Cloud Computing is Service-oriented.	**Grid Computing is Application-oriented.**
It is accessible through standard web protocols.	**It is accessible through grid middleware.**

Cloud Computing Applications

Cloud service providers provide various applications in the field of art, business, data storage and backup services, education, entertainment, management, social networking, etc.

1. Art Applications

Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets,** and **images**. Some most commonly used cloud art applications are given below:

1. **Moo:- Moo is one of the best cloud art applications. It is used for designing and printing business cards, postcards, and mini cards.**
2. **Vistaprint:- Vistaprint allows us to easily design various printed marketing products such as business cards, Postcards, Booklets, and wedding invitations cards.**
3. **Adobe Creative Cloud:- Adobe creative cloud is made for designers, artists, filmmakers, and other creative professionals. It is a suite of apps which includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.**

2. Business Applications

Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.

There are the following business applications of cloud computing -

i. MailChimp

MailChimp is an **email publishing platform** which provides various options to **design, send,** and **save** templates for emails.

iii. Salesforce

Salesforce platform provides tools for sales, service, marketing, e-commerce, and more. It also provides a cloud development platform.

iv. Chatter

Chatter helps us to **share important information** about the organization in real time.

v. Bitrix24

Bitrix24 is a **collaboration** platform which provides communication, management, and social collaboration tools.

vi. Paypal

Paypal offers the simplest and easiest **online payment** mode using a secure internet account. Paypal accepts the payment through debit cards, credit cards, and also from Paypal account holders.

vii. Slack

Slack stands for **Searchable Log of all Conversation and Knowledge**. It provides a **user-friendly** interface that helps us to create public and private channels for communication.

viii. Quickbooks

Quickbooks works on the terminology "**Run Enterprise anytime, anywhere, on any device**." It provides online accounting solutions for the business. It allows more than 20 users to work simultaneously on the same system.

3. Data Storage and Backup Applications

Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.

A list of data storage and backup applications in the cloud are given below -

i. Box.com

Box provides an online environment for **secure content management, workflow,** and **collaboration**. It allows us to store different files such as Excel, Word, PDF, and images on the cloud. The main advantage of using box is that it provides drag & drop service for files and easily integrates with Office 365, G Suite, Salesforce, and more than 1400 tools.

ii. Mozy

Mozy provides powerful **online backup solutions** for our personal and business data. It schedules automatically back up for each day at a specific time.

iii. Joukuu

Joukuu provides the simplest way to **share** and **track cloud-based backup files**. Many users use joukuu to search files, folders, and collaborate on documents.

iv. Google G Suite

Google G Suite is one of the best **cloud storage** and **backup** application. It includes Google Calendar, Docs, Forms, Google+, Hangouts, as well as cloud storage and tools for managing cloud apps. The most popular app in the Google G Suite is Gmail. Gmail offers free email services to users.

4. Education Applications

Cloud computing in the education sector becomes very popular. It offers various **online distance learning platforms** and **student information portals** to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.

There are the following education applications offered by the cloud -

i. Google Apps for Education

Google Apps for Education is the most widely used platform for free web-based email, calendar, documents, and collaborative study.

ii. Chromebooks for Education

Chromebook for Education is one of the most important Google's projects. It is designed for the purpose that it enhances education innovation.

iii. Tablets with Google Play for Education

It allows educators to quickly implement the latest technology solutions into the classroom and make it available to their students.

iv. AWS in Education

AWS cloud provides an education-friendly environment to universities, community colleges, and schools.

5. Entertainment Applications

Entertainment industries use a **multi-cloud strategy** to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing.

i. Online games

Today, cloud gaming becomes one of the most important entertainment media. It offers various online games that run remotely from the cloud. The best cloud gaming services are Shaow, GeForce Now, Vortex, Project xCloud, and PlayStation Now.

ii. Video Conferencing Apps

Video conferencing apps provides a simple and instant connected experience. It allows us to communicate with our business partners, friends, and relatives using a cloud-based video conferencing. The benefits of using video conferencing are that it reduces cost, increases efficiency, and removes interoperability.

6. Management Applications

Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

Some important management applications are -

i. Toggl

Toggl helps users to track allocated time period for a particular project.

ii. Evernote

Evernote allows you to sync and save your recorded notes, typed notes, and other notes in one convenient place. It is available for both free as well as a paid version.

It uses platforms like Windows, macOS, Android, iOS, Browser, and Unix.

iii. Outright

Outright is used by management users for the purpose of accounts. It helps to track income, expenses, profits, and losses in real-time environment.

iv. GoToMeeting

GoToMeeting provides **Video Conferencing** and **online meeting apps**, which allows you to start a meeting with your business partners from anytime, anywhere using mobile phones or tablets. Using GoToMeeting app, you can perform the tasks related to the management such as join meetings in seconds, view presentations on the shared screen, get alerts for upcoming meetings, etc.

7. Social Applications

Social cloud applications allow a large number of users to connect with each other using social networking applications such as **Facebook, Twitter, LinkedIn,** etc.

There are the following cloud based social applications -

i. Facebook

Facebook is a **social networking website** which allows active users to share files, photos, videos, status, more to their friends, relatives, and business partners using the

cloud storage system. On Facebook, we will always get notifications when our friends like and comment on the posts.

ii. Twitter

Twitter is a **social networking** site. It is a **microblogging** system. It allows users to follow high profile celebrities, friends, relatives, and receive news. It sends and receives short posts called tweets.

iii. Yammer

Yammer is the **best team collaboration** tool that allows a team of employees to chat, share images, documents, and videos.

iv. LinkedIn

LinkedIn is a **social network** for students, freshers, and professionals.

Types of Cloud

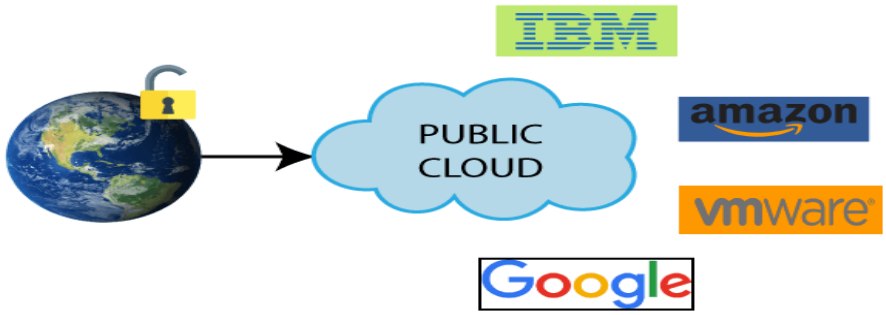
There are the following 4 types of cloud that you can deploy according to the organization's needs-

Public Cloud

Public cloud is **open to all** to store and access information via the Internet using the pay-per-usage method.

In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP).

Example: Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



Advantages of Public Cloud

- Public cloud is owned at a lower cost than the private and hybrid cloud.
- Public cloud is maintained by the cloud service provider, so do not need to worry about the maintenance.
- Public cloud is easier to integrate. Hence it offers a better flexibility approach to consumers.
- Public cloud is location independent because its services are delivered through the internet.
- Public cloud is highly scalable as per the requirement of computing resources.
- It is accessible by the general public, so there is no limit to the number of users.

Disadvantages of Public Cloud

- Public Cloud is less secure because resources are shared publicly.
- Performance depends upon the high-speed internet network link to the cloud provider.
- The Client has no control of data.

Private Cloud

Private cloud is also known as an **internal cloud** or **corporate cloud**. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.
Based on the location and management, National Institute of Standards and Technology (NIST) divide private cloud into the following two parts-

- On-premise private cloud
- Outsourced private cloud

Advantages of Private Cloud

There are the following advantages of the Private Cloud -

- Private cloud provides a high level of security and privacy to the users.
- Private cloud offers better performance with improved speed and space capacity.
- It allows the IT team to quickly allocate and deliver on-demand IT resources.
- The organization has full control over the cloud because it is managed by the organization itself. So, there is no need for the organization to depends on anybody.
- It is suitable for organizations that require a separate cloud for their personal use and data security is the first priority.

Disadvantages of Private Cloud

- Skilled people are required to manage and operate cloud services.
- Private cloud is accessible within the organization, so the area of operations is limited.

- Private cloud is not suitable for organizations that have a high user base, and organizations that do not have the prebuilt infrastructure, sufficient manpower to maintain and manage the cloud.

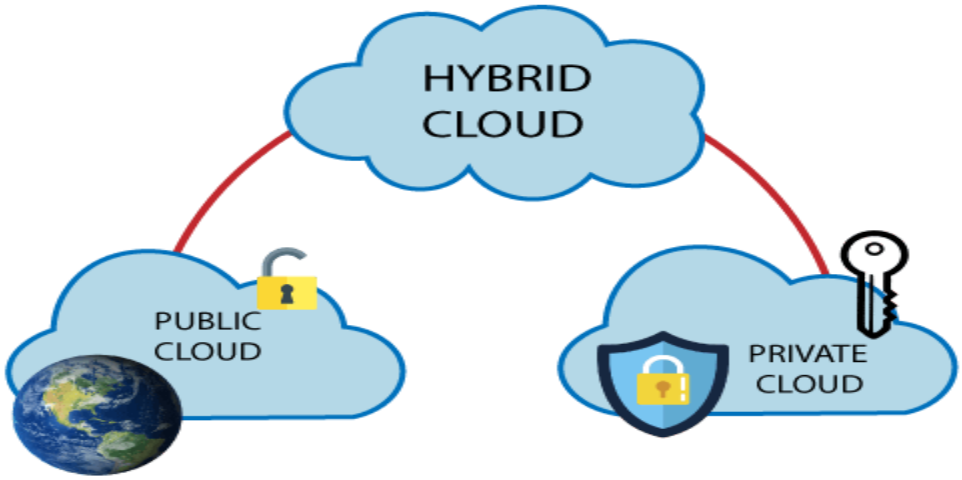
Hybrid Cloud

Hybrid Cloud is a combination of the public cloud and the private cloud. we can say:

Hybrid Cloud = Public Cloud + Private Cloud

Hybrid cloud is partially secure because the services which are running on the public cloud can be accessed by anyone, while the services which are running on a private cloud can be accessed only by the organization's users.

Example: Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office on the Web and One Drive), Amazon Web Services.



Advantages of Hybrid Cloud

There are the following advantages of Hybrid Cloud -

- Hybrid cloud is suitable for organizations that require more security than the public cloud.
- Hybrid cloud helps you to deliver new products and services more quickly.
- Hybrid cloud provides an excellent way to reduce the risk.
- Hybrid cloud offers flexible resources because of the public cloud and secure resources because of the private cloud.

Disadvantages of Hybrid Cloud

- In Hybrid Cloud, security feature is not as good as the private cloud.
- Managing a hybrid cloud is complex because it is difficult to manage more than one type of deployment model.
- In the hybrid cloud, the reliability of the services depends on cloud service providers.

Community Cloud

Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.

Example: Health Care community cloud

Advantages of Community Cloud

There are the following advantages of Community Cloud -

- Community cloud is cost-effective because the whole cloud is being shared by several organizations or communities.
- Community cloud is suitable for organizations that want to have a collaborative cloud with more security features than the public cloud.
- It provides better security than the public cloud.
- It provdes collaborative and distributive environment.
- Community cloud allows us to share cloud resources, infrastructure, and other capabilities among various organizations.

Disadvantages of Community Cloud

- Community cloud is not a good choice for every organization.
- Security features are not as good as the private cloud.
- It is not suitable if there is no collaboration.
- The fixed amount of data storage and bandwidth is shared among all community members.

SPI Framework:- A commonly agreed upon framework for describing cloud computing services goes by the acronym "SPI." This acronym stands for the three major services provided through the cloud: software-as-a-service (SaaS), platform-as-a-service (Paas), and infrastructure-as-a-service (Iaas).

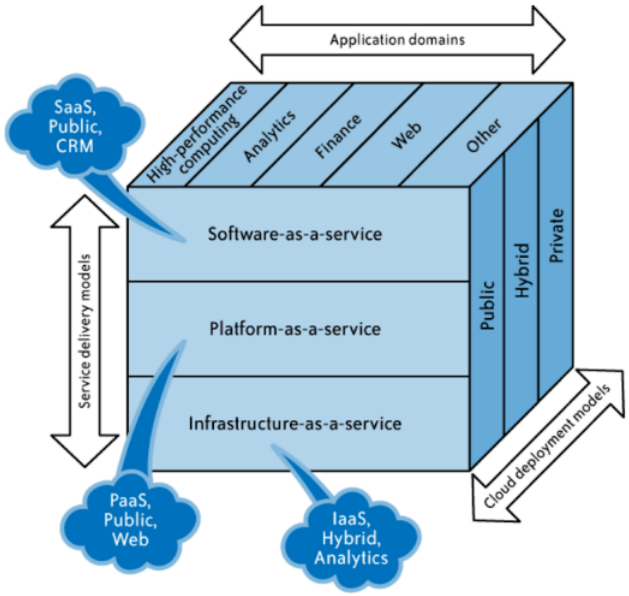


Fig.1 *SPI service model*

Difference between Cloud Computing and Distributed Computing :

S.No.	CLOUD COMPUTING	DISTRIBUTED COMPUTING
01.	Cloud computing refers to providing on demand IT resources/services like server, storage, database, networking, analytics, software etc. over internet.	Distributed computing refers to solve a problem over distributed autonomous computers and they communicate between them over a network.
02.	In simple cloud computing can be said as a computing technique that delivers hosted services over the internet to its users/customers.	In simple distributed computing can be said as a computing technique which allows to multiple computers to communicate and work to solve a single problem.
03.	It is classified into 4 different types such as Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud.	It is classified into 3 different types such as Distributed Computing Systems, Distributed Information Systems and Distributed Pervasive Systems.

04.	There are many benefits of cloud computing like cost effective, elasticity and reliable, economies of Scale, access to the global market etc.	There are many benefits of distributed computing like flexibility, reliability, improved performance etc.
05.	Cloud computing provides services such as hardware, software, networking resources through internet.	Distributed computing helps to achieve computational tasks more faster than using a single computer as it takes a lot of time.
06.	The goal of cloud computing is to provide on demand computing services over internet on pay per use model.	The goal of distributed computing is to distribute a single task among multiple computers and to solve it quickly by maintaining coordination between them.
07.	Some characteristics of cloud computing are providing shared pool of configurable computing resources, on-demand service, pay per use, provisioned by the Service Providers etc.	Some characteristics of distributed computing are distributing a single task among computers to progress the work at same time, Remote Procedure calls and Remote Method Invocation for distributed computations.
08.	Some disadvantage of cloud computing includes less control especially in the case of public clouds, restrictions on available services may be faced and cloud security	Some disadvantage of cloud computing includes chances of failure of nodes, slow network may create problem in communication.

Evolution of Cloud Computing:-

Distributed Systems:

It is a composition of multiple independent systems but all of them are depicted as a single entity to the users. The purpose of distributed systems is to share resources and also use them effectively and efficiently. Distributed systems possess characteristics such as scalability, concurrency, continuous availability, heterogeneity, and independence in failures. But the main problem with this system was that all the systems were required to be present at the same geographical location. Thus to solve

this problem, distributed computing led to three more types of computing and they were-Mainframe computing, cluster computing, and grid computing.

Mainframe computing:

Mainframes which first came into existence in 1951 are highly powerful and reliable computing machines. These are responsible for handling large data such as massive input-output operations. Even today these are used for bulk processing tasks such as online transactions etc.

Cluster computing:

In 1980s, cluster computing came as an alternative to mainframe computing. Each machine in the cluster was connected to each other by a network with high bandwidth. These were way cheaper than those mainframe systems. These were equally capable of high computations.Also, new nodes could easily be added to the cluster if it was required. Thus, the problem of the cost was solved to some extent but the problem related to geographical restrictions still pertained. To solve this, the concept of grid computing was introduced.

Grid computing:

In 1990s, the concept of grid computing was introduced. It means that different systems were placed at entirely different geographical locations and these all were connected via the internet. These systems belonged to different organizations and thus the grid consisted of heterogeneous nodes. Although it solved some problems but new problems emerged as the distance between the nodes increased. The main problem which was encountered was the low availability of high bandwidth connectivity and with it other network associated issues. Thus. cloud computing is often referred to as “Successor of grid computing”.

Virtualization:

It was introduced nearly 40 years back. It refers to the process of creating a virtual layer over the hardware which allows the user to run multiple instances simultaneously on the hardware. It is a key technology used in cloud computing. It is the base on which major cloud computing services such as Amazon EC2, VMware vCloud, etc work on. Hardware virtualization is still one of the most common types of virtualization.

Web 2.0:

It is the interface through which the cloud computing services interact with the clients. It is because of Web 2.0 that we have interactive and dynamic web pages. It also increases flexibility among web pages. Popular examples of web 2.0 include Google Maps, Facebook, Twitter, etc. Needless to say, social media is possible because of this technology only. In gained major popularity in 2004.

Service orientation:

It acts as a reference model for cloud computing. It supports low-cost, flexible, and evolvable applications. Two important concepts were introduced in this computing

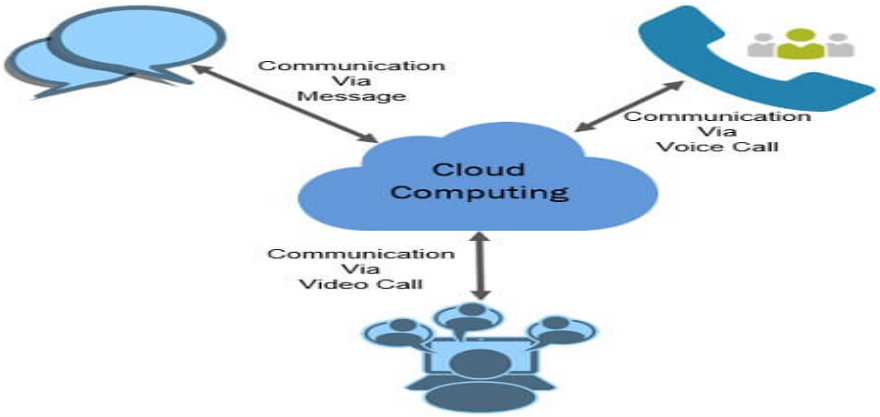
model. These were Quality of Service (QoS) which also includes the SLA (Service Level Agreement) and Software as a Service (SaaS).

Utility computing:

It is a computing model that defines service provisioning techniques for services such as compute services along with other major services such as storage, infrastructure, etc which are provisioned on a pay-per-use basis.

Communications as a Service (CaaS)

Communications as a Service (CaaS) provides Software as a Service (SaaS) for communications. There is no standard specification as to what is included in CaaS. Implementations vary. CaaS could include unified communications, broadcasting, individual calls (voice and video), conferencing (voice and video), voice over IP (VoIP), messaging, and so on.



Communication as a Service (CaaS) in Cloud Computing

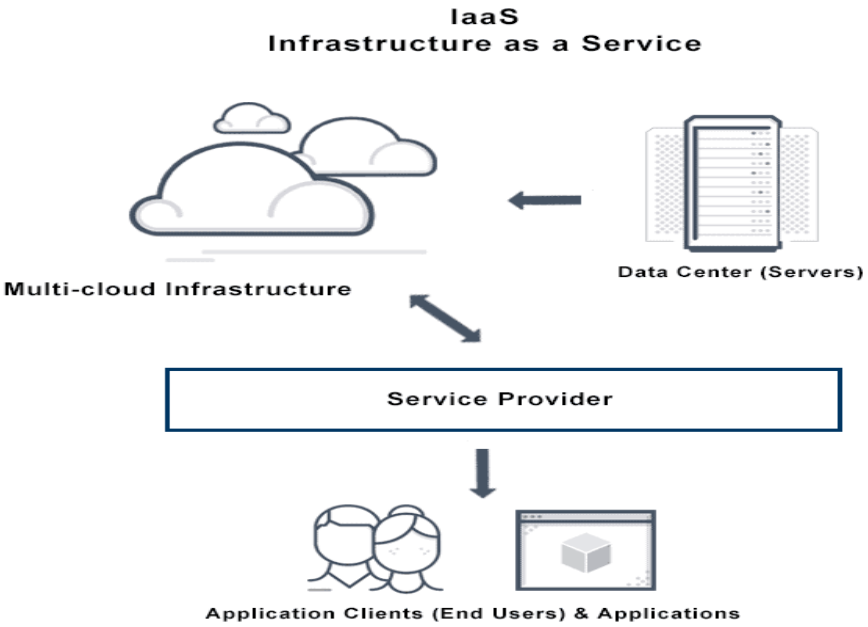
Infrastructure as a Service (IaaS)

IaaS is also known as **Hardware as a Service (HaaS)**. It is a computing infrastructure managed over the internet. The main advantage of using IaaS is that it helps users to avoid the cost and complexity of purchasing and managing the physical servers.

Characteristics of IaaS

There are the following characteristics of IaaS -

- Resources are available as a service
- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks
- **Example:** DigitalOcean, Linode, Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE)



Platform as a Service (PaaS)

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications.

Characteristics of PaaS

There are the following characteristics of PaaS -

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

Example: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine

Software as a Service (SaaS)

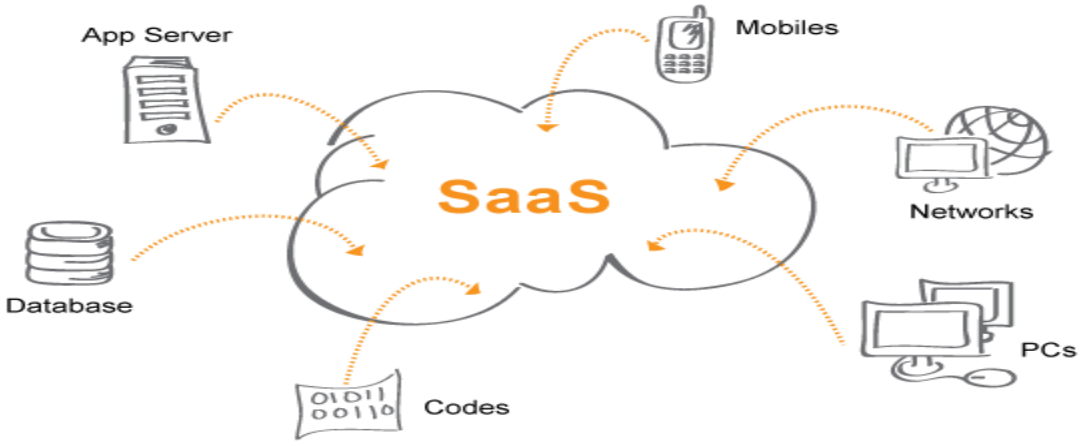
SaaS is also known as "**on-demand software**". It is a software in which the applications are hosted by a cloud service provider. Users can access these applications with the help of internet connection and web browser.

Characteristics of SaaS

There are the following characteristics of SaaS -

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.
- The services are purchased on the pay-as-per-use basis

Example: BigCommerce, Google Apps, Salesforce, Dropbox



Monitoring as a service(maas):-

Monitoring as a Service (MaaS) is a security service that provides security to IT assets of any business 24/7. It plays a vital role in securing an enterprise or government clients from any possible cyber threats. MaaS is a monitoring service that can be outsourced in a flexible and consumption-based subscription model.

Cloud Security Management:-

Cloud security management involves multiple strategies that allow a company to utilize cloud applications and networks to their fullest potential while minimizing threats and weak spots.Cloud security management is a shared responsibility. The cloud service provider has a significant role to play in providing secure infrastructure. But accountability does not end there.The client also has a substantial role in securing its digital assets including taking control of user access, user security training, and use guidance.

Cloud security is a shared responsibility:-

1. Securing the Data Center!

Is cloud hosting secure? **Before selecting your cloud service provider, you need to assess and analyze them for potential weaknesses.**
Be sure to check the providers reliability and performance against their SLAs (Service-level agreements). You can also investigate their certifications and standards.
Firewalls are an essential part of cloud architecture. They act as a safety wall around your network installation and your users.
Your cloud service provider should be able to demonstrate that their firewall and other technologies are at the leading edge of industry performance and security.

2. Manage Access Control!

Make sure that you manage who gets access to what. Employees can be internal threats to data security. Staff can either knowingly try to steal company data, become a security threat by using personal devices to attempt to access company information. Personal devices often pose a security risk as they are not secured. Make sure that you protect your data by setting access lists and permissions for all your assets. The best cloud management tools excel when it comes to creating roles and permissions.

3. Prevent Threats!

By using the right security settings, you can have full control over your data. These settings could include:

- the intelligent use of data masking
- virtual private networks (VPNs)
- encryption

These are just some ways to use security settings to prevent threats from becoming something more serious.
It's possible to lose sight of how your security settings are configured to protect you. This is why it's a good idea to use a reliable Cloud Security Posture Management (CSPM) system. A is a systemized process of continuous improvement that:

- cleans your cloud environment and
- alerts you to any risks.

It acts as a powerful warning system that will tell you if an external threat has bypassed any of your threat prevention measures.

4. Detect Threats!

Threat intelligence refers to the process of locating and managing potential threats that can cause harm to your network. Cloud computing has all the tools to give you superior threat detection at all your endpoints such as company laptops and phones.
You can even rank your assets in order of strategic importance. For example, a laptop might have access to more systems and might need stronger security than a mobile phone which might only be used for emails.
With robust threat detection measures, it becomes harder for malicious actors to access your cloud server.

5. Mitigate Threats!

When encrypting data, you must take special precautions to prevent data loss and keep high data integrity levels. Make sure that your systems have robust and intelligent threat mitigation mechanisms that can decide what to do with a suspicious file.
This could include:

- Blocking access
- Quarantining the file
- Purging the file
- Restoring the file

A good threat mitigation system should be able to do this without compromising genuine network traffic that is essential to your operations.

6. Redundancy!

If your data is lost or stolen, you will need a disaster recovery plan. Your cloud management system can manage data redundancy within the cloud. It's much better having a plan to recover data than to negotiate with a party that stole your data. Your operations will not suffer too much because you can quickly recover.

7. Legal Compliance!

Many large enterprises need to comply with data storage regulations. There are so many rules and regulations in terms of cloud computing implementation and security.
Once you find out your industry and location-specific legal requirements, you will find that managed cloud security has a solution for you. An example of this could involve retaining consumer information for a while or deleting it within a set period.

8. Cloud security reporting!

Companies sometimes overlook cloud security reporting because they assume that security is the cloud service provider's domain. You need to closely monitor the diagnostics from cloud software and report any suspicious events to your security teams.
Build up a bank of information so that you fully understand what your security exposure is. If one area of your network reports repeated irregularities, it's worth looking into it.

Cloud Security Architecture

A cloud security architecture (also sometimes called a "cloud computing security architecture") is defined by the security layers, design, and structure of the platform, tools, software, infrastructure, and best practices that exist within a cloud security solution. A cloud security architecture provides the written and visual model to define how to configure and secure activities and operations within the cloud, including such things as identity and access management; methods and controls to protect applications and data.

Key Elements of a Cloud Security Architecture

- Security at Each Layer
- Centralized Management of Components
- Redundant & Resilient Design
- Elasticity & Scalability
- Appropriate Storage for Deployments
- Alerts & Notifications
- Centralization, Standardization, & Automation

Principles of Cloud Security Architecture

A well-designed cloud security architecture should be based on the following key principles:

- **Identification**—Knowledge of the users, assets, business environment, policies, vulnerabilities and threats, and risk management strategies (business and supply chain) that exist within your cloud environment.
- **Security Controls**—Defines parameters and policies implemented across users, data, and infrastructure to help manage the overall security posture.
- **Security by Design**—Defines the control responsibilities, security configurations, and security baseline automations. Usually standardized and repeatable for deployment across common use cases, with security standards, and in audit requirements.
- **Compliance**—Integrates industry standards and regulatory components into the architecture and ensures standards and regulatory responsibilities are met.
- **Perimeter Security**—Protects and secures traffic in and out of organization's cloud-based resources, including connection points between corporate network and public internet.
- **Segmentation**—Partitions the architecture into isolated component sections to prevent lateral movement in the case of a breach. Often includes principles of 'least privilege'.
- **User Identity and Access Management**—Ensures understanding, visibility, and control into all users (people, devices, and systems) that access corporate assets. Enables enforcement of access, permissions, and protocols.
- **Data encryption**—Ensures data at rest and traveling between internal and external cloud connection points is encrypted to minimize breach impact.
- **Automation**—Facilitates rapid security and configuration provisioning and updates as well as quick threat detection.
- **Logging and Monitoring**—Captures activities and constant observation (often automated) of all activity on connected systems and cloud-based services to ensure compliance, visibility into operations, and awareness of threats.
- **Visibility**—Incorporates tools and processes to maintain visibility across an organization's multiple cloud deployments.
- **Flexible Design**—Ensuring architecture design is sufficiently agile to develop and incorporate new components and solutions without sacrificing inherent security.

Evolution of MSP:- The evolution of MSPs began in the 1990s with the emergence of application service providers (ASPs), which offered a level of service for remote application hosting. ASPs helped pave the way for cloud computing and companies that would provide remote support for customers' IT infrastructure. MSPs initially focused on the remote monitoring and management (RMM) of servers and networks.

What is a managed service provider ?

A managed service provider (MSP) is a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems. Small and medium-sized businesses (SMBs), nonprofits and government agencies hire MSPs to perform a defined set of day-to-day management services. These services may include network and infrastructure management, security and monitoring.

types of MSPs?

- **Pure-play MSPs.** These tend to be smaller providers that focus on monitoring networks and application performance. They offer their own native services that focus mainly on reporting and alerts.
- **Staffing legacy MSPs.** These MSPs generally target midlevel organizations and Fortune 500 companies and often offer a wide range of services, including monitoring, reporting, and software installation and upgrades.
- **High-level MSPs.** These consist of small and large providers that enable their clients to outsource as much of their IT processes as needed. Typically, high-level MSPs offer a wide range of services.
-

MSPs can also be categorized by the type of services they offer:

- **Monitoring.** These MSPs offer real-time monitoring software for different applications, network devices, servers or websites.
- **Remote support.** These MSPs offer cloud-based software, support remote devices and remotely troubleshoot technical issues.
- **Proactive support.** These MSPs perform preventative maintenance to stay ahead of any device or network issues that could arise.
- **Centralized management.** These MSPs provide a management console for complex networks, remote monitoring, patch management and security software.

- **Scheduled maintenance.** These MSPs offer organizations regularly scheduled network maintenance.
- **Simplified billing.** These MSPs handle invoicing, payments and budgeting via a billing management system.

benefits of managed service providers?

Benefits of managed service providers include the following:

- **Help an organization fill staff shortages.** If an organization lacks workers, it can outsource some of its tasks to the MSP.
- **Provide expertise.** Hiring a reputable MSP provides an organization with access to expert resources.
- **Provide business continuity**. An SLA documents the MSP's obligations to the business to prepare for or recover from a disaster.
- **Provide constant network monitoring.** Many MSPs offer 24/7 monitoring services using network monitoring tools that offer system visibility and cloud management.
- **Improve security.** Some MSPs provide security software and awareness training.

Virtualization:-Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource.With the help of Virtualization, multiple operating systems and applications can run on same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

BENEFITS OF VIRTUALIZATION

1. More flexible and efficient allocation of resources.
2. Enhance development productivity.
3. It lowers the cost of IT infrastructure.
4. Remote access and rapid scalability.
5. High availability and disaster recovery.
6. Pay peruse of the IT infrastructure on demand.
7. Enables running multiple operating systems.

Types of Virtualization:

1.Application Virtualization.
2.Network Virtualization.
3.Desktop Virtualization.

4.Storage Virtualization.
5.Server Virtualization.
6.Data virtualization.

1. Application Virtualization:

Application virtualization helps a user to have remote access of an application from a server. The server stores all personal information and other characteristics of the application but can still run on a local workstation through the internet. Example of this would be a user who needs to run two different versions of the same software. Technologies that use application virtualization are hosted applications and packaged applications.

2. Network Virtualization:

The ability to run multiple virtual networks with each has a separate control and data plan. It co-exists together on top of one physical network. It can be managed by individual parties that potentially confidential to each other.

Network virtualization provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.

3. Desktop Virtualization:

Desktop virtualization allows the users' OS to be remotely stored on a server in the data centre. It allows the user to access their desktop virtually, from any location by a different machine. Users who want specific operating systems other than Windows Server will need to have a virtual desktop. Main benefits of desktop virtualization are user mobility, portability, easy management of software installation, updates, and patches.

4. Storage Virtualization:

Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is stored, and instead function more like worker bees in a hive. It makes managing storage from multiple sources to be managed and utilized as a single repository. storage virtualization software maintains smooth operations, consistent performance and a continuous suite of advanced functions despite changes, break down and differences in the underlying equipment.

5. Server Virtualization:

This is a kind of virtualization in which masking of server resources takes place. Here, the central-server(physical server) is divided into multiple different virtual servers by

changing the identity number, processors. So, each system can operate its own operating systems in isolate manner. Where each sub-server knows the identity of the central server. It causes an increase in the performance and reduces the operating cost by the deployment of main server resources into a sub-server resource. It's beneficial in virtual migration, reduce energy consumption, reduce infrastructural cost, etc.

6. Data virtualization:

This is the kind of virtualization in which the data is collected from various sources and managed that at a single place without knowing more about the technical information like how data is collected, stored & formatted then arranged that data logically so that its virtual view can be accessed by its interested people and stakeholders, and users through the various cloud services remotely. Many big giant companies are providing their services like Oracle, IBM, At scale, Cdata, etc.

Hardware Virtualization:-Hardware virtualization can be done by extracting the physical hardware with the help of the *virtual machine monitor* (VVM).

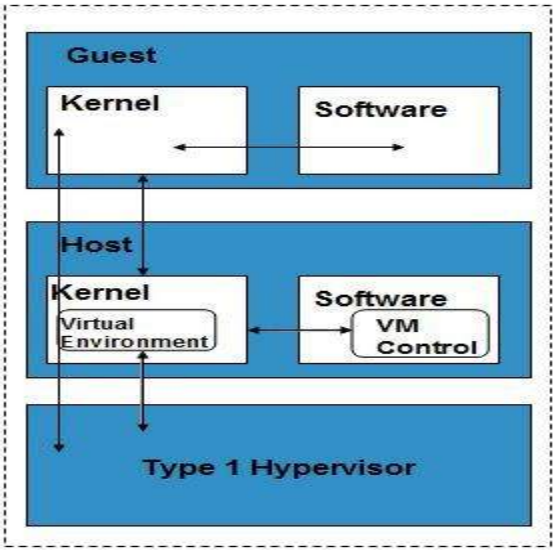
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

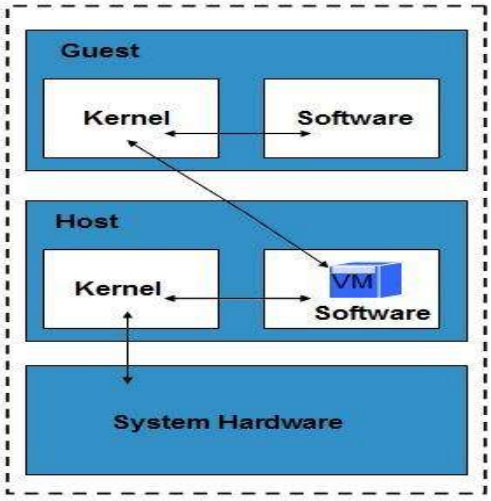
Full Virtualization

In full virtualization, the underlying hardware is completely simulated. Guest software does not require any modification to run.



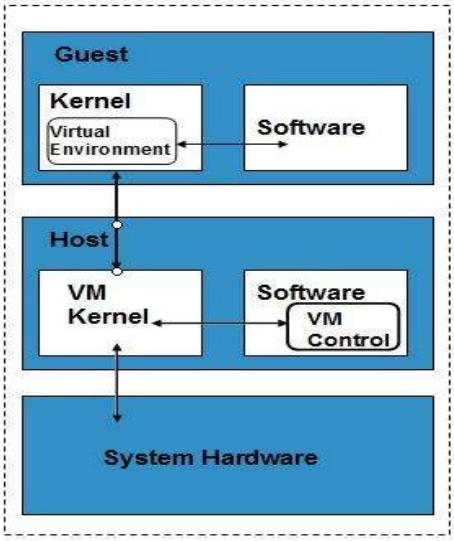
Emulation Virtualization

In Emulation, the virtual machine simulates the hardware and hence becomes independent of it. In this, the guest operating system does not require modification.



Paravirtualization

In Paravirtualization, the hardware is not simulated. The guest software run their own isolated domains.



Software Visualization:- in Cloud Computing allows the single computer server to run one or more virtual environments. It is quite similar to virtualizations but here it abstracts the software installation procedure and creates a virtual software out of it.

Types of Software Virtualization:-

- **Operating System Virtualization:-** In operating system virtualization, the hardware is used which consists of software on which different operating systems work. Here, the operating system does not interfere with each other so that each one of them works efficiently.
- **Application Virtualization:-** Application virtualization is a technology, encapsulates the computer program within the operating system. It can say that application virtualizations refer to running an application on a thin client.
- **Service Virtualization:-** In the service virtualization, the DevOps team can use the virtual servers rather than the physical one. It emulates the behaviour of essential components which will be present in the final production environment.

Virtualization Security:-

Virtualization security is the collective measures, procedures and processes that ensure the protection of a virtualization infrastructure /environment.

It addresses the security issues faced by the components of a virtualization environment and methods through which it can be mitigated or prevented.

virtualization security may include processes such as:

- Implementation of security controls and procedures granularly at each virtual machine.
- Securing virtual machines, virtual network and other virtual appliance with attacks and vulnerabilities surfaced from the underlying physical device.
- Ensuring control and authority over each virtual machine.
- Creation and implementation of security policy across the infrastructure / environment