UNIT-2

CLOUD ARCHITECTURE

Cloud Service Models

What Do You Mean By Cloud Services?

Cloud services include infrastructure, platforms, or software that are hosted by third-party cloud providers and can be accessed via users.

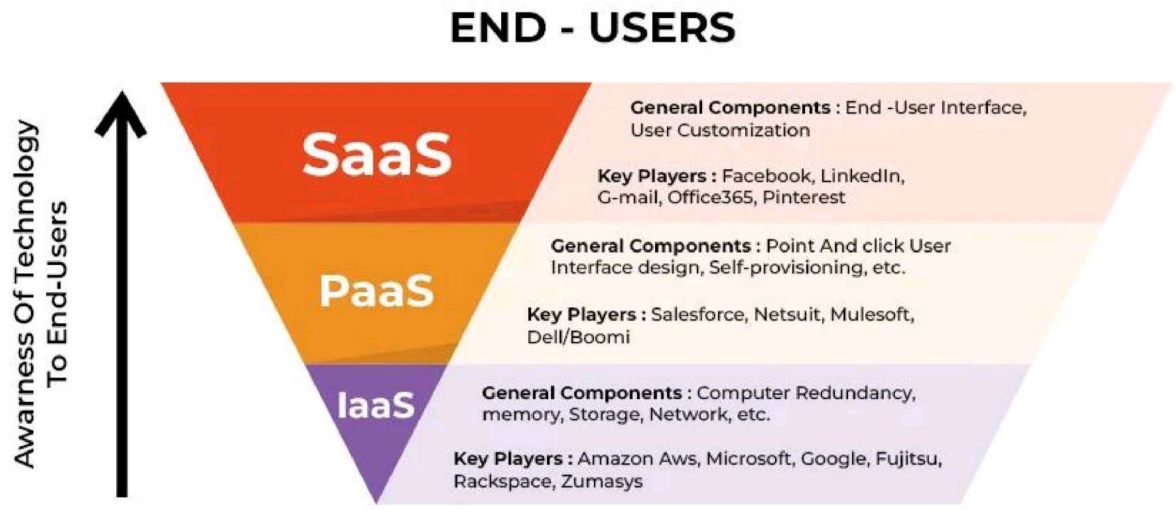
Earlier in traditional IT companies, the setup of hardware and software is done by them only to manage their data locally but with time the cloud service providers came into play which ultimately helps companies to reduce their setup and maintenance costs.

What Is A Service Model?

It is a fast-emerging business model that shifts the customer-company relationship from the traditional model of ownership to a model that evolves around providing services on a non-ownership basis.

Types Of Cloud Service Models

Based on the level of service provided, below are the 3 types of cloud service models:



1. Infrastructure As A Service (IaaS)

IaaS provides access to hardware-based fundamental resources such as physical machines, virtual machines, storage, runtime engines, firewalls, etc.

All of the above resources are made available to end users via server virtualization. Even though users do not buy the hardware resources, these resources are accessed by the customers as if they own them.

Characteristics

- Virtual machines with pre-installed software and Operating Systems such as Windows, Linux, and Solaris.
- On-demand availability of resources.
- The computing resources can be easily scaled up and down on demand.

Advantages of IaaS

- The resources can be deployed by the provider to a customer's environment at any given time.
- Its ability to offer the users to scale the business based on their requirements.
- The provider has various options when deploying resources including virtual machines, applications, storage, and networks.
- It has the potential to handle an immense number of users.
- It is easy to expand and saves a lot of money. Companies can afford the huge costs associated with the implementation of advanced technologies.
- Cloud provides the architecture.
- Enhanced scalability and quite flexible.
- Dynamic workloads are supported.

Disadvantages of IaaS

- Security issues are there.
- Service and Network delays are quite a issue in IaaS.

2. Platform As A Service (PaaS)

Platform as a Service (PaaS) offers the run time environment for applications. In layman's language, It also offers development & deployment tools, required to develop applications. PaaS has a feature of point-and-click tools that enables non-developers to create web applications.

The Salesforce platform used by developers and admins to build applications is an example of PaaS.

Characteristics

- PaaS offers a browser-based development environment. It allows the developer to create a database and edit the application code either via Application Programming Interface or point-and-click tools.
- PaaS provides built-in security, scalability, and web service interfaces.
- PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

Advantages of PaaS –

- Programmers need not worry about what specific database or language the application has been programmed in.
- It offers developers the to build applications without the overhead of the underlying operating system or infrastructure.
- Provides the freedom to developers to focus on the application's design while the platform takes care of the language and the database.
- It is flexible and portable.
- It is quite affordable.
- It manages application development phases in the cloud very efficiently.

Disadvantages of PaaS

- Data is not secure and is at big risk.
- As data is stored both in local storage and cloud, there are high chances of data mismatch while integrating the data.

3. Software As A Service (SaaS)

Software as a Service (SaaS) makes the software available over the internet. This model allows software applications to be provided as a service to end users. It refers to software that is deployed on a hosted service and accessible via the Internet.

There are several SaaS applications, such as billing and invoicing systems, customer relationship management (CRM) applications, help desk applications, and human resource (HR) solutions.

Characteristics

- Available on demand.
- The Software is maintained by the vendor rather than where they are running and hence making it cost-effective.
- The license to the software may be subscription-based or usage-based. And it is billed on a recurring basis.
- Scaled up or down on demand.

- Automatically upgraded and updated.
- SaaS offers a shared data model.
- All users can run the same version of the software.

Advantages of SaaS

- It is a cloud computing service category providing a wide range of hosted capabilities and services. These can be used to build and deploy web-based software applications.
- It provides a lower cost of ownership than on-premises software. The reason is it does not require the purchase or installation of hardware or licenses.
- It can be easily accessed through a browser along a thin client.
- No cost is required for initial setup.
- Low maintenance costs.
- Installation time is less, so time is managed properly.

Disadvantages of SaaS

- Low performance.
- It has limited customization options.
- It has security and data concerns.

Anything As A Service (XaaS)

Anything-as-a-Service (XaaS) is yet another service model, which includes Network-as-a-Service, Business-as-a-Service, Identity-as-a-Service, Database-as-a-Service, and Strategy-as-a-Service.

Difference Between IaaS, PaaS, and SaaS

Basis Of	IAAS	PAAS	SAAS
Stands for	Infrastructure as a service.	Platform as a service.	Software as a service.
Uses	IAAS is used by network architects.	PAAS is used by developers.	SAAS is used by the end user.
Access	IAAS gives access to the resources like virtual machines and virtual storage.	PAAS gives access to run time environment to deployment and development tools for application.	SAAS gives access to the end user.
Model	It is a service model	It is a cloud computing	It is a service model in

Basis Of	IAAS	PAAS	SAAS
	that provides virtualized computing resources over the internet.	model that delivers tools that are used for the development of applications.	cloud computing that hosts software to make it available to clients.
Technical understanding.	It requires technical knowledge.	Some knowledge is required for the basic setup.	There is no requirement about technicalities company handles everything.
Popularity	It is popular among developers and researchers.	It is popular among developers who focus on the development of apps and scripts.	It is popular among consumers and companies, such as file sharing, email, and networking.
Percentage rise	It has around a 12% increment.	It has around 32% increment.	It has about a 27 % rise in the cloud computing model.
Usage	Used by the skilled developer to develop unique applications.	Used by mid-level developers to build applications.	Used among the users of entertainment.
Cloud services.	Amazon Web Services, sun, vCloud Express.	Facebook, and Google search engine.	MS Office web, Facebook and Google Apps.
Enterprise services.	AWS virtual private cloud.	Microsoft Azure.	IBM cloud analysis.
Outsourced cloud services.	Salesforce	Force.com, Gigaspaces.	AWS, Terremark
User Controls	Operating System, Runtime, Middleware, and Application data	Data of the application	Nothing
Others	It is highly scalable and flexible.	It is highly scalable to suit the different businesses according to resources.	It is highly scalable to suit the small, mid and enterprise level business

Cloud Deployment Models

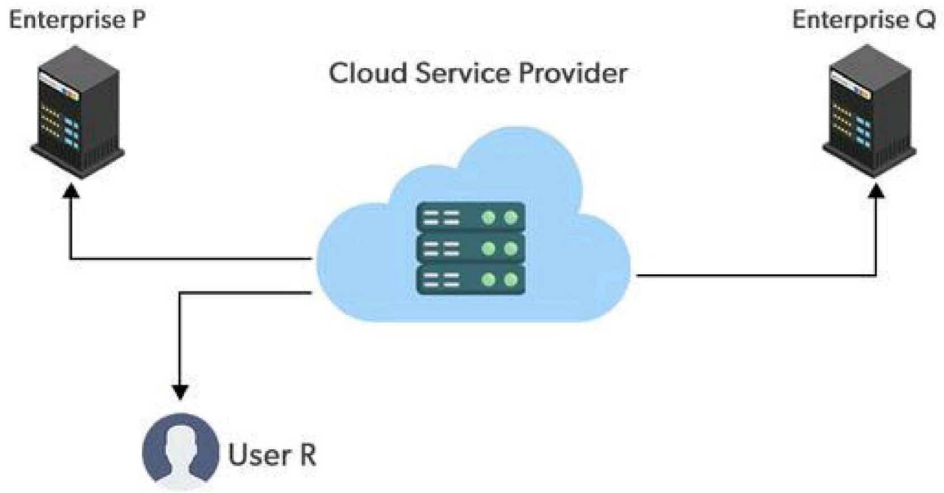
Cloud Deployment means utilization of cloud environment to run the applications through the use of different cloud models such as SaaS,PaaS and IaaS.
Cloud Deployment Model functions as a virtual computing environment with a deployment architecture that varies depending on the amount of data you want to store and who has access to the infrastructure.

Types of Cloud Computing Deployment Models

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose. The location of the servers you're utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types. Different types of cloud computing deployment models are described below.

Public Cloud

The public cloud makes it possible for anybody to access systems and services. The public cloud may be less secure as it is open to everyone. The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer. It is a type of cloud hosting that allows customers and users to easily access systems and services. This form of cloud computing is an excellent example of cloud hosting, in which service providers supply services to a variety of customers. In this arrangement, storage backup and retrieval services are given for free, as a subscription, or on a per-user basis. For example, Google App Engine etc.



Advantages of the Public Cloud Model

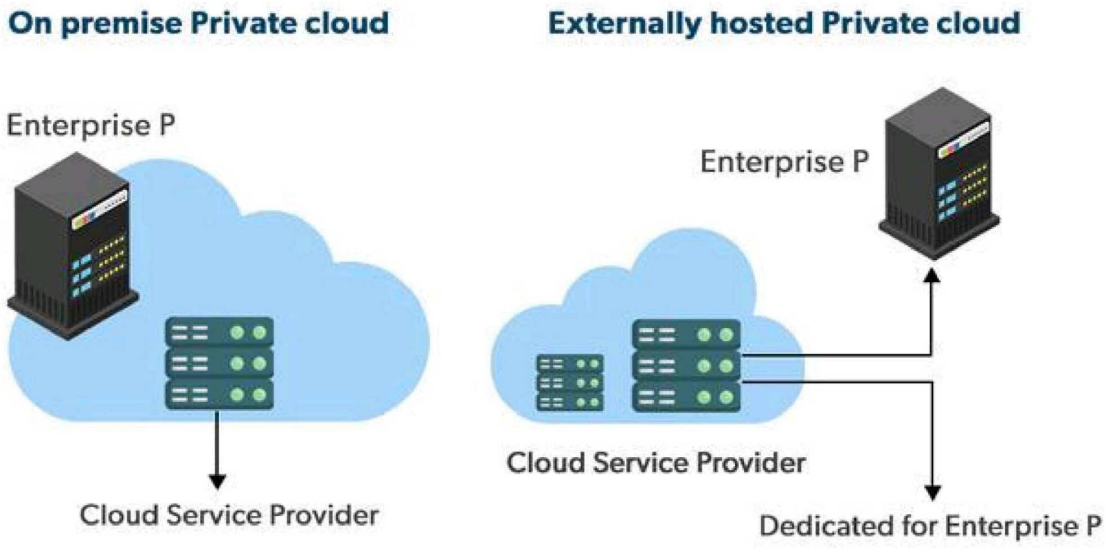
- **Minimal Investment:** Because it is a pay-per-use service, there is no substantial upfront fee, making it excellent for enterprises that require immediate access to resources.
- **No setup cost:** The entire infrastructure is fully subsidized by the cloud service providers, thus there is no need to set up any hardware.
- **Infrastructure Management is not required:** Using the public cloud does not necessitate infrastructure management.
- **No maintenance:** The maintenance work is done by the service provider (not users).
- **Dynamic Scalability:** To fulfill your company's needs, on-demand resources are accessible.

Disadvantages of the Public Cloud Model

- **Less secure:** Public cloud is less secure as resources are public so there is no guarantee of high-level security.
- **Low customization:** It is accessed by many public so it can't be customized according to personal requirements.

Private Cloud

The private cloud deployment model is the exact opposite of the public cloud deployment model. It's a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else. The distinction between private and public clouds is in how you handle all of the hardware. It is also called the "internal cloud" & it refers to the ability to access systems and services within a given border or organization. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization's IT department. The private cloud gives greater flexibility of control over cloud resources.



Advantages of the Private Cloud Model

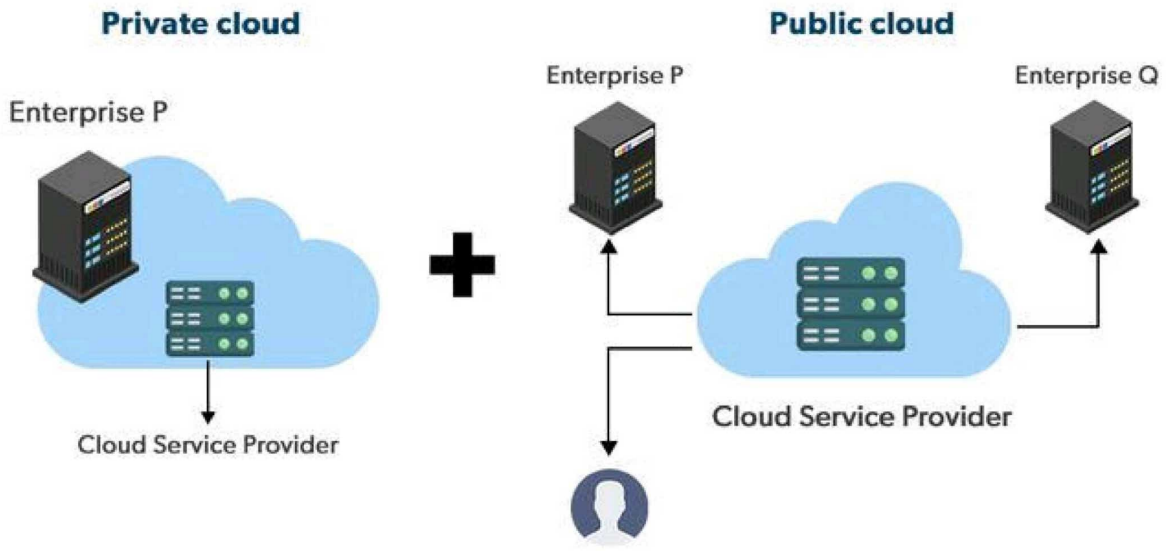
- **Better Control:** You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behavior.
- **Data Security and Privacy:** It's suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.
- **Supports Legacy Systems:** This approach is designed to work with legacy systems that are unable to access the public cloud.
- **Customization:** Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

Disadvantages of the Private Cloud Model

- **Less scalable:** Private clouds are scaled within a certain range as there is less number of clients.
- **Costly:** Private clouds are more costly as they provide personalized facilities.

Hybrid Cloud

By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds. With a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud's cost savings. Organizations can move data and applications between different clouds using a combination of two or more cloud deployment methods, depending on their needs.



Advantages of the Hybrid Cloud Model

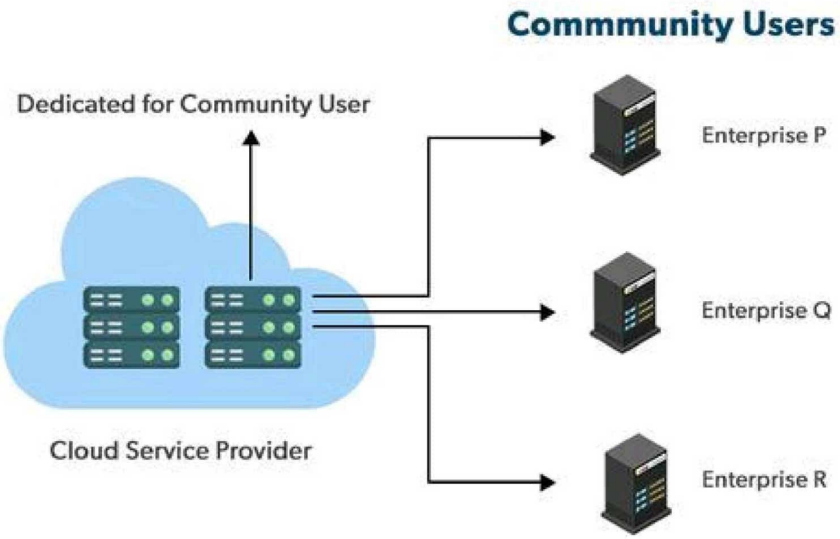
- **Flexibility and control:** Businesses with more flexibility can design personalized solutions that meet their particular needs.
- **Cost:** Because public clouds provide scalability, you'll only be responsible for paying for the extra capacity if you require it.
- **Security:** Because data is properly separated, the chances of data theft by attackers are considerably reduced.

Disadvantages of the Hybrid Cloud Model

- **Difficult to manage:** Hybrid clouds are difficult to manage as it is a combination of both public and private cloud. So, it is complex.
- **Slow data transmission:** Data transmission in the hybrid cloud takes place through the public cloud so latency occurs.

Community Cloud

It allows systems and services to be accessible by a group of organizations. It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business. The infrastructure of the community could be shared between the organization which has shared concerns or tasks. It is generally managed by a third party or by the combination of one or more organizations in the community.



Advantages of the Community Cloud Model

- **Cost Effective:** It is cost-effective because the cloud is shared by multiple organizations or communities.
- **Security:** Community cloud provides better security.

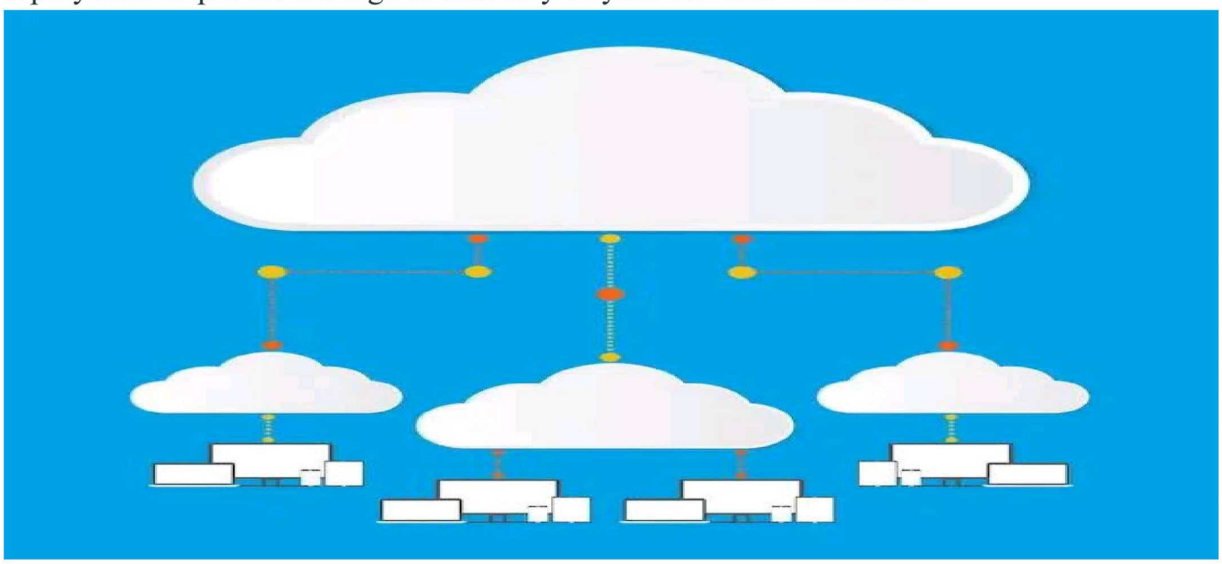
- **Shared resources:** It allows you to share resources, infrastructure, etc. with multiple organizations.
- **Collaboration and data sharing:** It is suitable for both collaboration and data sharing.

Disadvantages of the Community Cloud Model

- **Limited Scalability:** Community cloud is relatively less scalable as many organizations share the same resources according to their collaborative interests.
- **Rigid in customization:** As the data and resources are shared among different organizations according to their mutual interests if an organization wants some changes according to their needs they cannot do so because it will have an impact on other organizations.

Multi-Cloud

We're talking about employing multiple cloud providers at the same time under this paradigm, as the name implies. It's similar to the hybrid cloud deployment approach, which combines public and private cloud resources. Instead of merging private and public clouds, multi-cloud uses many public clouds. Although public cloud providers provide numerous tools to improve the reliability of their services, mishaps still occur. It's quite rare that two distinct clouds would have an incident at the same moment. As a result, multi-cloud deployment improves the high availability of your services even more.



Advantages of the Multi-Cloud Model

- You can mix and match the best features of each cloud provider's services to suit the demands of your apps, workloads, and business by choosing different cloud providers.
- **Reduced Latency:** To reduce latency and improve user experience, you can choose cloud regions and zones that are close to your clients.

- **High availability of service:** It's quite rare that two distinct clouds would have an incident at the same moment. So, the multi-cloud deployment improves the high availability of your services.

Disadvantages of the Multi-Cloud Model

- **Complex:** The combination of many clouds makes the system complex and bottlenecks may occur.
- **Security issue:** Due to the complex structure, there may be loopholes to which a hacker can take advantage hence, makes the data insecure.

Cloud Computing Architecture

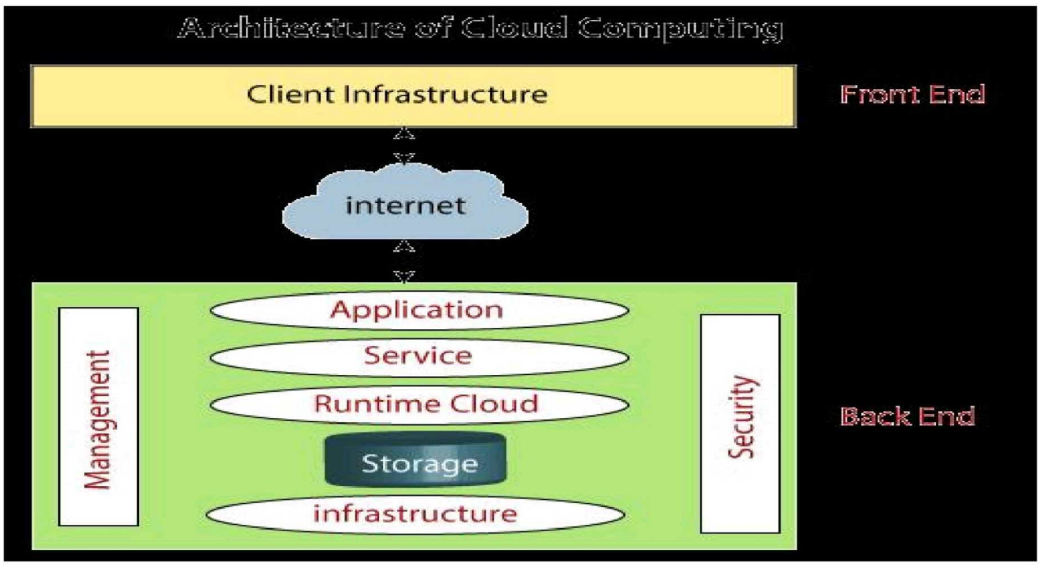
As we know, cloud computing technology is used by both small and large organizations to **store the information** in cloud and **access** it from anywhere at anytime using the internet connection.

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.

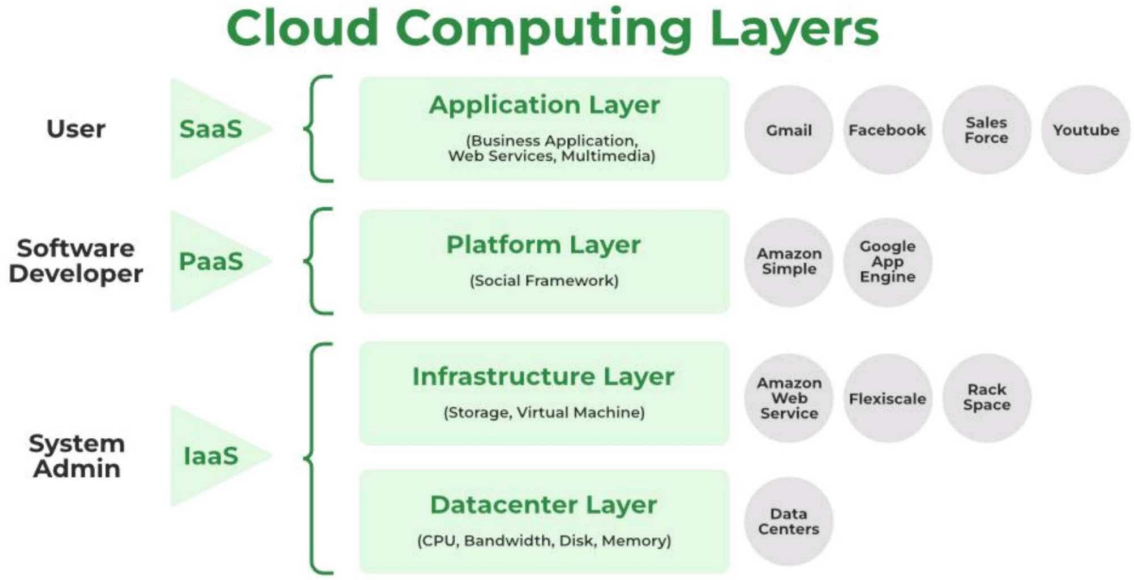
8. Security

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.

Layered Architecture of Cloud



Application Layer

1. The application layer, which is at the top of the stack, is where the actual cloud apps are located. Cloud applications, as opposed to traditional applications, can take advantage of the **automatic-scaling** functionality to gain greater performance, availability, and lower operational costs.
2. This layer consists of different Cloud Services which are used by cloud users. Users can access these applications according to their needs. Applications are divided into **Execution layers** and **Application layers**.
3. In order for an application to transfer data, the application layer determines whether communication partners are available. Whether enough cloud resources are accessible for the required communication is decided at the application layer. Applications must cooperate in order to communicate, and an application layer is in charge of this.
4. The application layer, in particular, is responsible for processing IP traffic handling protocols like Telnet and FTP. Other examples of application layer systems include web browsers, SNMP protocols, HTTP protocols, or HTTPS, which is HTTP's successor protocol.

Platform Layer

1. The operating system and application software make up this layer.
2. Users should be able to rely on the platform to provide them with **Scalability, Dependability, and Security Protection** which gives users a space to create their apps, test operational processes, and keep track of execution outcomes and performance. SaaS application implementation's application layer foundation.
3. The objective of this layer is to deploy applications directly on virtual machines.

4. Operating systems and application frameworks make up the platform layer, which is built on top of the infrastructure layer. The platform layer's goal is to lessen the difficulty of deploying programmers directly into VM containers.
5. By way of illustration, Google App Engine functions at the platform layer to provide API support for implementing storage, databases, and business logic of ordinary web apps.

Infrastructure Layer

1. It is a layer of virtualization where physical resources are divided into a collection of virtual resources using virtualization technologies like Xen, KVM, and VMware.
2. **This layer serves as the Central Hub of the Cloud Environment**, where resources are constantly added utilizing a variety of virtualization techniques.
3. A base upon which to create the platform layer. constructed using the virtualized network, storage, and computing resources. Give users the flexibility they want.
4. Automated resource provisioning is made possible by virtualization**,** which also improves infrastructure management.
5. The infrastructure layer sometimes referred to as the virtualization layer, partitions the physical resources using virtualization technologies like **Xen, KVM, Hyper-V, and VMware** to create a pool of compute and storage resources.
6. The infrastructure layer is crucial to cloud computing since virtualization technologies are the only ones that can provide many vital capabilities, like dynamic resource assignment.

Datacenter Layer

- In a cloud environment, this layer is responsible for **Managing Physical Resources** such as servers, switches, routers, power supplies, and cooling systems.
- Providing end users with services requires all resources to be available and managed in data centers.
- Physical servers connect through high-speed devices such as routers and switches to the data center.
- In software application designs, the division of business logic from the persistent data it manipulates is well-established. This is due to the fact that the same data cannot be incorporated into a single application because it can be used in numerous ways to support numerous use cases. The requirement for this data to become a service has arisen with the introduction of microservices.
- A single database used by many microservices creates a very close coupling. As a result, it is hard to deploy new or emerging services separately if such services need database modifications that may have an impact on other services. A data layer containing many databases, each serving a single microservice or perhaps a few closely related microservices, is needed to break complex service interdependencies.

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.

What is the 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.**

Features of virtualization

Resource isolation

Isolated virtual machines are a result of virtualization. Every virtual machine is capable of having multiple guest users in the form of devices, applications, operating systems or other entities. Since virtual machines offer isolated virtual environments to guest users, their sensitive information is secured. However, these isolated environments do not keep guest users from being interconnected with one another.

Virtualization also enables performance tuning. This involves tuning the properties of the resources in the virtual environment to adjust the performance of a guest.

Emulation

The virtualization layer controls the environment in which guest programs are executed. Additionally, guest programs that need specific features that may be missing in a physical host can also be executed in an environment that emulates the host.

Portability

The guest can be stored in a virtual image and can be moved and run on top of different virtual machines in the context of hardware virtualization. The binary code that represents application components is executable without having to recompile on any implementation of the corresponding virtual machine in virtualization on a programming level.

Security

The power to transparently regulate how guest programs execute makes it possible to deliver a secure and controlled execution environment. Managing a virtual machine provides the ability to not only control but also filter the activities of guest programs. This makes it possible to avert harmful operations from being executed.

Benefits of Virtualization

- More flexible and efficient allocation of resources.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.

- Remote access and rapid scalability.
- High availability and disaster recovery.
- Pay peruse of the IT infrastructure on demand.
- Enables running multiple operating systems.

Drawback of Virtualization

- **High Initial Investment:** Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
- **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
- **Risk of Data:** Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.

Types of Virtualization:

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

1) 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.

2) 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.

3) 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.

4) 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.

5). Application Virtualization:

Application virtualization helps a user to have remote access to 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. An 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.

How does virtualization work in cloud computing?

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.

What is Paravirtualization?

Paravirtualization is a computer hardware virtualization technique that allows virtual machines (VMs) to have an interface similar to that of the underlying or host hardware. This technique aims to improve the VM's performance by modifying the guest operating system (OS).

With paravirtualization, the guest OS is modified, so it knows that it is running in a virtualized environment on top of a hypervisor (the hardware running the VM) and not on the physical hardware.

Xen is an open source hypervisor based on paravirtualization. It is the most popular application of paravirtualization. Xen has been extended to compatible with full virtualization using hardware-assisted virtualization. It enables high performance to execute guest operating system. This is probably done by removing the performance loss while executing the instructions requiring significant handling and by modifying portion of the guest operating system executed by Xen, with reference to the execution of such instructions. Hence this especially support x86, which is the most used architecture on commodity machines and servers.

VMware: Full Virtualization

In full virtualization primary hardware is replicated and made available to the guest operating system, which executes unaware of such abstraction and no requirements to modify. Technology of VMware is based on the key concept of Full Virtualization. Either in desktop environment, with the help of type-II hypervisor, or in server environment, through type-I hypervisor, VMware implements full virtualization. In both the cases, full virtualization is possible through the direct execution for non-sensitive instructions and binary translation for sensitive instructions or hardware traps, thus enabling the virtualization of architecture like x86.

Microsoft Hyper-V

Virtualization can be used for different purposes. Cloud computing and container technology work with it, for example. Fortunately, as a user of Windows you won't be dependent on external - and sometimes very complex - software. With Hyper-V, Windows has installed its own hypervisor. So what does the tool do?

What is Hyper-V?

To virtualize hardware, i.e. create a hardware environment that does not have a physical form, you need an intermediary between the physical computer and the virtual machine. This interface is called a **hypervisor**. The physical host system can be mapped to **multiple virtual guest systems** (child partitions) that share the host hardware (parent partition). Microsoft has created its own hypervisor, Hyper-V, which is included in the professional versions of Windows 10 or Windows 8. The software is also installed in Windows Server.

Hyper-V gives Windows users the ability to start their **own virtual machine**. In this virtual machine, a complete hardware infrastructure with RAM, hard disk space, processor power, and other components can be virtualized. A **separate operating system** runs on this basis, which does not necessarily have to be Windows. It is very popular, for example, to run an open-source distribution of Linux in a virtual machine.

What do you need Hyper-V for?

Virtualization technology can be used in different situations for different needs. Hyper-V is usually used in test environments. In this context, virtualization has two advantages:

1. Computer environments which are otherwise not accessible **can be accessed**. For example, instead of setting up your own PC with Linux, you can easily display the Linux operating system in a virtual machine.
2. The virtual machine is **self-contained**. This means that if you run software that causes a system crash, the physical device is not at risk. Only the virtual machine would need to be reset.

Private users can use Hyper-V, for example, if they want to use software that would not run under their current version of Windows - either because the program requires an older version of the operating system or because only Linux is supported.

Virtualization via Hyper-V is a great advantage for software developers in particular. Any program they create can be tested under a huge variety of software and hardware conditions. In addition, due to the self-contained nature of the virtual machines, there is no need to worry about **faulty code** causing damage to their own systems.