Cloud

A *cloud* refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. The term originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources.

The technology of distributed data processing in which some scalable information , resources and capacities are provided as a service to multiple external customers through internet. As a specific environment used to remotely provision IT resources, a cloud has a finite boundary. There are many individual clouds that are accessible via the Internet.

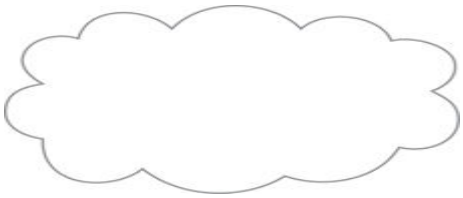


Figure - The symbol used to denote the boundary of a cloud environment.

Cloud Computing

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations.

Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available.

Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

"Cloud computing is a specialized form of distributed computing that introduces utilization models for remotely provisioning scalable and measured resources."

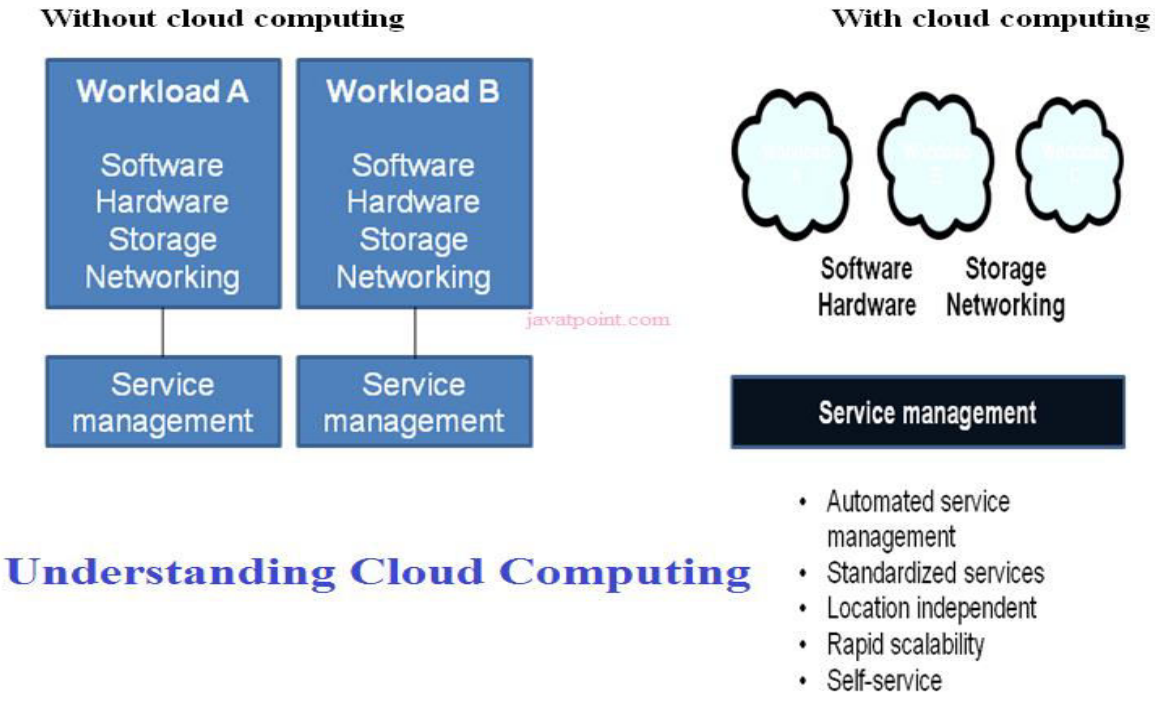
Cloud computing means *on demand delivery of IT resources* via the internet with pay-as-you-go pricing. It provides a solution of IT infrastructure in low cost.

Why Cloud Computing?

Actually, Small as well as some large IT companies follows the traditional methods to provide the IT infrastructure. That means **for any IT company, we need a Server Room that is the basic need of IT companies**.

In that server room, there should be a *database server*, *mail server*, *networking*, *firewalls*, *routers*, *modem*, *switches*, *QPS*(Query Per Second means how much queries or load will be handled by the server) , configurable system, *high net speed* and the *maintainability* of the internet.

To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence.



Characteristics of Cloud Computing

The characteristics of cloud computing are given below:

1) Agility

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

2) High availability and reliability

Availability of servers is high and more reliable, because **chances of infrastructure failure are minimal**.

3) High Scalability

Means **"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 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**.

CLOUD STORAGE:

Cloud storage is defined as "*the storage of data online in the cloud*," wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Cloud storage is a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet).

Users generally pay for their cloud data storage on a per-consumption, monthly rate. Although the per-gigabyte cost has been radically driven down, cloud storage providers have added operating expenses that can make the technology more expensive than users bargained for.

Cloud security continues to be a concern among users. Providers have tried to deal with those fears by building security capabilities, such as encryption and authentication, into their services.

Cloud storage can provide the benefits of

- greater accessibility and reliability;
- rapid deployment;
- strong protection for data backup,archival and
- disaster recovery purposes; and
- lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware.

There are many benefits of using cloud storage, however, cloud storage does have the potential for security and compliance concerns that are not associated with traditional storage systems.

Benefits of Cloud Storage

Storing data in the cloud lets IT departments transform three areas:

1. **Total Cost of Ownership**. With cloud storage, there is no hardware to purchase, storage to provision, or capital being used for "someday" scenarios. You can add or remove capacity on demand, quickly change performance and retention characteristics, and only pay for storage that you actually use. Less frequently accessed data can even be automatically moved to lower cost tiers in accordance with auditable rules, driving economies of scale.

2. **Time to Deployment.** When development teams are ready to execute, infrastructure should never slow them down. Cloud storage allows IT to quickly deliver the exact amount of storage needed, right when it's needed. This allows IT to focus on solving complex application problems instead of having to manage storage systems.

3. **Information Management.** Centralizing storage in the cloud creates a tremendous leverage point for new use cases. By using cloud storage lifecycle management policies, you can perform powerful information management tasks including automated tiering or locking down data in support of compliance requirements.

4. **File accessibility**. Files stored in the cloud can be accessed at any time from any place so long as you have Internet access. Files stored in the cloud can be accessed at any time from any place so long as you have Internet access.

5**.Off-site (remote) backups** of data which reduces costs associated with disaster recovery .

Disadvantages of Cloud Storage

Unfortunately, the biggest disadvantage to cloud storage is that users are **limited by bandwidth**. If your Internet connection is slow or unstable, you might have problems accessing or sharing your files.

Organizations that require a large amount of storage may also find costs increase significantly after the first few gigabytes of data stored.

TYPES OF CLOUD STORAGE

Personal Cloud Storage

Also known as mobile cloud storage, personal cloud storage is a subset of public cloud storage that applies to storing an individual's data in the cloud and providing the individual with access to the data from anywhere. It also provides data syncing and sharing capabilities across multiple devices. Apple's iCloud is an example of personal cloud storage.

Public Cloud Storage

Public cloud storage is where the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data center. The cloud storage provider fully manages the enterprise's public cloud storage.

Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure.

Generally, public cloud providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access over the Internet.

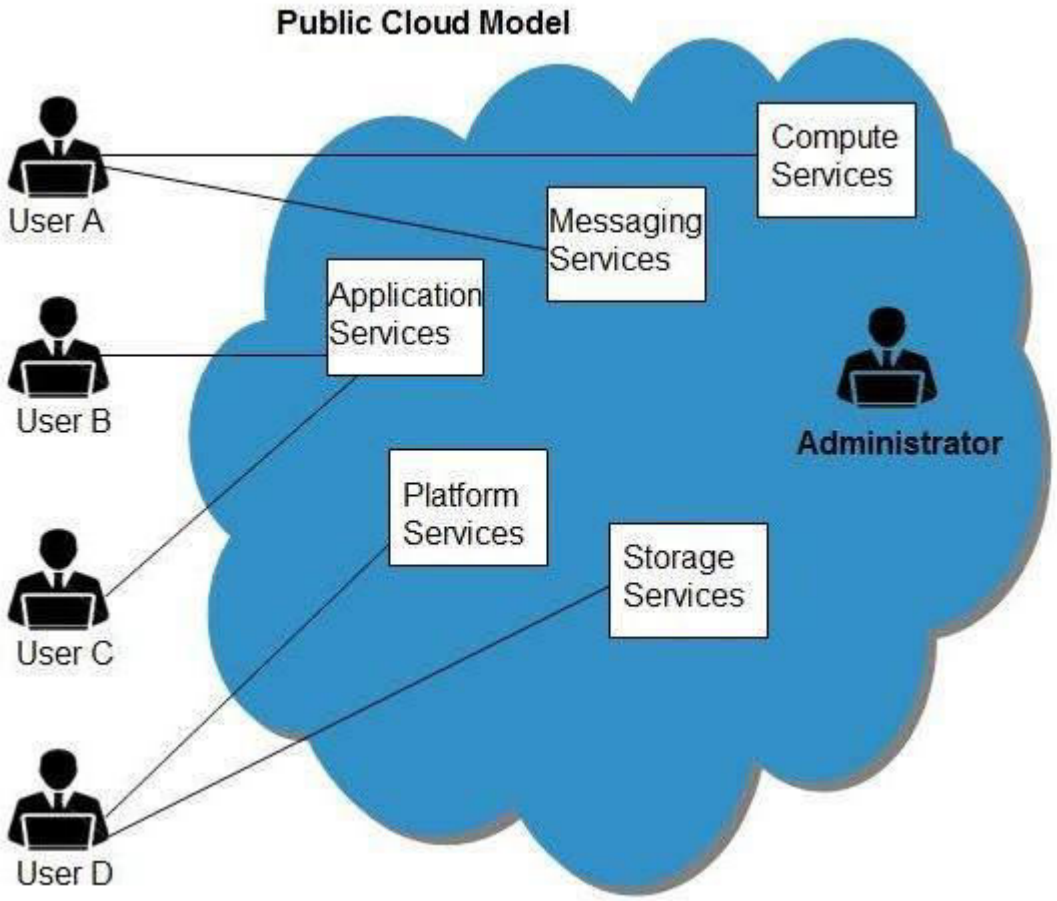
A public cloud is the obvious choice when:

o Your standardized workload for applications is used by lots of people, such as email. o You need to test and develop application code.

o You need incremental capacity (the ability to add compute resources for peak times).

o You're doing collaboration projects.

The Public Cloud Model is shown in the diagram below.



Benefits

There are many benefits of deploying cloud as public cloud model. The following diagram shows some of those benefits:

Cost Effective

Since **public cloud** shares same resources with large number of customers it turns out inexpensive.

Reliability

The **public cloud** employs large number of resources from different locations. If any of the resources fails, public cloud can employ another one.

Flexibility

The public cloud can smoothly integrate with private cloud, which gives customers a flexible approach.

Location Independence

Public cloud services are delivered through Internet, ensuring location independence.

Utility Style Costing

Public cloud is also based on **pay-per-use** model and resources are accessible whenever customer needs them.

High Scalability

Cloud resources are made available on demand from a pool of resources, i.e., they can be scaled up or down according the requirement.

Disadvantages

Here are some disadvantages of public cloud model:

Low Security

In **public cloud model,** data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.

Less Customizable

It is comparatively less customizable than private cloud.

Private Cloud Storage

A form of cloud storage where the enterprise and cloud storage provider are integrated in the enterprise's data center. In private cloud storage, the storage provider has infrastructure in the enterprise's data center that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally.

There are two variations of private clouds:

o On-Premise Private Cloud: This type of cloud is hosted within an organization's own facility. A businesses IT department would incur the capital and operational costs for the physical resources with this model. On-Premise Private Clouds are best used for applications that require complete control and configurability of the infrastructure and security.

o Externally Hosted Private Cloud: Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources.

Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and it will require the organization to reevaluate decisions about existing resources. Private clouds are more expensive but also more secure when compared to public clouds. An Info-Tech survey shows that 76% of IT decision-makers will focus exclusively on the private cloud, as these clouds offer the greatest level of security and control.

When is a Private Cloud for you?

o You need data sovereignty but want cloud efficiencies

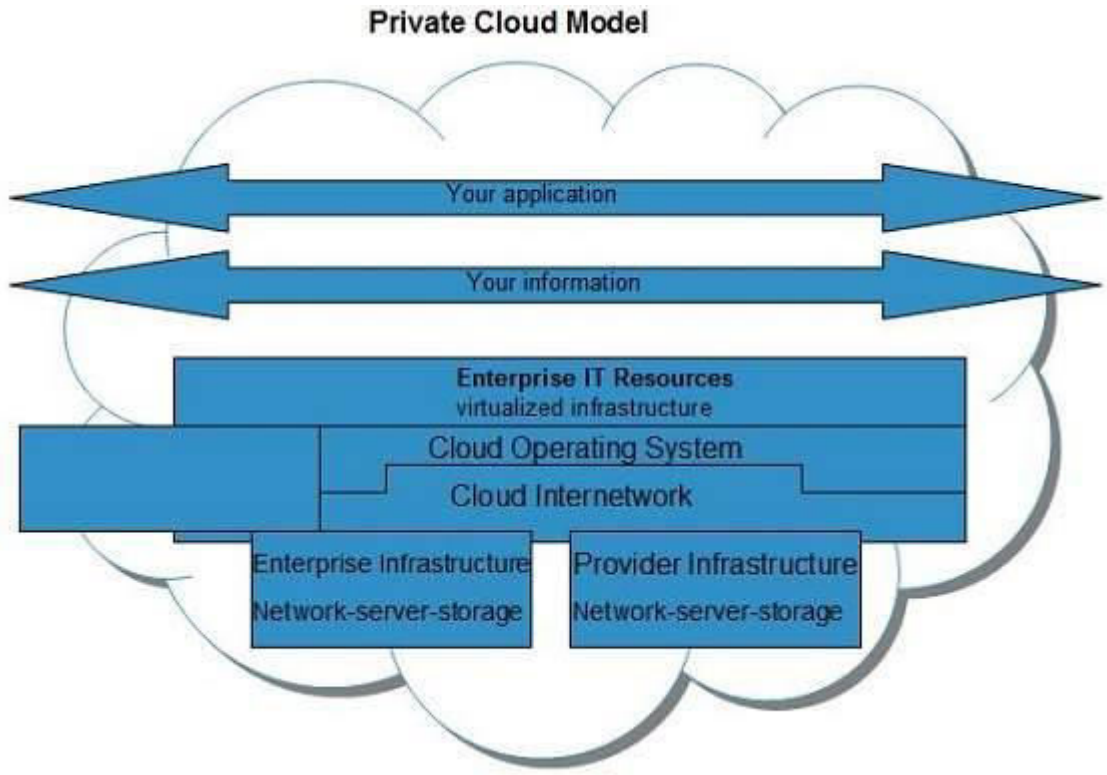
o You want consistency across services

o You have more server capacity than your organization can use

o Your data center must become more efficient

o You want to provide private cloud services

The private cloud model is shown in the diagram below.



Benefits

There are many benefits of deploying cloud as private cloud model. The following diagram shows some of those benefits:

High Security and Privacy

Private cloud operations are not available to general public and resources are shared from distinct pool of resources. Therefore, it ensures high **security** and **privacy.**

More Control

The **private cloud** has more control on its resources and hardware than public cloud because it is accessed only within an organization.

Energy Efficiency

The **private cloud** resources are not as cost effective as resources in public clouds but they offer more efficiency than public cloud resources.

Disadvantages

Here are the disadvantages of using private cloud model:

Restricted Area of Operation

The private cloud is only accessible locally and is very difficult to deploy globally.

High Priced

Purchasing new hardware in order to fulfill the demand is a costly transaction.

Limited Scalability

The private cloud can be scaled only within capacity of internal hosted resources.

Additional Skills

In order to maintain cloud deployment, organization requires skilled expertise.

Hybrid Cloud Storage

Hybrid cloud storage is a combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

Hybrid Clouds are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, you can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. Hybrid cloud architecture requires both on-premise resources and off-site server based cloud infrastructure. By spreading things out over a hybrid cloud, you keep each aspect of your business in the most efficient environment possible. The downside is that you have to keep track of multiple cloud security platforms and ensure that all aspects of your business can communicate with each other.

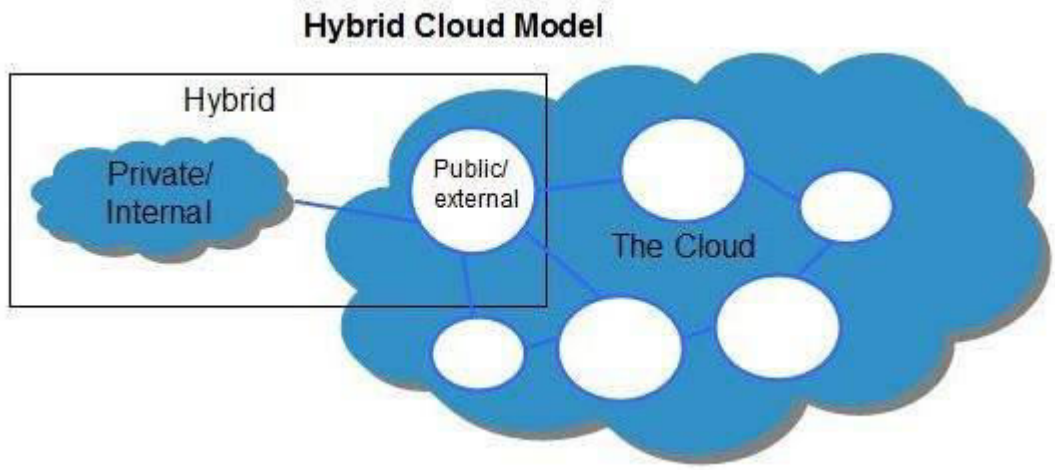
Here are a couple of situations where a hybrid environment is best:

- Your company wants to use a SaaS application but is concerned about security.

o Your company offers services that are tailored for different vertical markets. You can use a public cloud to interact with the clients but keep their data secured within a private cloud.

o You can provide public cloud to your customers while using a private cloud for internal IT.

The Hybrid Cloud Model is shown in the diagram below.



Benefits

There are many benefits of deploying cloud as hybrid cloud model. The following diagram shows some of those benefits:

Scalability

It offers features of both, the public cloud scalability and the private cloud scalability.

Flexibility

It offers secure resources and scalable public resources.

Cost Efficiency

Public clouds are more cost effective than private ones. Therefore, hybrid clouds can be cost saving.

Security

The private cloud in hybrid cloud ensures higher degree of security.

Disadvantages

Networking Issues

Networking becomes complex due to presence of private and public cloud.

Security Compliance

It is necessary to ensure that cloud services are compliant with security policies of the organization.

Infrastructure Dependency

The **hybrid cloud model** is dependent on internal IT infrastructure, therefore it is necessary to ensure redundancy across data centers.

Community Cloud

A community cloud is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider. It may be managed internally by organizations or by the third-party.

Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives.

The goal of community clouds is to have participating organizations realize the benefits of a public cloud with the added level of privacy, security, and policy compliance usually associated with a private cloud. Community clouds can be either on-premise or off-premise.

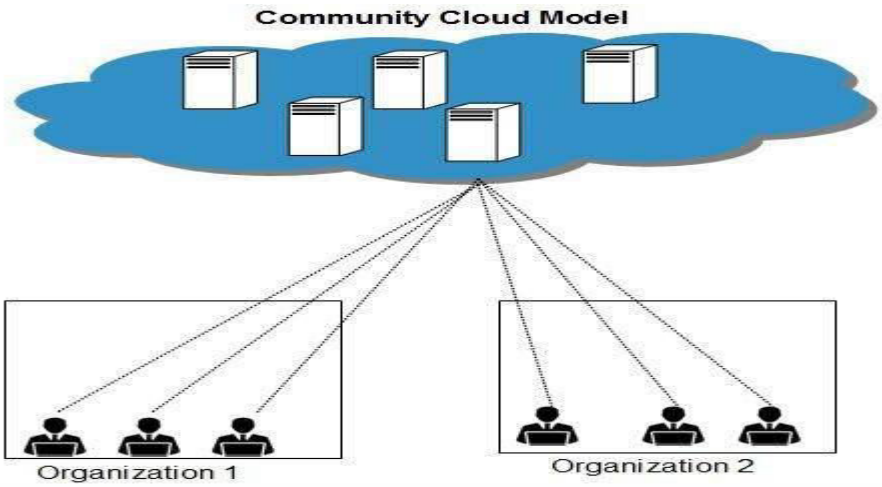
Here are a couple of situations where a community cloud environment is best:

o Government organizations within a state that need to share resoures

o A private HIPAA compliant cloud for a group of hospitals or clinics

o Telco community cloud for telco DR to meet specific FCC regulations

The Community Cloud Model is shown in the diagram below.



Benefits

There are many benefits of deploying cloud as **community cloud model.**

Cost Effective

Community cloud offers same advantages as that of private cloud at low cost.

Sharing Among Organizations

Community cloud provides an infrastructure to share cloud resources and capabilities among several organizations.

Security

The community cloud is comparatively more secure than the public cloud but less secured than the private cloud.

Issues

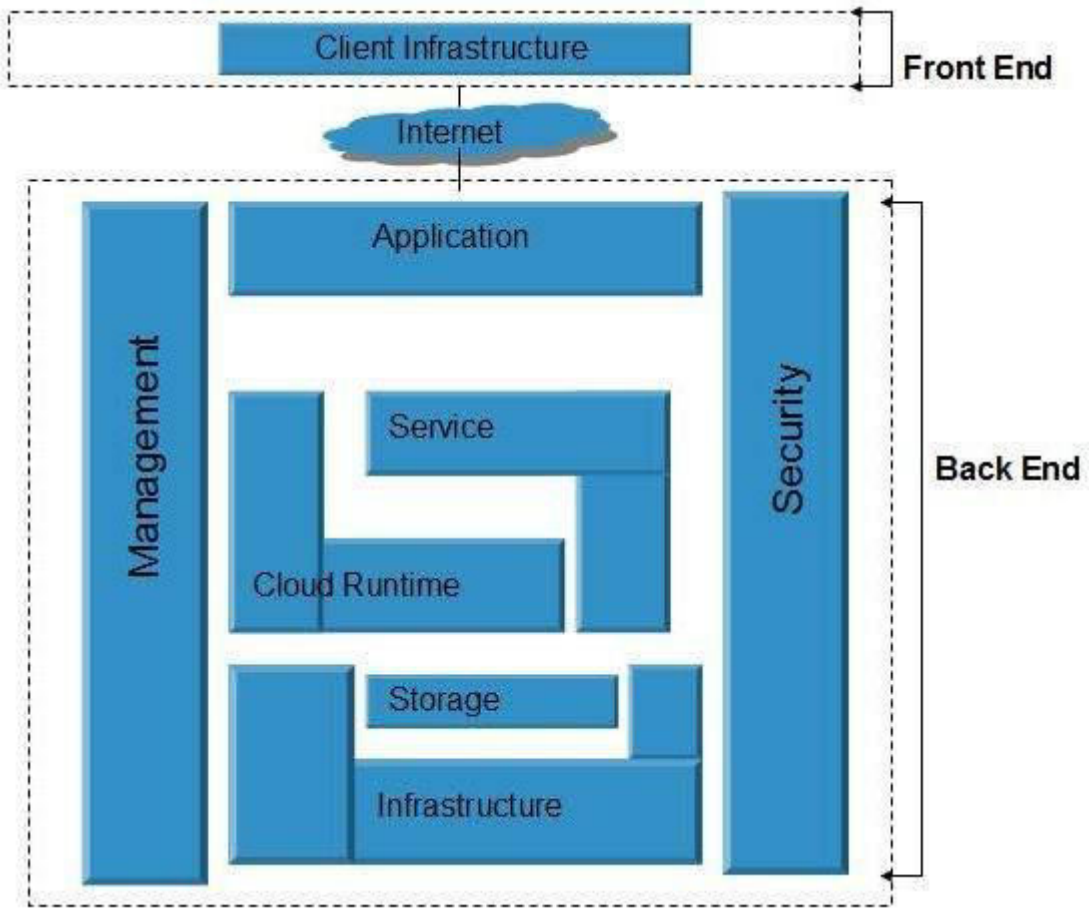
- Since all data is located at one place, one must be careful in storing data in community cloud because it might be accessible to others.
- It is also challenging to allocate responsibilities of governance, security and cost among organizations.

Cloud Computing Architecture

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:



Front End

The **front end** refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End

The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

Note

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.

- The server employs certain protocols known as middleware, which help the connected devices to communicate with each other.

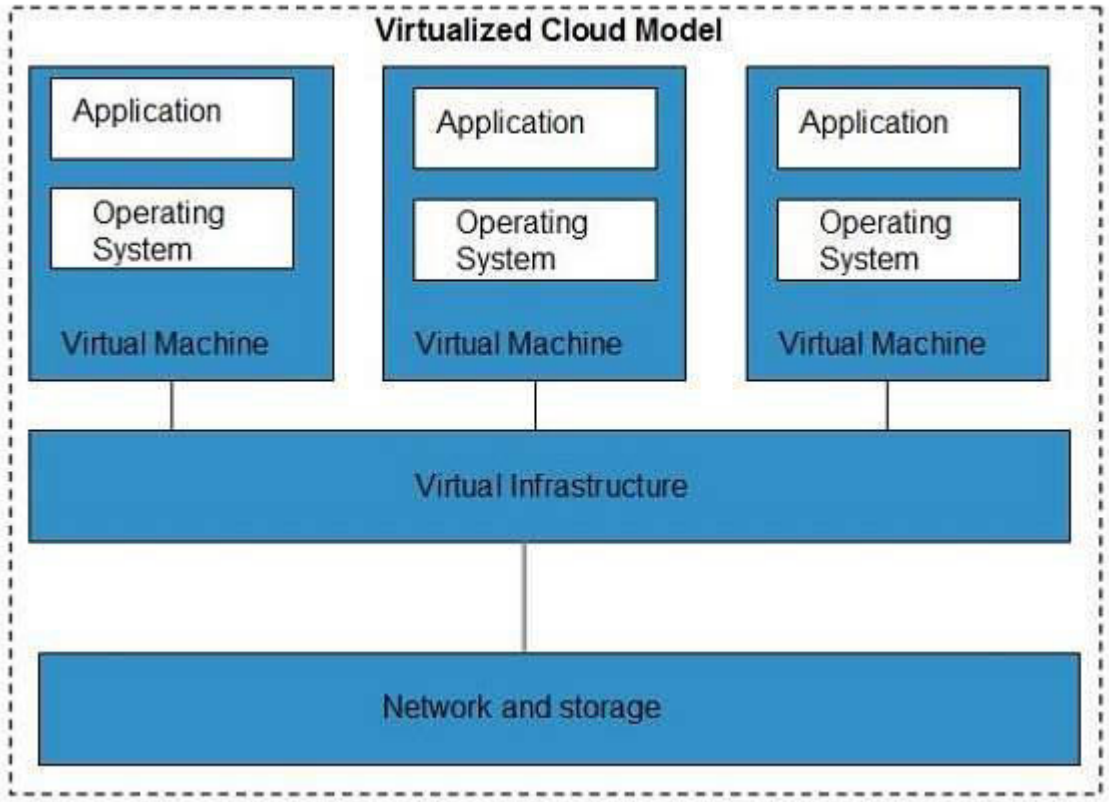
Cloud Computing Technologies

There are certain technologies working behind the cloud computing platforms making cloud computing flexible, reliable, and usable. These technologies are listed below:

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid Computing
- Utility Computing

Virtualization

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



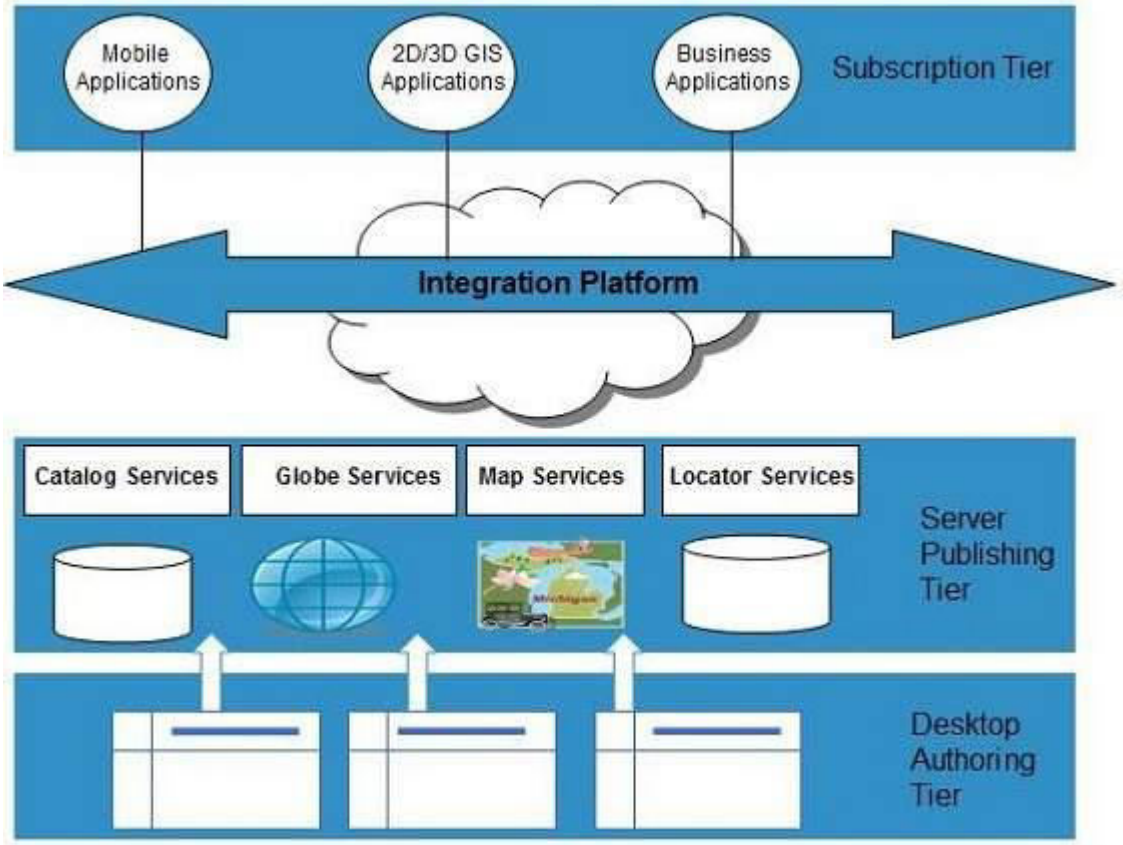
The **Multitenant** architecture offers **virtual isolation** among the multiple tenants. Hence, the organizations can use and customize their application as though they each have their instances running.

Service-Oriented Architecture (SOA)

Service-Oriented Architecture helps to use applications as a service for other applications regardless the type of vendor, product or technology. Therefore, it is possible to exchange

the data between applications of different vendors without additional programming or making changes to services.

The cloud computing service oriented architecture is shown in the diagram below.



Grid Computing

Grid Computing refers to distributed computing, in which a group of computers from multiple locations are connected with each other to achieve a common objective. These computer resources are heterogeneous and geographically dispersed.

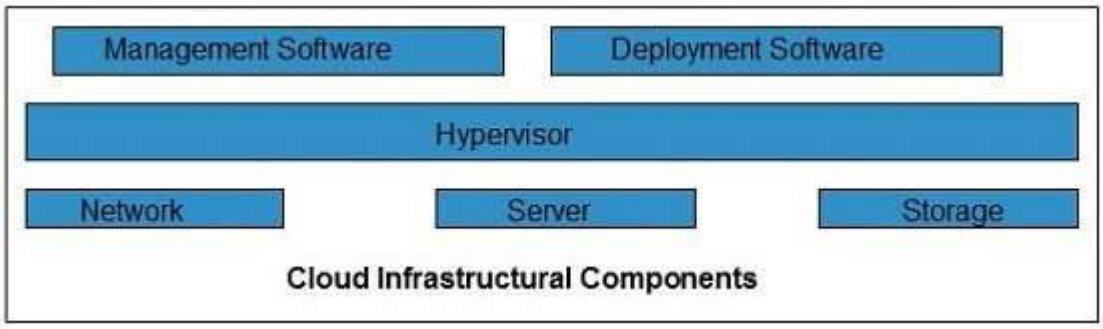
Grid Computing breaks complex task into smaller pieces, which are distributed to CPUs that reside within the grid.

Utility Computing

Utility computing is based on **Pay-per-Use model.** It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of utility computing.

Cloud Computing Infrastructure

Cloud infrastructure consists of servers, storage devices, network, cloud management software, deployment software, and platform virtualization.



Hypervisor

Hypervisor is a **firmware** or **low-level program** that acts as a Virtual Machine Manager. It allows to share the single physical instance of cloud resources between several tenants.

Management Software

It helps to maintain and configure the infrastructure.

Deployment Software

It helps to deploy and integrate the application on the cloud.

Network

It is the key component of cloud infrastructure. It allows to connect cloud services over the Internet. It is also possible to deliver network as a utility over the Internet, which means, the customer can customize the network route and protocol.

Server

The **server** helps to compute the resource sharing and offers other services such as resource allocation and de-allocation, monitoring the resources, providing security etc.

Storage

Cloud keeps multiple replicas of storage. If one of the storage resources fails, then it can be extracted from another one, which makes cloud computing more reliable.

Infrastructural Constraints

Transparency

Virtualization is the key to share resources in cloud environment. But it is not possible to satisfy the demand with single resource or server. Therefore, there must be transparency in resources, load balancing and application, so that we can scale them on demand.

Scalability

Scaling up an application delivery solution is not that easy as scaling up an application because it involves configuration overhead or even re-architecting the network. So, application delivery solution is need to be scalable which will require the virtual infrastructure such that resource can be provisioned and de-provisioned easily.

Intelligent Monitoring

To achieve transparency and scalability, application solution delivery will need to be capable of intelligent monitoring.

Security

The mega data center in the cloud should be securely architected. Also the control node, an entry point in mega data center, also needs to be secure.

Cloud provider

A service provider that offers customers storage or software services available via a private (private cloud) or public network (cloud). Usually, it means the storage and software is available for access via the Internet.

Cloud Computing Infrastructure as a Service (IaaS)

IaaS is one of the layers of cloud computing platform wherein the customer organization outsources its IT infrastructure such as servers, networking, processing, storage, virtual machines and other resources. Customers access these resources over internet i.e. cloud computing platform, on a pay-per-use model.

Iaas, **earlier called Hardware as a Service** (HaaS), is a cloud computing platform based model.

In traditional hosting services, IT infrastructure was rented out for a specific periods of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requires, and are billed only for the services actually used.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

IaaS is offered in three models: public, private, and hybrid cloud. Private cloud implies that the infrastructure resides at the customer-premise. In case of public cloud, it is located at the cloud computing platform vendor's data center; and hybrid cloud is a combination of two with customer choosing the best of both worlds.

Advantages of IaaS cloud computing layer

1) You can dynamically choose a CPU, memory and storage configuration as per your needs.

2) You easily access the vast computing power available on IaaS cloud platform.

3) You can eliminate the need of investment in rarely used IT hardware.

4) IT infra will be handled by the IaaS cloud computing platform vendors.

Disadvantages of IaaS cloud computing layer

1) There is a risk of IaaS cloud computing platform vendor by gaining the access to the organizations data. But it can be avoided by opting for private cloud.

2) IaaS cloud computing platform model is dependent on internet availability.

3) It is also dependent on the availability of virtualization services.

4) IaaS cloud computing platform can limit the user privacy and customization options.

Some pinpoint about IaaS cloud computing layer

IaaS cloud computing platform cannot replace traditional hosting method but it provides more than that and each resources which are used are predictable as per the usage.

IaaS cloud computing platform may not eliminate the need for an in-house IT department. It will be needed to monitor or control the IaaS setup. IT salary expenditure might not reduce significantly, but other IT expenses can be reduced.

Breakdowns at the IaaS cloud computing platform vendor's end can bring your business to at the halt stage. Assess the IaaS cloud computing platform vendor's stability and finances. Make sure that SLAs (i.e. Service Level Agreement) provide backups for data, hardware, network and application failures. Image portability and third-party support is a plus point.

The IaaS cloud computing platform vendor can get access to your sensitive data. So, engage with the credible companies or organizations. Study their security policies and precautions.

Amazon Web Services, Tata Communication

Cloud Computing Platform as a Service (PaaS)

PaaS cloud computing platform is a developer programming platform which *is created for the programmer to develop, test, run and manage the applications*.

A developer is able to write the application as well as deploy it directly into this layer easily.

PaaS extend and abstract the IaaS layer by removing the hassle of managing the individual virtual machine.

In PaaS cloud computing platform, back end scalability is handled by the cloud service provider and the end user does not have to worry about to manage the infrastructure.

All the infrastructure to run the applications will be over the internet.

Advantages of PaaS cloud computing layer

1) Simplified Development

Developers can focus on development and innovation without worrying about the infrastructure.

---

2) Lower risk

No requirements of up-front investment in hardware and software. Developers only need a PC and an internet connection to start building applications.

---

3) Prebuilt business functionality

Some PaaS vendors also provide already defined business functionality so that users can avoid building everything from very scratch and hence can directly start the projects only.

---

4) Instant community

PaaS vendors frequently provides online communities where developer can get the ideas, share experiences and seek advice from others.

---

5) Scalability

Applications deployed can scale from one to thousands of users without any changes to the applications.

Disadvantages of PaaS cloud computing layer

1) Vendor lock-in

One have to write the applications according to the platform provided by PaaS vendor so migration of an application to another PaaS vendor would be a problem.

---

2) Data Privacy

Corporate data, whether it can be critical or not, will be private so if it is not located within the walls of the company there can be a risk in terms of privacy of data.

---

3) Integration with the rest of the systems applications

It may happen that some applications are local and some are in cloud. So there will be chances of increased complexity when we want to use data which in the cloud with the local data.

Top vendors who are providing PaaS cloud computing platform

1. Google Apps Engine (GAE)
2. SalesFroce.com
3. Windows Azure
4. AppFog
5. Openshift
6. Cloud Foundary from VMware

Cloud Computing Software as a Service (SaaS)

SaaS is a software distribution model in which applications are hosted by a cloud service provider and made available to customers over internet. SaaS is also known as **"On-Demand Software"**.

In SaaS, software and associated data are centrally hosted on the cloud server. SaaS is accessed by users using a thin client via a web browser.

Advantages of SaaS cloud computing layer

1) SaaS is easy to buy

SaaS pricing is based on a monthly fee or annual fee, SaaS allows organizations to access business functionality at a low cost which is less than licensed applications.

Unlike traditional software which is sold as a licensed based with an up-front cost (and often an optional ongoing support fee), SaaS providers generally pricing the applications using a subscription fee, most commonly a monthly or annually fee.

---

2) Less hardware required for SaaS

The software is hosted remotely, so organizations don't need to invest in additional hardware.

---

3) Low Maintenance required for SaaS

Software as a service removes the necessity of installation, set-up, and often daily unkeep and maintenance for organizations. Initial set-up cost for SaaS is typically less than the enterprise software. SaaS vendors actually pricing their applications based on some usage parameters, such as number of users using the application. So SaaS does easy to monitor and automatic updates.

---

4) No special software or hardware versions required

All users will have the same version of software and typically access it through the web browser. SaaS reduces IT support costs by outsourcing hardware and software maintenance and support to the IaaS provider.

Disadvantages of SaaS cloud computing layer

1) Security

Actually data is stored in cloud, so security may be an issue for some users. However, cloud computing is not more secure than in-house deployment. Learn more cloud security.

---

2) Latency issue

Because the data and application are stored in cloud at a variable distance from the end user, so there is a possibility that there may be more latency while interacting with the application than a local deployment. So, SaaS model is not suitable for applications whose demand response times are in milliseconds.

---

3) Total Dependency on Internet

Without internet connection, most SaaS applications are not usable.

---

4) Switching between SaaS vendors is difficult

Switching SaaS vendors involves the difficult and slow task of transferring the very large data files over the Internet and then converting and importing them into another SaaS also.

Cloud Computing Security

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

Security Planning

Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:

- Select resource that needs to move to the cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS,** and **SaaS.** These models require customer to be responsible for security at different levels of service.
- Consider the cloud type to be used such as **public, private, community** or **hybrid.**
- Understand the cloud service provider's system about data storage and its transfer into and out of the cloud.

The risk in cloud deployment mainly depends upon the service models and cloud types.

Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.

- Access Control
- Auditing
- Authentication
- Authorization

All of the service models should incorporate security mechanism operating in all above-mentioned areas.

Isolated Access to Data

Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.

Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:

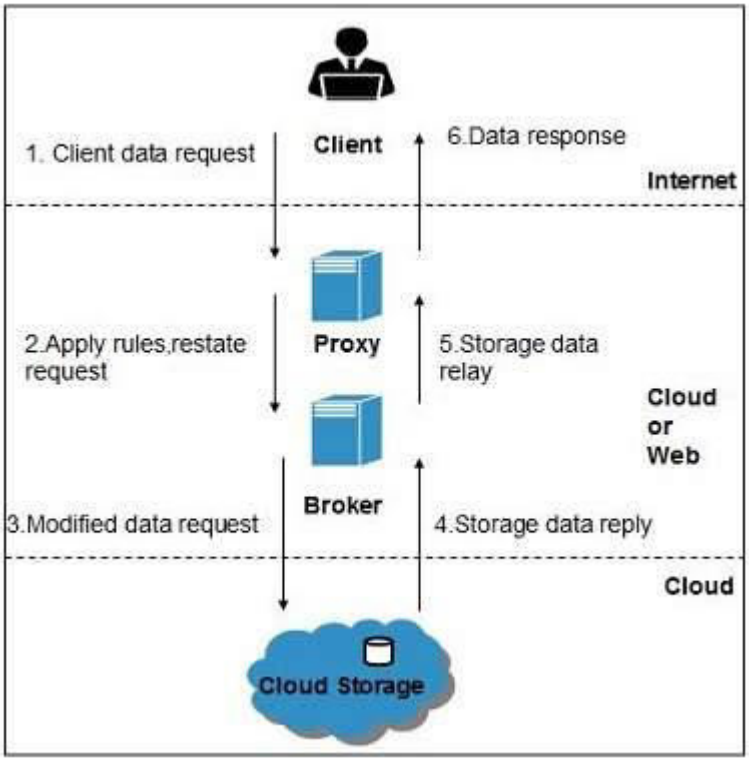
- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

Working Of Brokered Cloud Storage Access System

When the client issues request to access data:

- The client data request goes to the external service interface of proxy.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.

All of the above steps are shown in the following diagram:



Encryption

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

Cloud integration

Cloud integration is the process of configuring multiple application programs to share data in the cloud. In a network that incorporates cloud integration, diverse applications communicate either directly or through third-party software.

Cloud integration offers the following advantages over older, compartmentalized organizational methods.

- Each user can access personal data in real time from any device.
- Each user can access personal data from any location with Internet access.
- Each user can integrate personal data such as calendars and contact lists served by diverse application programs.
- Each user can employ the same logon information (username and password) for all personal applications.
- The system efficiently passes control messages among application programs.

- By avoiding the use of data silos, data integrity is maintained and data conflicts (which can arise from redundancy) are avoided.
- Cloud integration offers scalability to allow for future expansion in terms of the number of users, the number of applications, or both.

In recent years, cloud integration has gained favor among organizations, corporations, and government agencies that implement SaaS (Software as a Service), a software distribution model in which applications are hosted by a vendor or service provider and made available to users over the Internet.

Cloud Computing Challenges

Cloud computing, an emergent technology, has placed many challenges in different aspects of data and information handling.

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.