Cloud Computing Overview

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

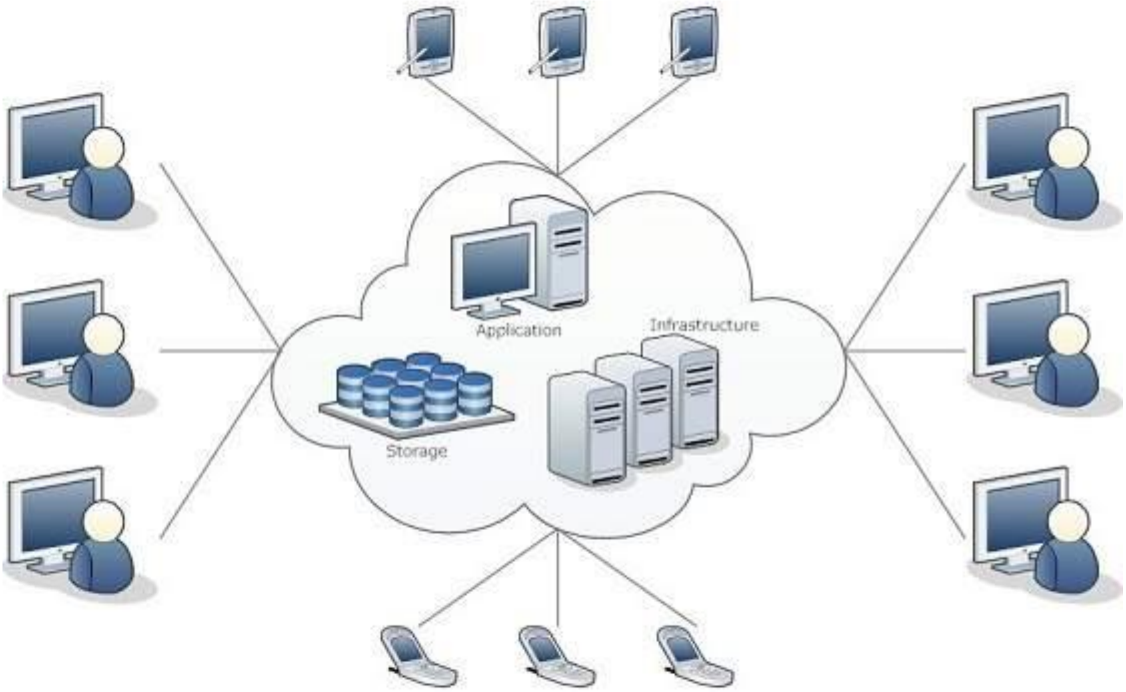
What is Cloud?

The term **Cloud** refers to a **Network** or **Internet.** In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN.

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

What is Cloud Computing?

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



Cloud computing offers **platform independency,** as the software is not required to be installed locally on the PC. Hence, the Cloud Computing is making our business applications **mobile** and **collaborative.**

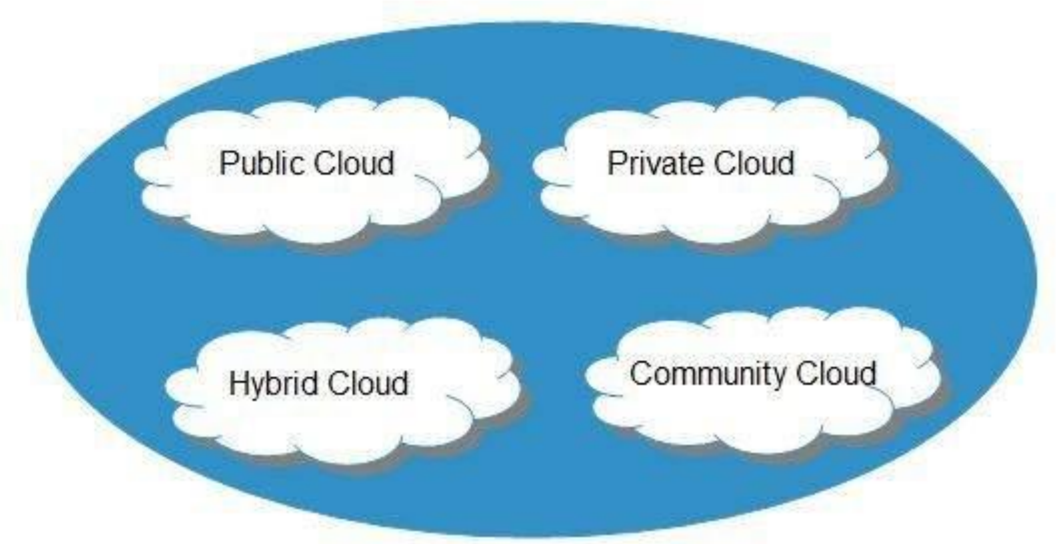
Basic Concepts

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

- Deployment Models
- Service Models

Deployment Models

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



Public Cloud

The **public cloud** allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness.

Private Cloud

The **private cloud** allows systems and services to be accessible within an organization. It is more secured because of its private nature.

Community Cloud

The **community cloud** allows systems and services to be accessible by a group of organizations.

Hybrid Cloud

The **hybrid cloud** is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

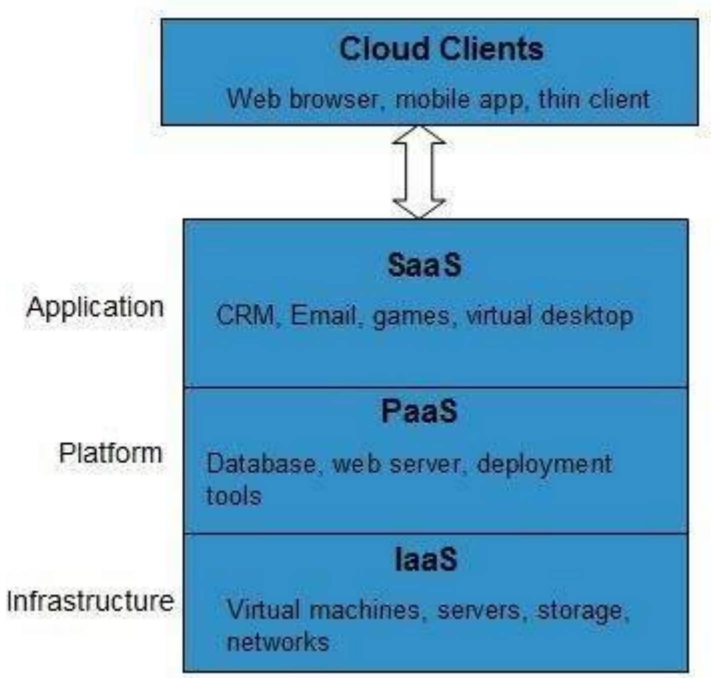
Service Models

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

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

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 or Strategy-as-a-Service.

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


Cloud Clients
Web browser, mobile app, thin client
SaaS
Application
CRM, Email, games, virtual desktop
PaaS
Platform
Database, web server, deployment tools
IaaS
Infrastructure
Virtual machines, servers, storage, networks

Infrastructure-as-a-Service (IaaS)

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

Platform-as-a-Service (PaaS)

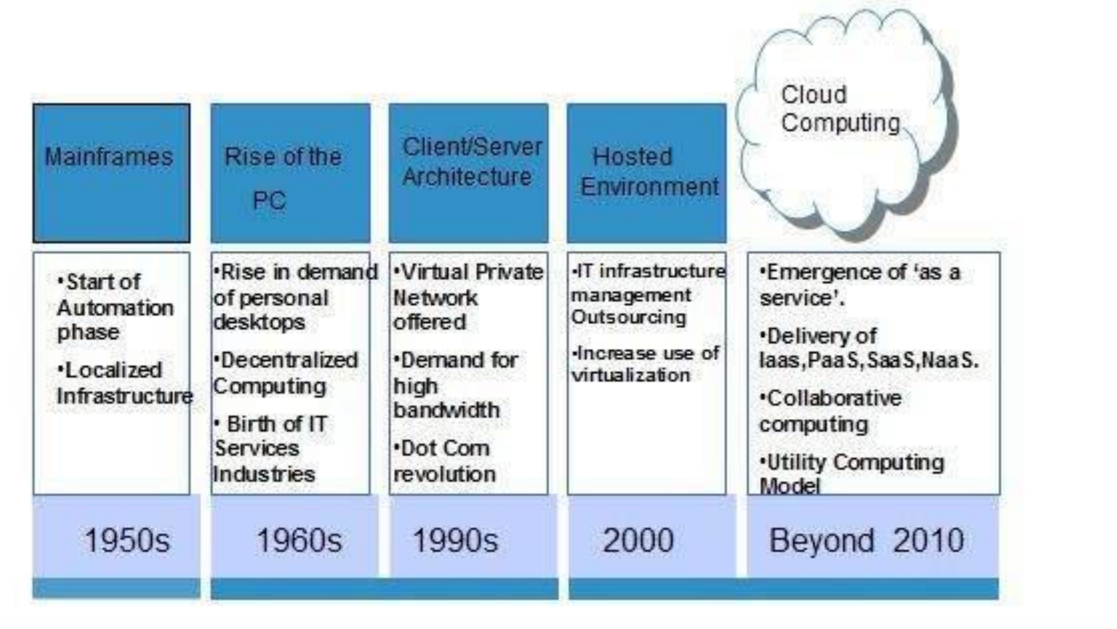
PaaS provides the runtime environment for applications, development and deployment tools, etc.

Software-as-a-Service (SaaS)

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

History of Cloud Computing

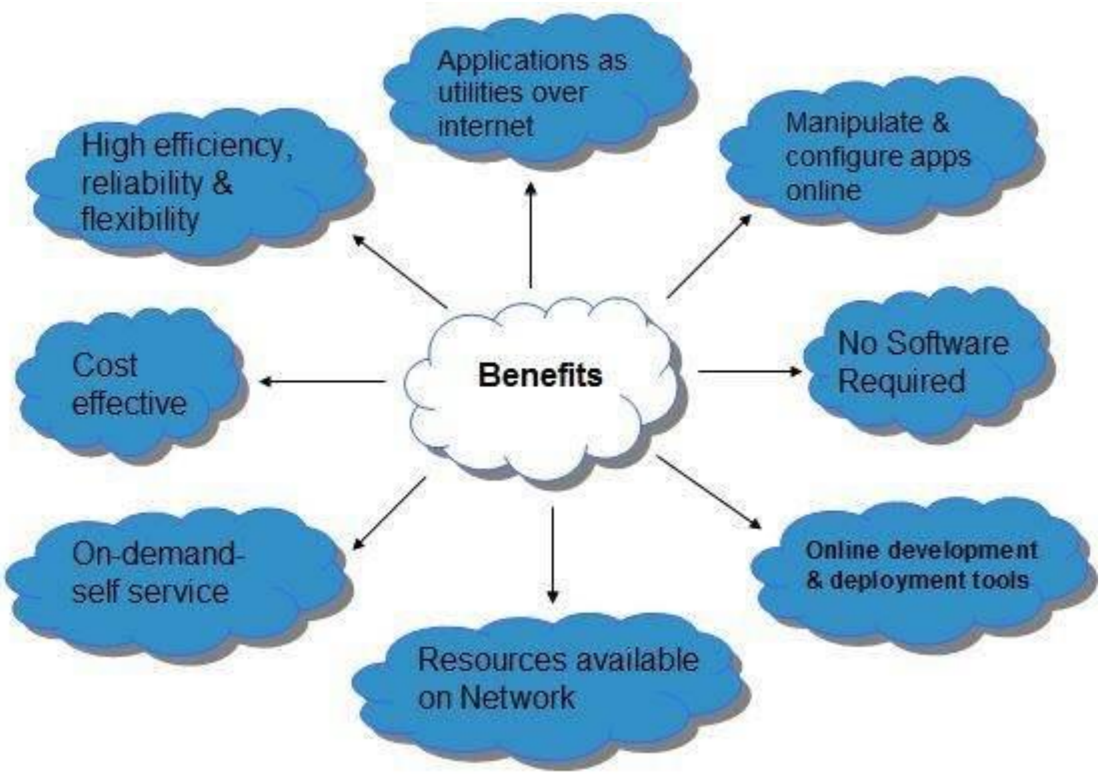
The concept of **Cloud Computing** came into existence in the year 1950 with implementation of mainframe computers, accessible via **thin/static clients.** Since then, cloud computing has been evolved from static clients to dynamic ones and from software to services. The following diagram explains the evolution of cloud computing:


Cloud Computing
Mainframes
Rise of the PC
Client/Server Architecture
Hosted Environment
•Start of Automation phase
•Localized Infrastructure
•Rise in demand of personal desktops
•Decentralized Computing
• Birth of IT Services Industries
•Virtual Private Network offered
•Demand for high bandwidth
•Dot Com revolution
•IT infrastructure management Outsourcing
•Increase use of virtualization
•Emergence of 'as a service'.
•Delivery of Iaas,PaaS,SaaS,NaaS.
•Collaborative computing
•Utility Computing Model
1950s
1960s
1990s
2000
Beyond 2010

Benefits

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

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


Applications as utilities over internet
High efficiency, reliability & flexibility
Manipulate & configure apps online
Benefits
Cost effective
No Software Required
On-demand-self service
Online development & deployment tools
Resources available on Network

Risks related to Cloud Computing

Although cloud Computing is a promising innovation with various benefits in the world of computing, it comes with risks. Some of them are discussed below:

Security and Privacy

It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to cloud service providers.

Although the cloud computing vendors ensure highly secured password protected accounts, any sign of security breach may result in loss of customers and businesses.

Lock In

It is very difficult for the customers to switch from one **Cloud Service Provider (CSP)** to another. It results in dependency on a particular CSP for service.

Isolation Failure

This risk involves the failure of isolation mechanism that separates storage, memory, and routing between the different tenants.

Management Interface Compromise

In case of public cloud provider, the customer management interfaces are accessible through the Internet.

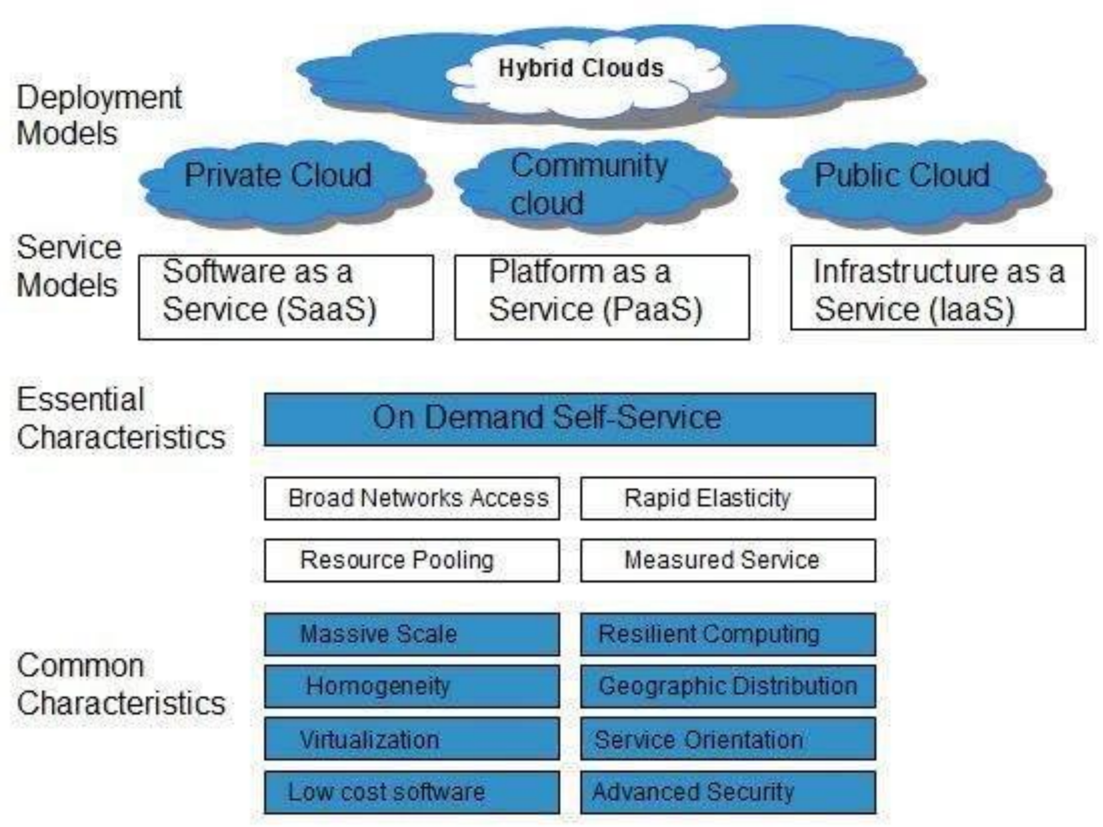
Insecure or Incomplete Data Deletion

It is possible that the data requested for deletion may not get deleted. It happens because either of the following reasons

- Extra copies of data are stored but are not available at the time of deletion
- Disk that stores data of multiple tenants is destroyed.

Characteristics of Cloud Computing

There are four key characteristics of cloud computing. They are shown in the following diagram:



On Demand Self Service

Cloud Computing allows the users to use web services and resources on demand. One can logon to a website at any time and use them.

Broad Network Access

Since cloud computing is completely web based, it can be accessed from anywhere and at any time.

Resource Pooling

Cloud computing allows multiple tenants to share a pool of resources. One can share single physical instance of hardware, database and basic infrastructure.

Rapid Elasticity

It is very easy to scale the resources vertically or horizontally at any time. Scaling of resources means the ability of resources to deal with increasing or decreasing demand.

The resources being used by customers at any given point of time are automatically monitored.

Measured Service

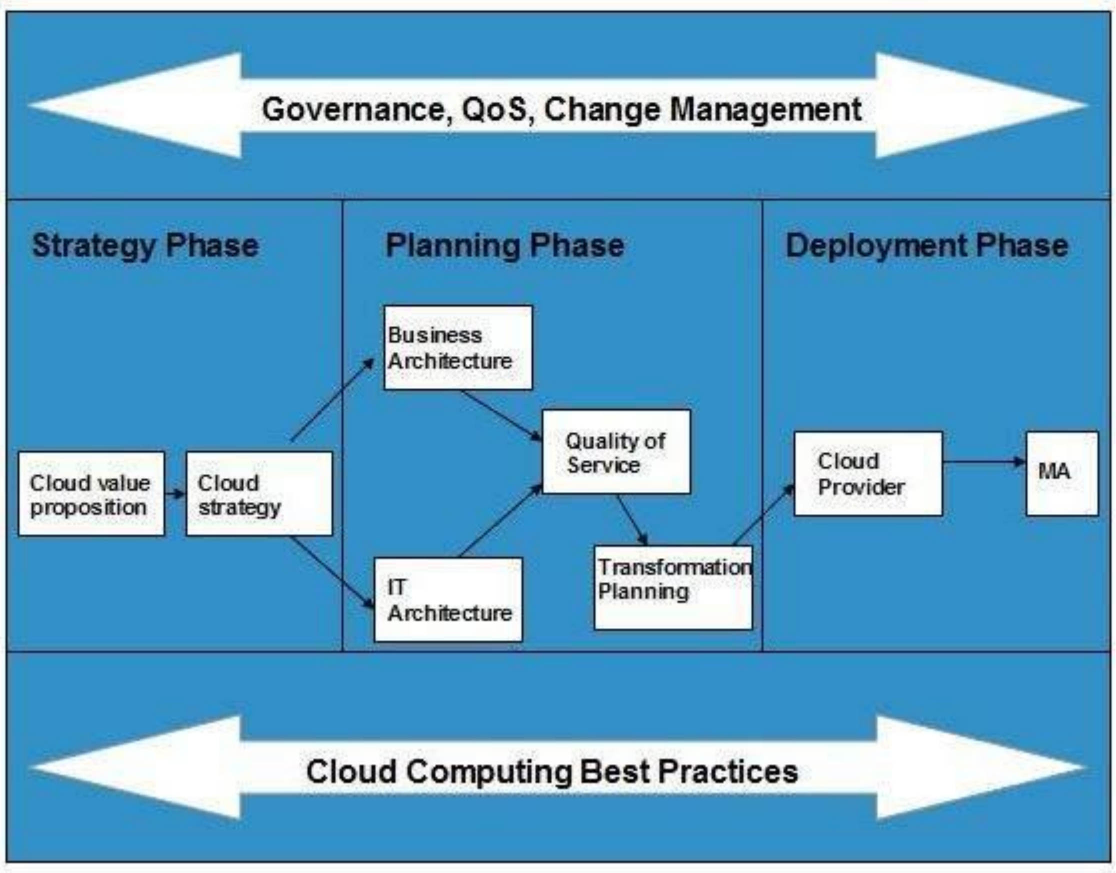
In this service cloud provider controls and monitors all the aspects of cloud service. Resource optimization, billing, and capacity planning etc. depend on it.

Cloud Computing Planning

Before deploying applications to cloud, it is necessary to consider your business requirements. Following are the issues one must consider:

- Data Security and Privacy Requirement
- Budget Requirements
- Type of cloud - public, private or hybrid
- Data backup requirements
- Training requirements
- Dashboard and reporting requirements
- Client access requirements
- Data export requirements

To meet all of these requirements, it is necessary to have well-compiled planning. In this tutorial, we will discuss the various planning phases that must be practised by an enterprise before migrating the entire business to cloud. Each of these planning phases are described in the following diagram:



Strategy Phase

In this phase, we analyze the strategy problems that customer might face. There are two steps to perform this analysis:

- Cloud Computing Value Proposition
- Cloud Computing Strategy Planning

Cloud Computing Value Proposition

In this, we analyze the factors influencing the customers when applying cloud computing mode and target the key problems they wish to solve. These key factors are:

- IT management simplification
- operation and maintenance cost reduction
- business mode innovation
- low cost outsourcing hosting
- high service quality outsourcing hosting.

All of the above analysis helps in decision making for future development.

Cloud Computing Strategy Planning

The strategy establishment is based on the analysis result of the above step. In this step, a strategy document is prepared according to the conditions a customer might face when applying cloud computing mode.

Planning Phase

This step performs analysis of problems and risks in the cloud application to ensure the customers that the cloud computing is successfully meeting their business goals. This phase involves the following planning steps:

- Business Architecture Development
- IT Architecture development
- Requirements on Quality of Service Development
- Transformation Plan development

Business Architecture Development

In this step, we recognize the risks that might be caused by cloud computing application from a business perspective.

IT Architecture Development

In this step, we identify the applications that support the business processes and the technologies required to support enterprise applications and data systems.

Requirements on Quality of Service Development

Quality of service refers to the non-functional requirements such as reliability, security, disaster recovery, etc. The success of applying cloud computing mode depends on these non-functional factors.

Transformation Plan Development

In this step, we formulate all kinds of plans that are required to transform current business to cloud computing modes.

Deployment Phase

This phase focuses on both of the above two phases. It involves the following two steps:

- Selecting Cloud Computing Provider
- Maintenance and Technical Service

Selecting Cloud Computing Provider

This step includes selecting a cloud provider on basis of Service Level Agreement (SLA), which defines the level of service the provider will meet.

Maintenance and Technical Service

Maintenance and Technical services are provided by the cloud provider. They need to ensure the quality of services.

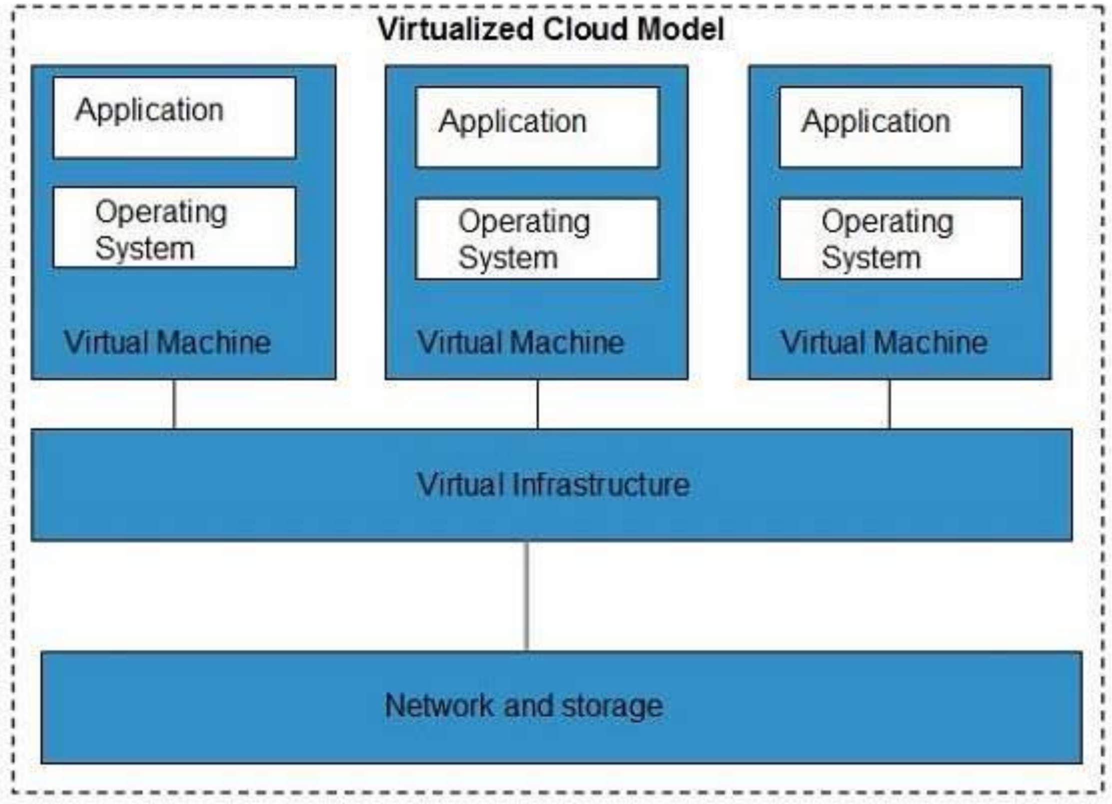
Cloud Computing Technologies

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.

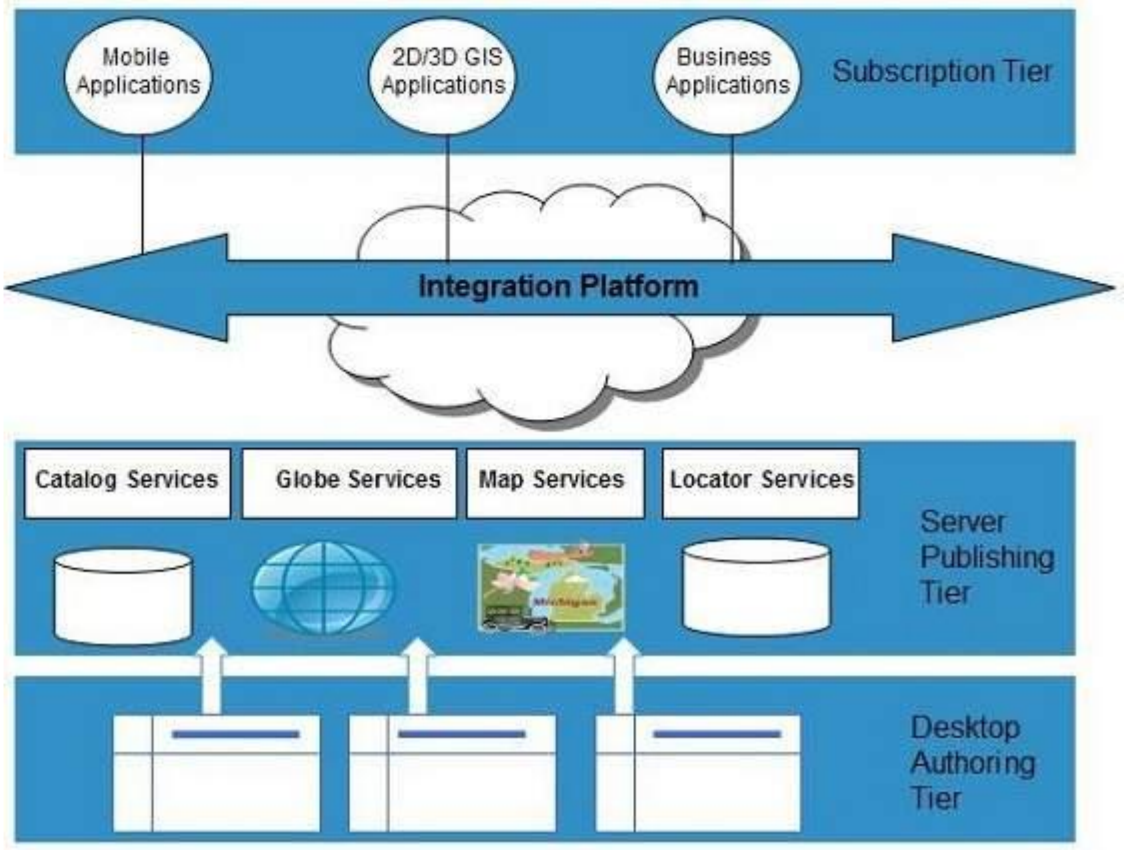


The **Multitenant** architecture offers **virtual isolation** among the multiple tenants. Hence, the organizations can use and customize their application as though they each have their instances running.

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.

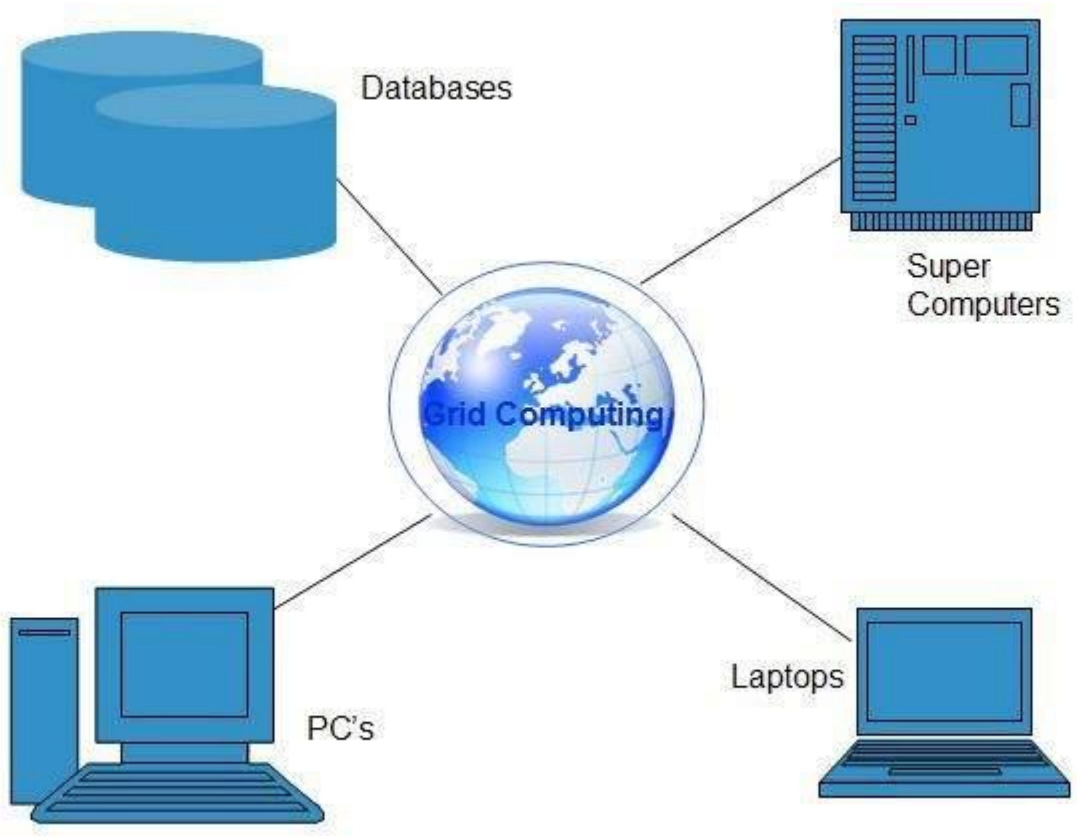
The cloud computing service oriented architecture is shown in the diagram below.



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

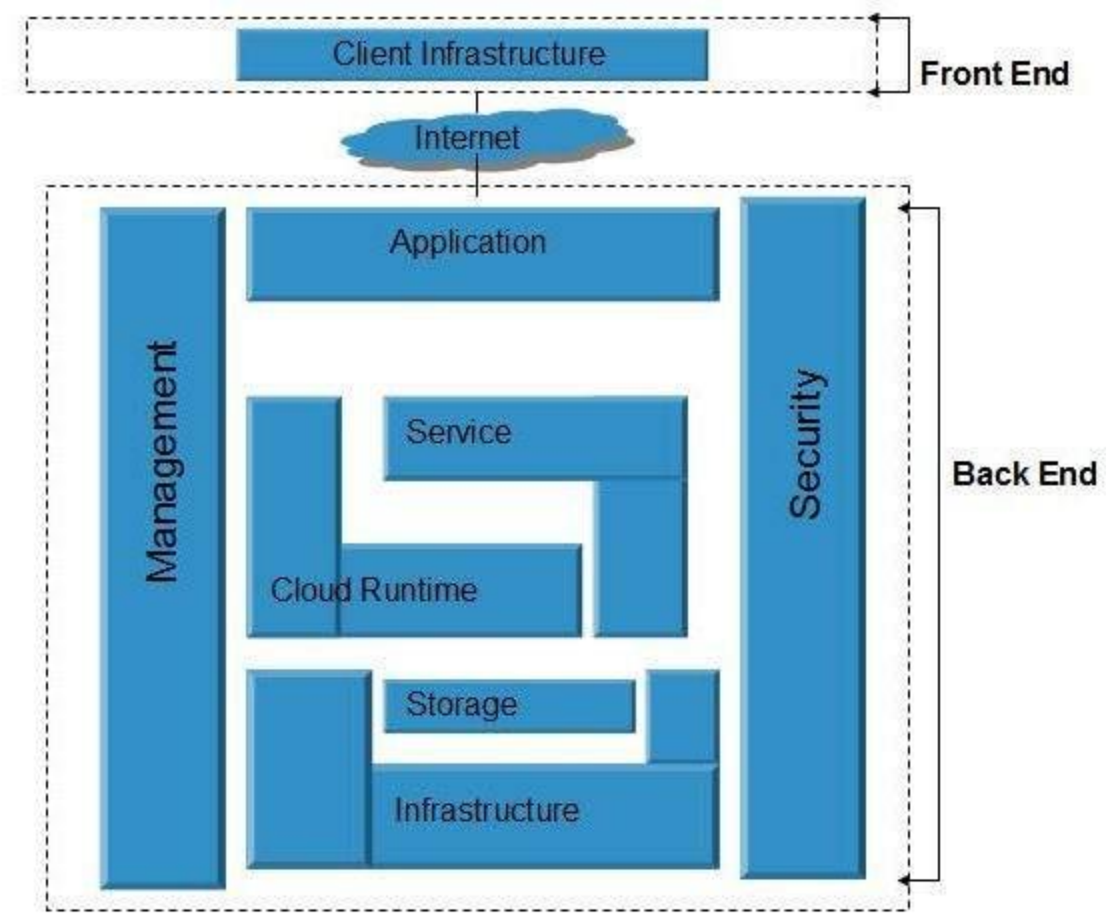
Utility computing is based on **Pay-per-Use model.** It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of utility computing.

Cloud Computing 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

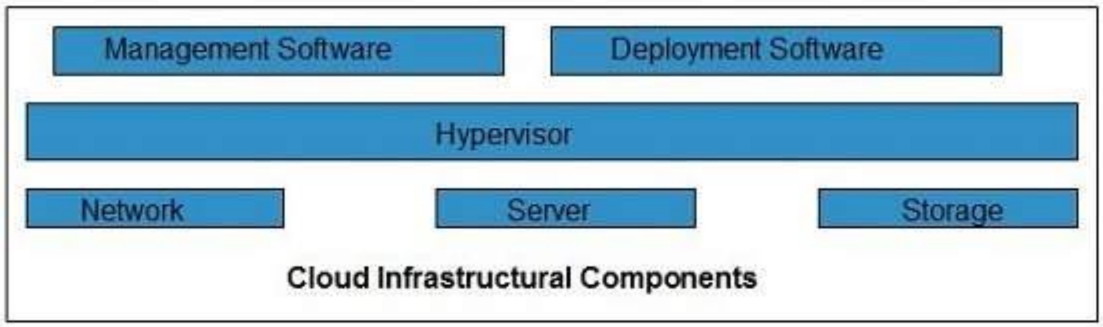
The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

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 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

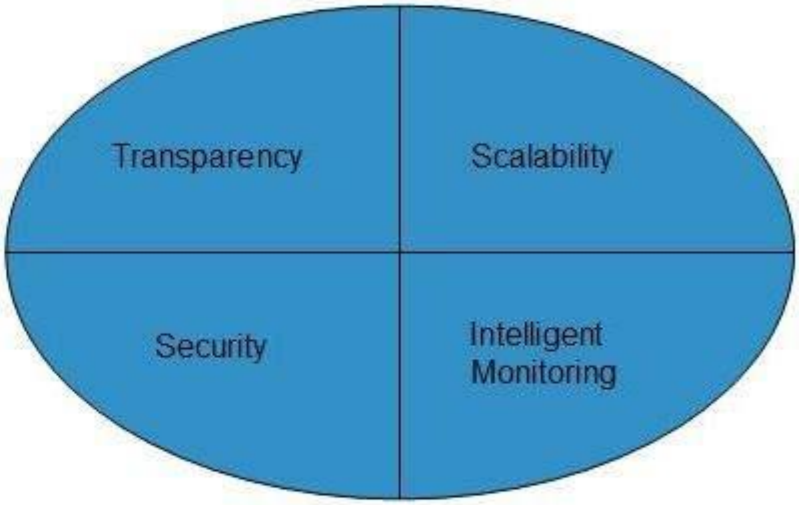
The **server** helps to compute the resource sharing and offers other services such as resource allocation and de-allocation, monitoring the resources, providing security etc.

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

Fundamental constraints that cloud infrastructure should implement are shown in the following diagram:



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

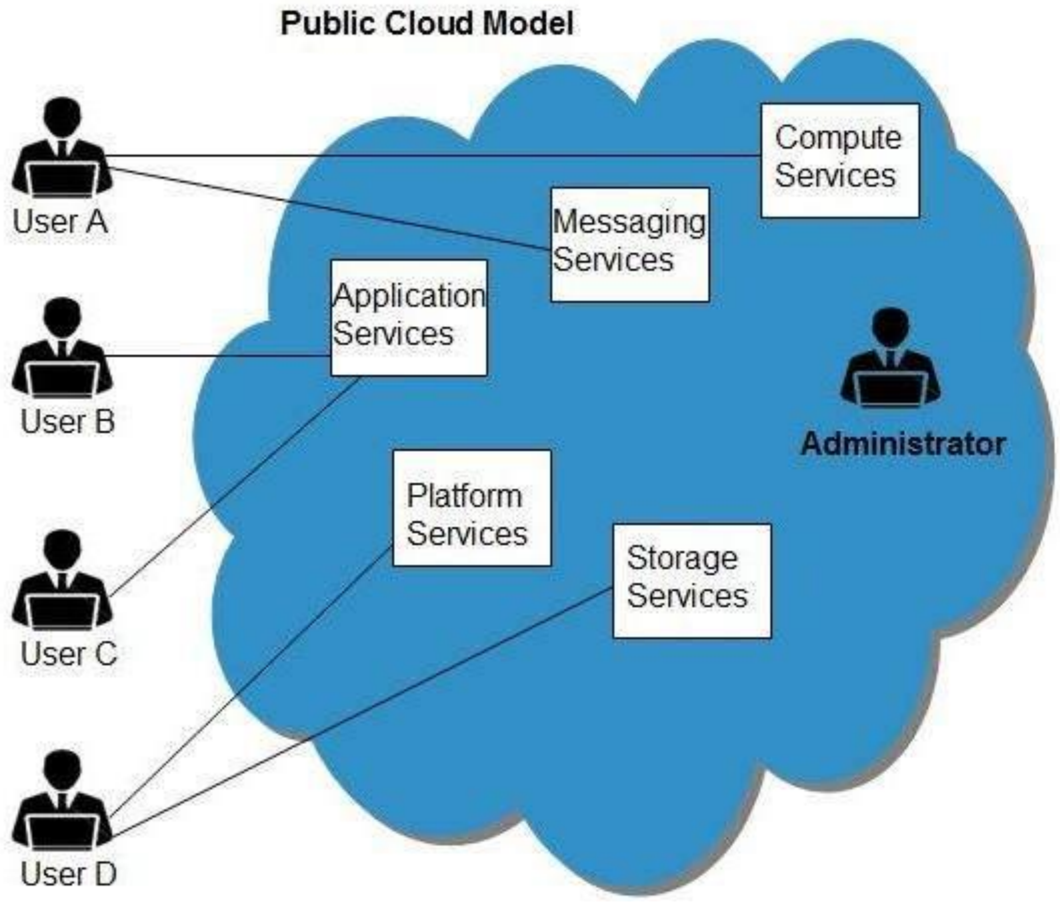
To achieve transparency and scalability, application solution delivery will need to be capable of intelligent monitoring.

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.

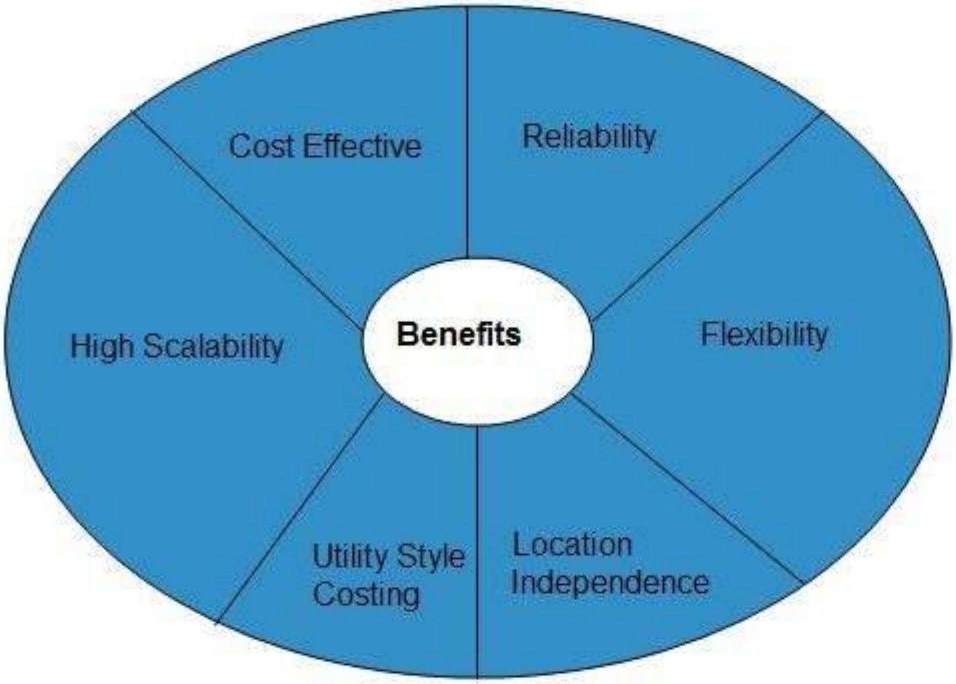
Public Cloud Model

Public Cloud allows systems and services to be easily accessible to general public. The IT giants such as **Google, Amazon** and **Microsoft** offer cloud services via Internet. 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

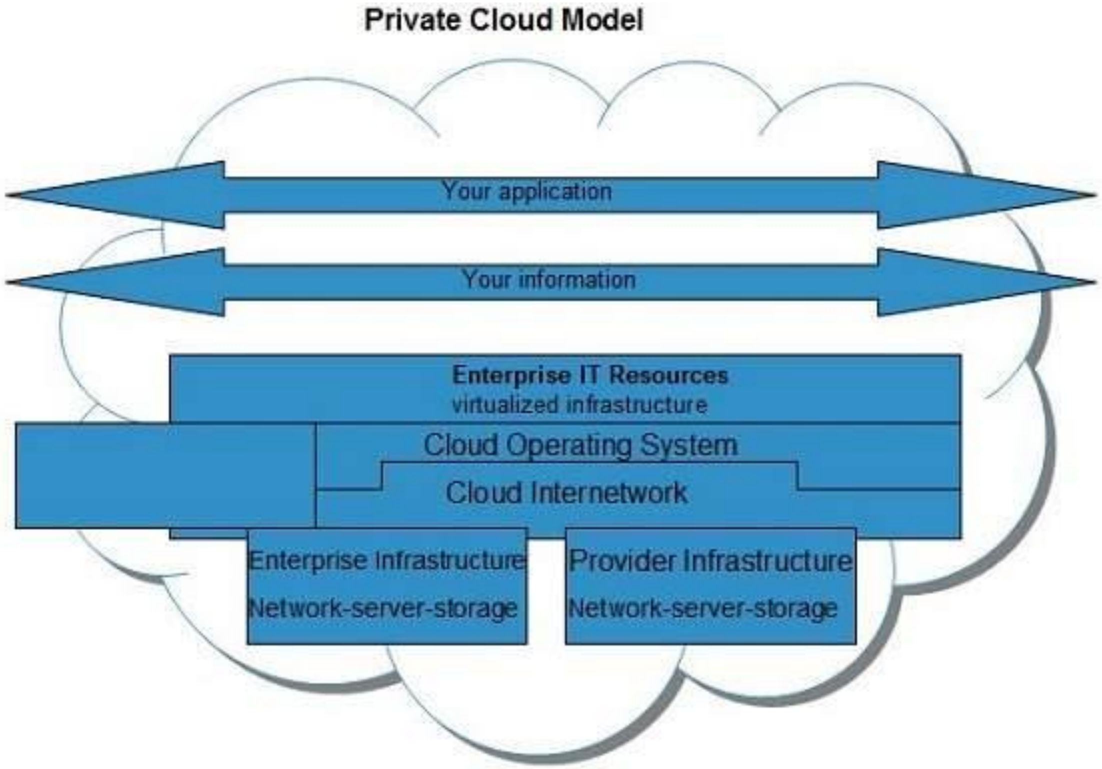
In **public cloud model,** data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.

Less Customizable

It is comparatively less customizable than private cloud.

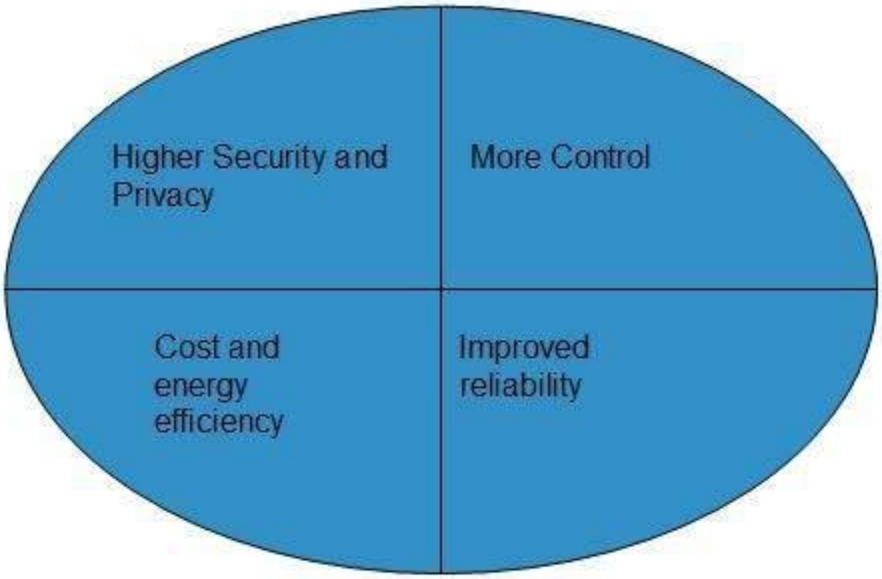
Private Cloud Model

Private Cloud allows systems and services to be accessible within an organization. The Private Cloud is operated only within a single organization. However, it may be managed internally by the organization itself or by third-party. 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.

Cost and 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

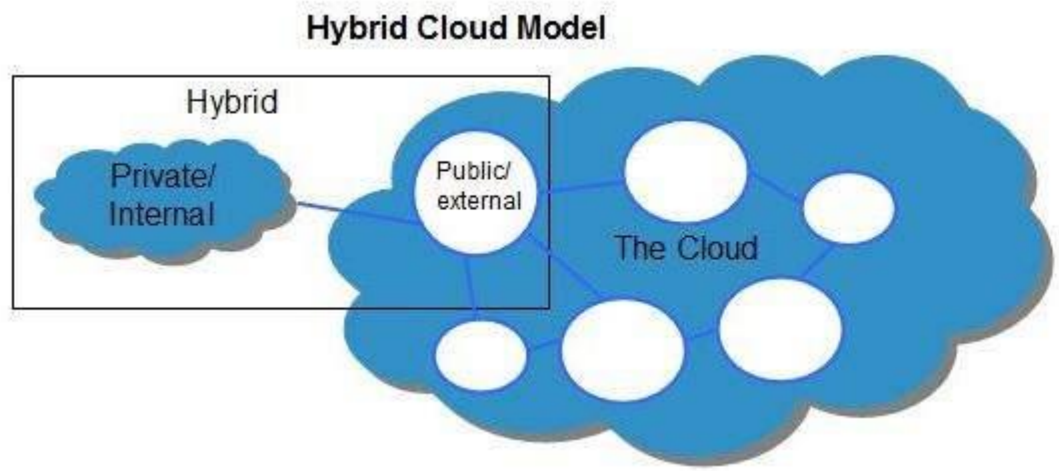
The private cloud can be scaled only within capacity of internal hosted resources.

Additional Skills

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

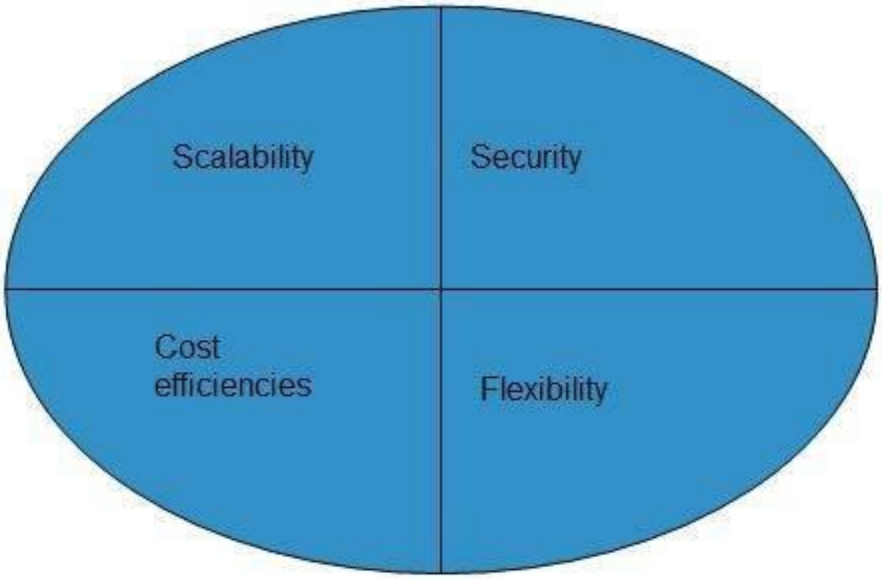
Hybrid Cloud Model

Hybrid Cloud is a mixture of **public** and **private** cloud. Non-critical activities are performed using public cloud while the critical activities are performed using private cloud. 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

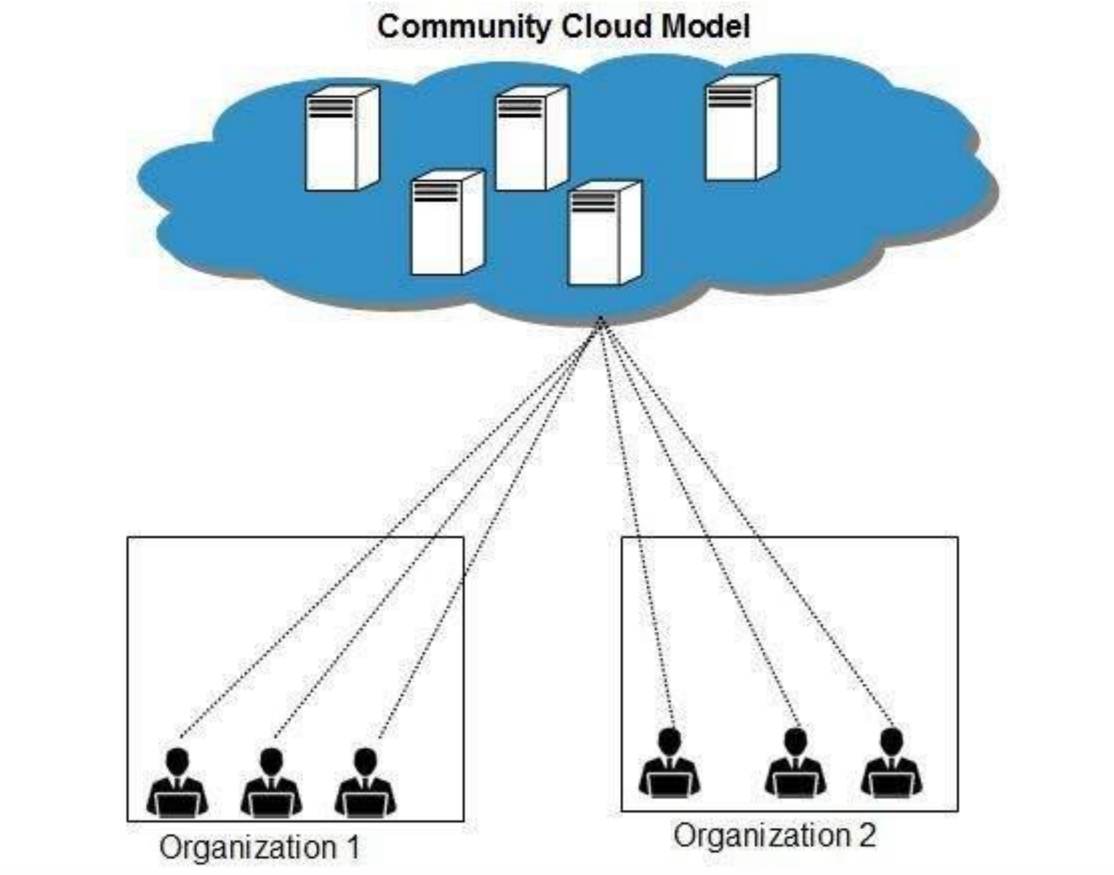
It is necessary to ensure that cloud services are compliant with security policies of the organization.

Infrastructure Dependency

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

Community Cloud Model

Community Cloud allows system and services to be accessible by group of organizations. It shares the infrastructure between several organizations from a specific community. It may be managed internally by organizations or by the third-party. 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.

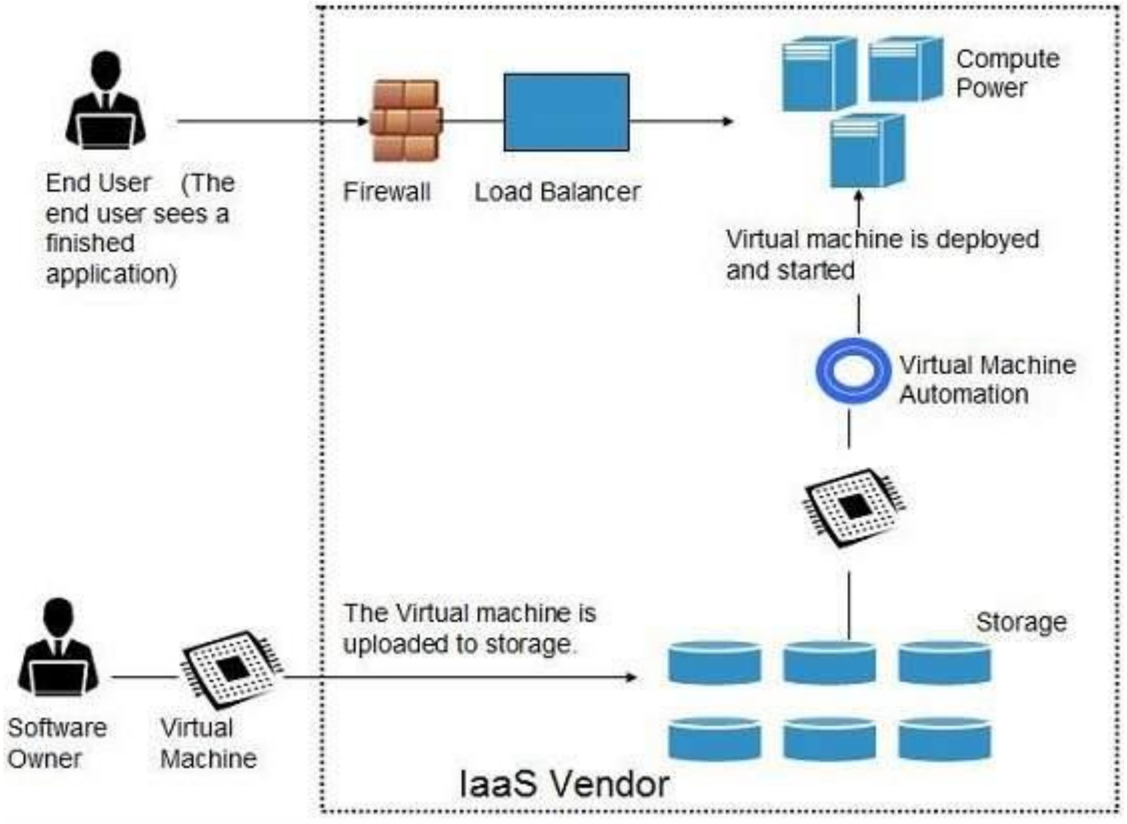
CLOUD SERVICE MODELS

Cloud Computing Infrastructure as a Service (IaaS)

Infrastructure-as-a-Service provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. Apart from these resources, the IaaS also offers:

- Virtual machine disk storage
- Virtual local area network (VLANs)
- Load balancers
- IP addresses
- Software bundles

All of the above resources are made available to end user via **server virtualization.** Moreover, these resources are accessed by the customers as if they own them.


End User (The end user sees a finished application)
Firewall
Load Balancer
Compute Power
Virtual machine is deployed and started
Virtual Machine Automation
The Virtual machine is uploaded to storage.
Storage
Software Owner
Virtual Machine
IaaS Vendor

Benefits

IaaS allows the cloud provider to freely locate the infrastructure over the Internet in a cost-effective manner. Some of the key benefits of IaaS are listed below:

- Full control of the computing resources through administrative access to VMs.
- Flexible and efficient renting of computer hardware.
- Portability, interoperability with legacy applications.

Full control over computing resources through administrative access to VMs

IaaS allows the customer to access computing resources through administrative access to virtual machines in the following manner:

- Customer issues administrative command to cloud provider to run the virtual machine or to save data on cloud server.
- Customer issues administrative command to virtual machines they owned to start web server or to install new applications.

Flexible and efficient renting of computer hardware

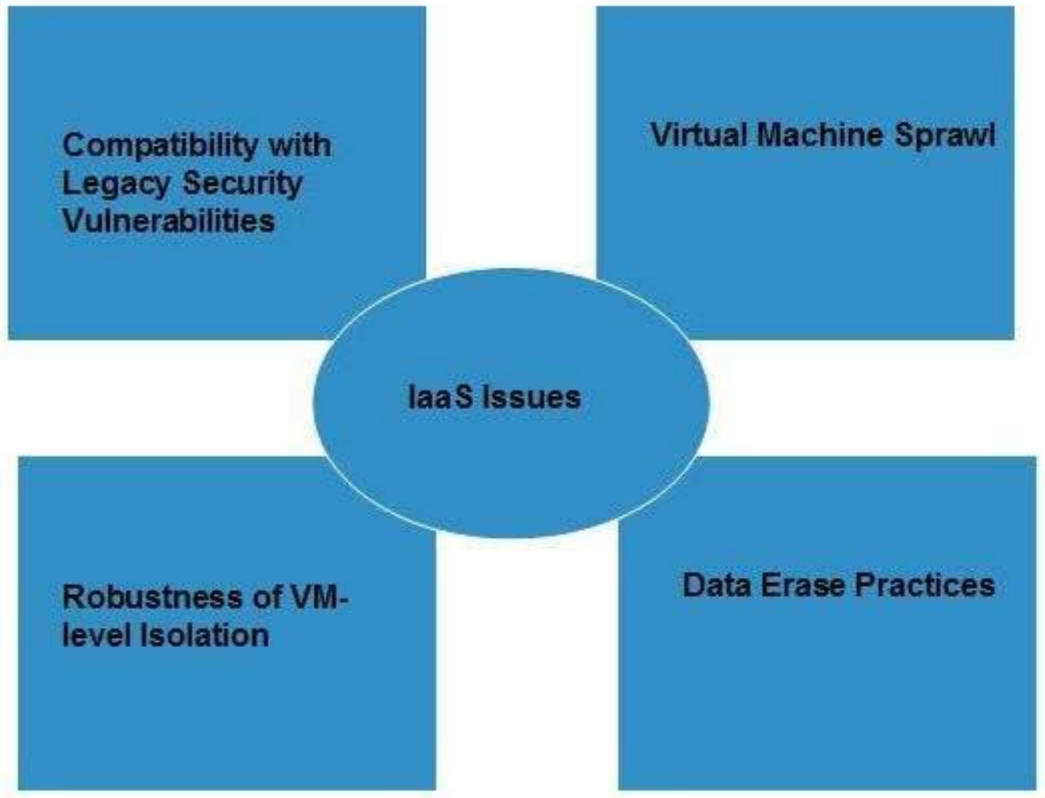
IaaS resources such as virtual machines, storage devices, bandwidth, IP addresses, monitoring services, firewalls, etc. are made available to the customers on rent. The payment is based upon the amount of time the customer retains a resource. Also with administrative access to virtual machines, the customer can run any software, even a custom operating system.

Portability, interoperability with legacy applications

It is possible to maintain legacy between applications and workloads between IaaS clouds. For example, network applications such as web server or e-mail server that normally runs on customer-owned server hardware can also run from VMs in IaaS cloud.

Issues

IaaS shares issues with PaaS and SaaS, such as Network dependence and browser based risks. It also has some specific issues, which are mentioned in the following diagram:


Compatibility with Legacy Security Vulnerabilities
Virtual Machine Sprawl
IaaS Issues
Robustness of VM-level Isolation
Data Erase Practices

Compatibility with legacy security vulnerabilities

Because IaaS offers the customer to run legacy software in provider's infrastructure, it exposes customers to all of the security vulnerabilities of such legacy software.

Virtual Machine sprawl

The VM can become out-of-date with respect to security updates because IaaS allows the customer to operate the virtual machines in running, suspended and off state. However, the provider can automatically update such VMs, but this mechanism is hard and complex.

Robustness of VM-level isolation

IaaS offers an isolated environment to individual customers through hypervisor. Hypervisor is a software layer that includes hardware support for virtualization to split a physical computer into multiple virtual machines.

Data erase practices

The customer uses virtual machines that in turn use the common disk resources provided by the cloud provider. When the customer releases the resource, the cloud provider must ensure that next customer to rent the resource does not observe data residue from previous customer.

Characteristics

Here are the characteristics of IaaS service model:

- Virtual machines with pre-installed software.
- Virtual machines with pre-installed operating systems such as Windows, Linux, and Solaris.
- On-demand availability of resources.
- Allows to store copies of particular data at different locations.
- The computing resources can be easily scaled up and down.

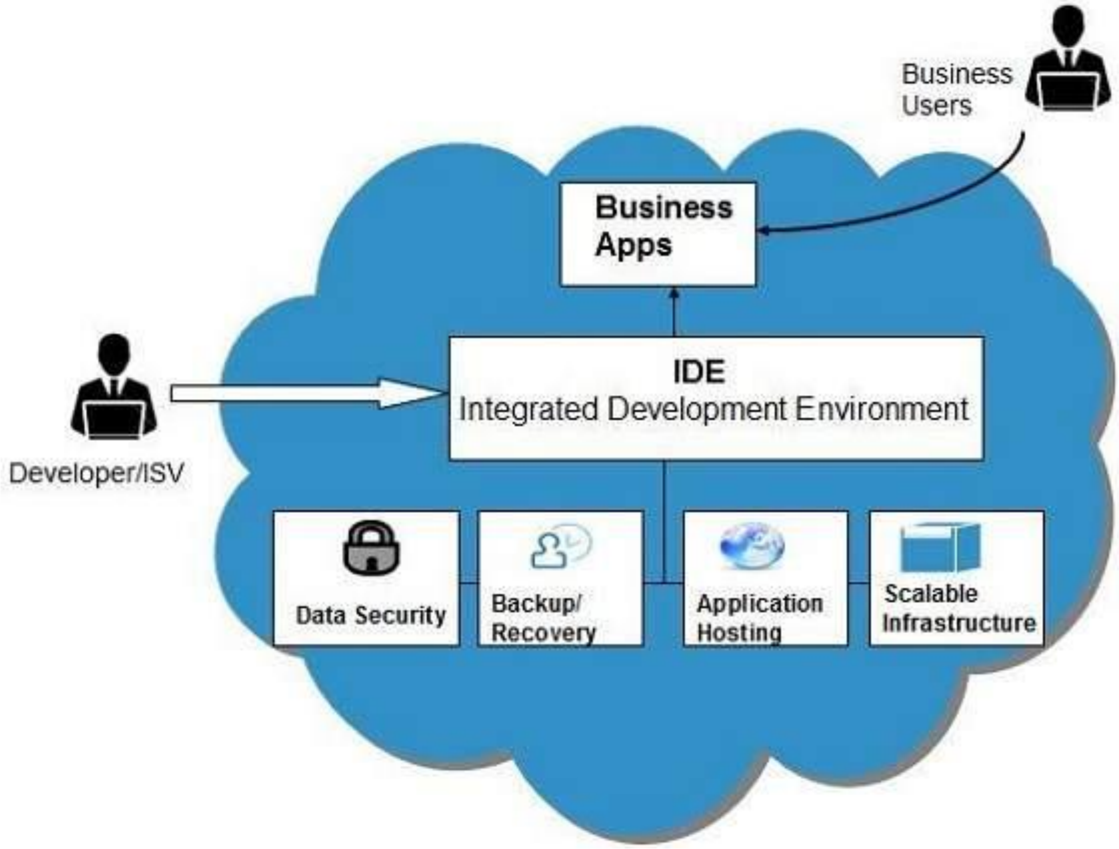
Cloud Computing Platform as a Service (PaaS)

Platform-as-a-Service offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of **point-and-click** tools that enables non-developers to create web applications.

App Engine of Google and **Force.com** are examples of PaaS offering vendors. Developer may log on to these websites and use the **built-in API** to create web-based applications.

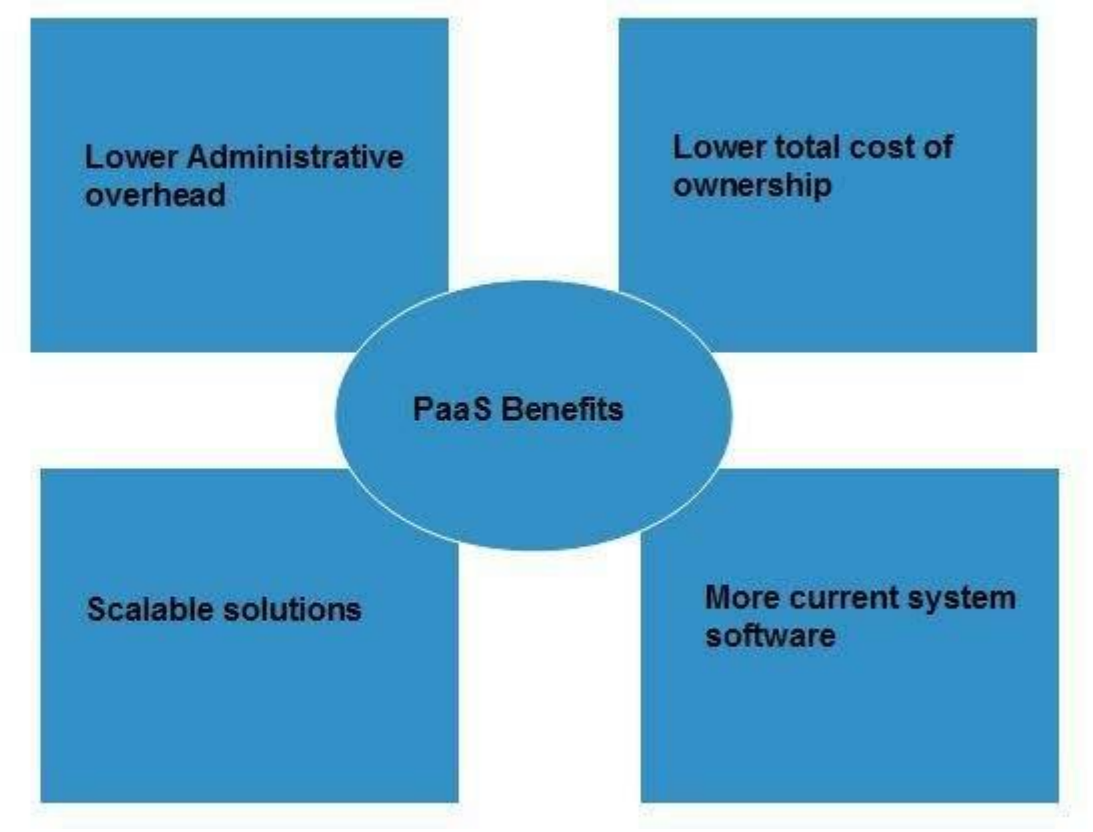
But the disadvantage of using PaaS is that, the developer **locks-in** with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

The following diagram shows how PaaS offers an API and development tools to the developers and how it helps the end user to access business applications.



Benefits

Following are the benefits of PaaS model:


Lower Administrative overhead
Lower total cost of ownership
PaaS Benefits
Scalable solutions
More current system software

Lower administrative overhead

Customer need not bother about the administration because it is the responsibility of cloud provider.

Lower total cost of ownership

Customer need not purchase expensive hardware, servers, power, and data storage.

Scalable solutions

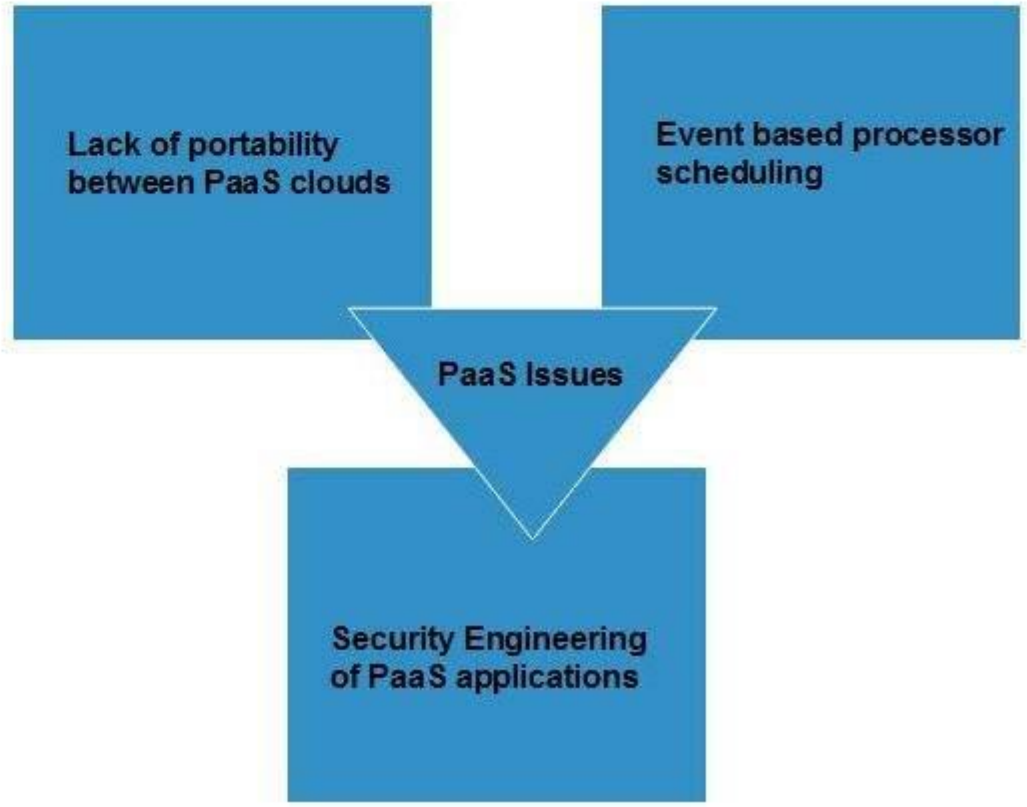
It is very easy to scale the resources up or down automatically, based on their demand.

More current system software

It is the responsibility of the cloud provider to maintain software versions and patch installations.

Issues

Like **SaaS, PaaS** also places significant burdens on customer's browsers to maintain reliable and secure connections to the provider’s systems. Therefore, PaaS shares many of the issues of SaaS. However, there are some specific issues associated with PaaS as shown in the following diagram:


Lack of portability between PaaS clouds
Event based processor scheduling
PaaS Issues
Security Engineering of PaaS applications

Lack of portability between PaaS clouds

Although standard languages are used, yet the implementations of platform services may vary. For example, file, queue, or hash table interfaces of one platform may differ from another, making it difficult to transfer the workloads from one platform to another.

Event based processor scheduling

The PaaS applications are event-oriented which poses resource constraints on applications, i.e., they have to answer a request in a given interval of time.

Security engineering of PaaS applications

Since PaaS applications are dependent on network, they must explicitly use cryptography and manage security exposures.

Characteristics

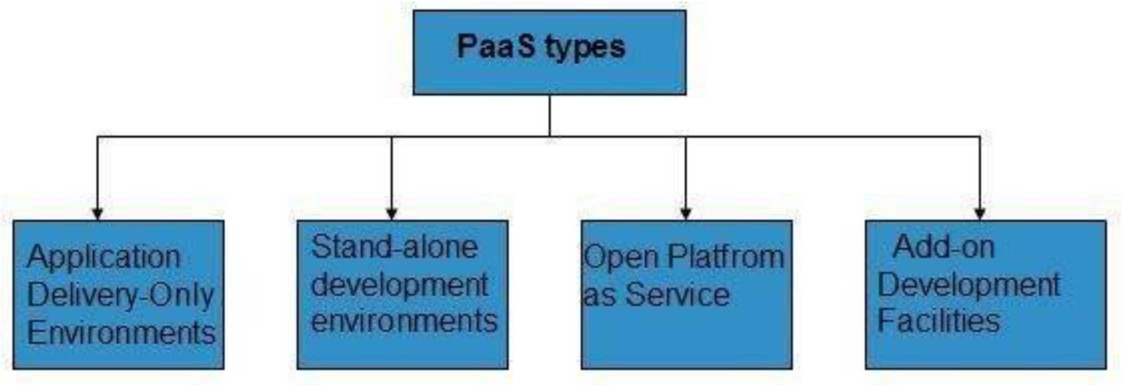
Here are the characteristics of PaaS service model:

- PaaS offers **browser based development environment.** It allows the developer to create 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 provides built-in tools for defining **workflow, approval processes,** and business rules.
- It is easy to integrate PaaS with other applications on the same platform.
- PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

PaaS Types

Based on the functions, PaaS can be classified into four types as shown in the following diagram:


PaaS types
Application Delivery-Only Environments
Stand-alone development environments
Open Platfrom as Service
Add-on Development Facilities

Stand-alone development environments

The **stand-alone PaaS** works as an independent entity for a specific function. It does not include licensing or technical dependencies on specific SaaS applications.

Application delivery-only environments

The **application delivery PaaS** includes **on-demand scaling** and **application security.**

Open platform as a service

Open PaaS offers an **open source software** that helps a PaaS provider to run applications.

Add-on development facilities

The **add-on PaaS** allows to customize the existing SaaS platform.

Cloud Computing Software as a Service (SaaS)

Software-as–a-Service (SaaS) model allows to provide software application as a service to the end users. It refers to a software that is deployed on a host service and is accessible via Internet. There are several SaaS applications listed below:

- Billing and invoicing system
- Customer Relationship Management (CRM) applications
- Help desk applications
- Human Resource (HR) solutions

Some of the SaaS applications are not customizable such as **Microsoft Office Suite.** But SaaS provides us **Application Programming Interface (API),** which allows the developer to develop a customized application.

Characteristics

Here are the characteristics of SaaS service model:

- SaaS makes the software available over the Internet.
- The software applications are maintained by the vendor.
- The license to the software may be subscription based or usage based. And it is billed on recurring basis.
- SaaS applications are cost-effective since they do not require any maintenance at end user side.
- They are available on demand.
- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SaaS offers shared data model. Therefore, multiple users can share single instance of infrastructure. It is not required to hard code the functionality for individual users.
- All users run the same version of the software.

Benefits

Using SaaS has proved to be beneficial in terms of scalability, efficiency and performance. Some of the benefits are listed below:

- Modest software tools
- Efficient use of software licenses
- Centralized management and data
- Platform responsibilities managed by provider

- Multitenant solutions

Modest software tools

The SaaS application deployment requires a little or no client side software installation, which results in the following benefits:

- No requirement for complex software packages at client side
- Little or no risk of configuration at client side
- Low distribution cost

Efficient use of software licenses

The customer can have single license for multiple computers running at different locations which reduces the licensing cost. Also, there is no requirement for license servers because the software runs in the provider's infrastructure.

Centralized management and data

The cloud provider stores data centrally. However, the cloud providers may store data in a decentralized manner for the sake of redundancy and reliability.

Platform responsibilities managed by providers

All platform responsibilities such as backups, system maintenance, security, hardware refresh, power management, etc. are performed by the cloud provider. The customer does not need to bother about them.

Multitenant solutions

Multitenant solutions allow multiple users to share single instance of different resources in virtual isolation. Customers can customize their application without affecting the core functionality.

Issues

There are several issues associated with SaaS, some of them are listed below:

- Browser based risks
- Network dependence
- Lack of portability between SaaS clouds

Browser based risks

If the customer visits malicious website and browser becomes infected, the subsequent access to SaaS application might compromise the customer's data.

To avoid such risks, the customer can use multiple browsers and dedicate a specific browser to access SaaS applications or can use virtual desktop while accessing the SaaS applications.

Network dependence

The SaaS application can be delivered only when network is continuously available. Also network should be reliable but the network reliability cannot be guaranteed either by cloud provider or by the customer.

Lack of portability between SaaS clouds

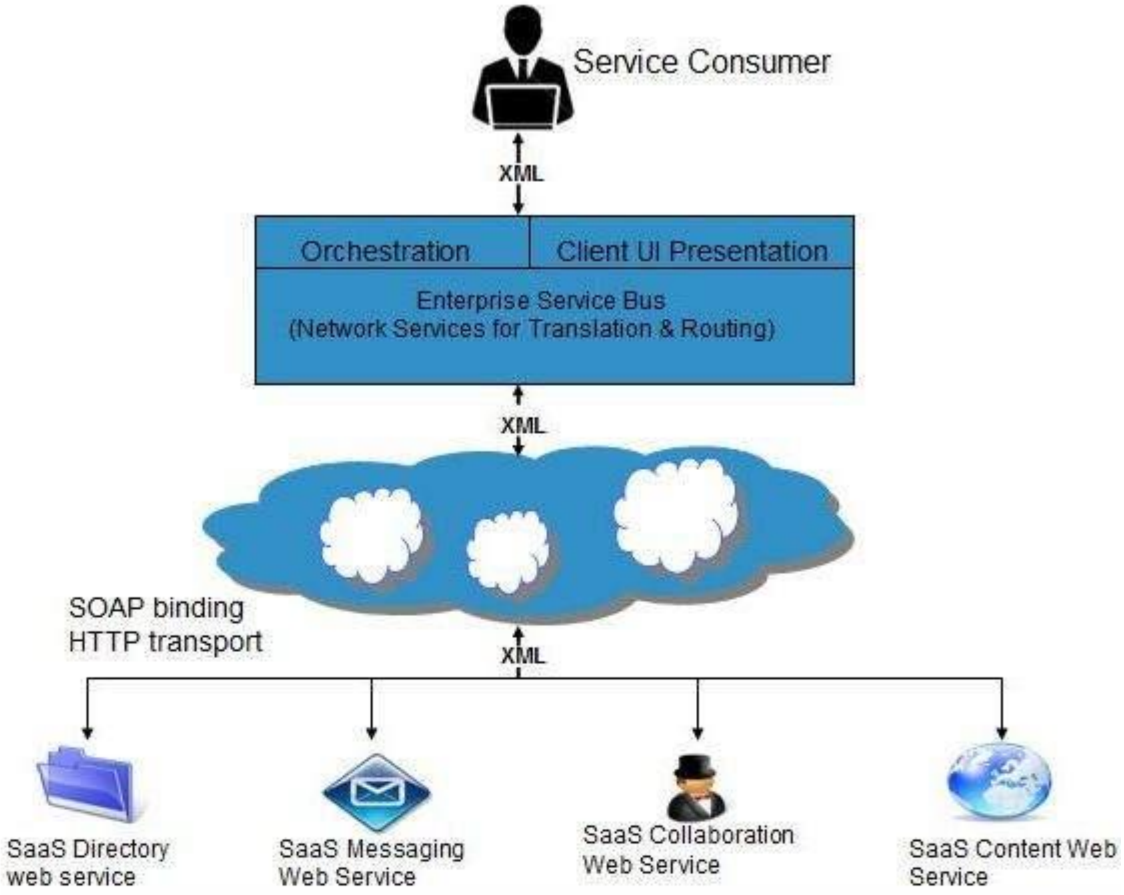
Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.

Open SaaS and SOA

Open SaaS uses those SaaS applications, which are developed using open source programming language. These SaaS applications can run on any open source operating system and database. Open SaaS has several benefits listed below:

- No License Required
- Low Deployment Cost
- Less Vendor Lock-in
- More portable applications
- More Robust Solution

The following diagram shows the SaaS implementation based on SOA:



Cloud Computing Identity as a Service (IDaaS)

Employees in a company require to login to system to perform various tasks. These systems may be based on local server or cloud based. Following are the problems that an employee might face:

- Remembering different username and password combinations for accessing multiple servers.
- If an employee leaves the company, it is required to ensure that each account of that user is disabled. This increases workload on IT staff.

To solve above problems, a new technique emerged which is known as **Identity-as–a-Service (IDaaS).**

IDaaS offers management of identity information as a digital entity. This identity can be used during electronic transactions.

Identity

Identity refers to set of attributes associated with something to make it recognizable. All objects may have same attributes, but their identities cannot be the same. A unique identity is assigned through unique identification attribute.

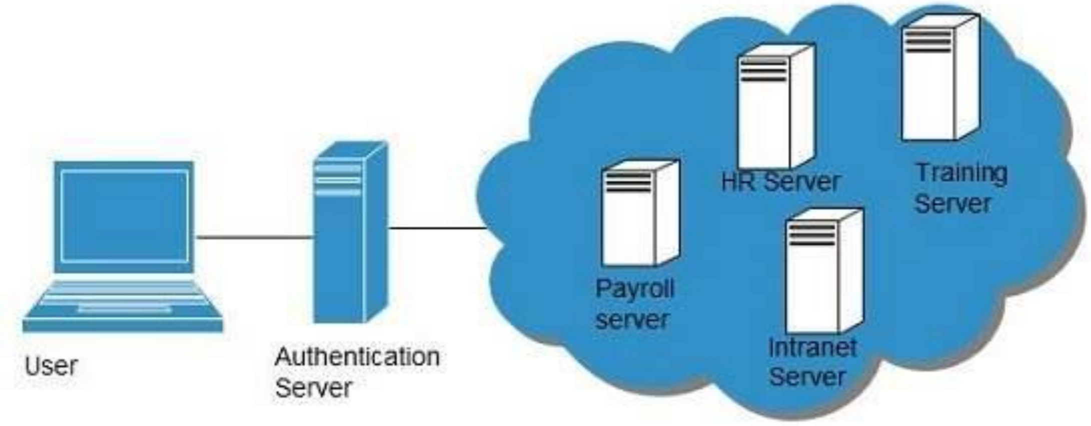
There are several **identity services** that are deployed to validate services such as validating web sites, transactions, transaction participants, client, etc. Identity-as-a-Service may include the following:

- Directory services
- Federated services
- Registration
- Authentication services
- Risk and event monitoring
- Single sign-on services
- Identity and profile management

Single Sign-On (SSO)

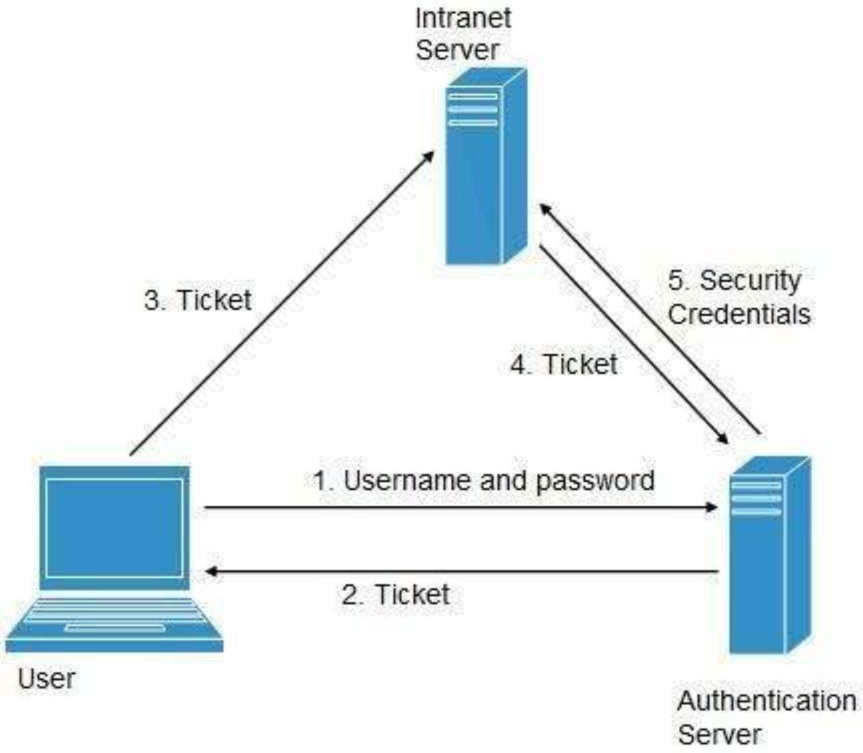
To solve the problem of using different username and password combinations for different servers, companies now employ Single Sign-On software, which allows the user to login only one time and manage the access to other systems.

SSO has single authentication server, managing multiple accesses to other systems, as shown in the following diagram:



SSO Working

There are several implementations of SSO. Here, we discuss the common ones:



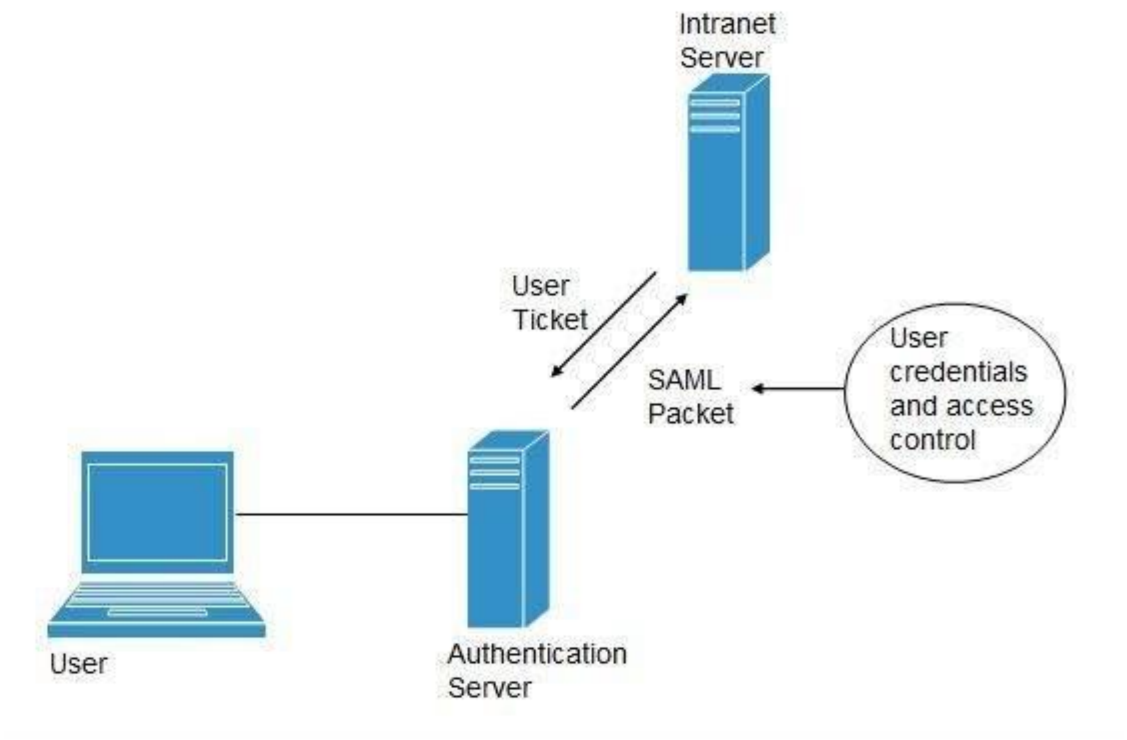
Following steps explain the working of Single Sign-On software:

- User logs into the authentication server using a username and password.
- The authentication server returns the user's ticket.
- User sends the ticket to intranet server.
- Intranet server sends the ticket to the authentication server.
- Authentication server sends the user's security credentials for that server back to the intranet server.

If an employee leaves the company, then disabling the user account at the authentication server prohibits the user's access to all the systems.

Federated Identity Management (FIDM)

FIDM describes the technologies and protocols that enable a user to package security credentials across security domains. It uses **Security Markup Language (SAML)** to package a user's security credentials as shown in the following diagram:



OpenID

It offers users to login into multiple websites with single account. Google, Yahoo!, Flickr, MySpace, WordPress.com are some of the companies that support OpenID.

Benefits

- Increased site conversation rates
- Access to greater user profile content
- Fewer problems with lost passwords
- Ease of content integration into social networking sites

Cloud Computing Network as a Service (NaaS)

Network-as-a-Service allows us to access to network infrastructure directly and securely. NaaS makes it possible to deploy **custom routing protocols.**

NaaS uses **virtualized network infrastructure** to provide network services to the customer. It is the responsibility of NaaS provider to maintain and manage the network resources. Having a provider working for a customer decreases the workload of the customer. Moreover, NaaS offers **network as a utility.** NaaS is also based on **pay-per-use model.**

How NaaS is delivered?

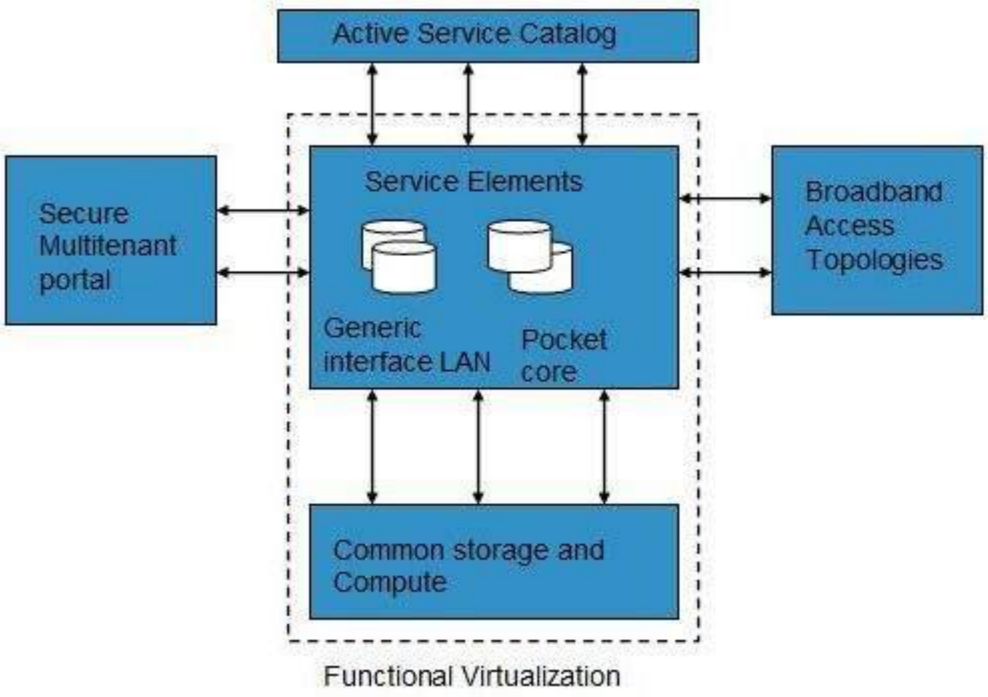
To use NaaS model, the customer is required to logon to the web portal, where he can get online API. Here, the customer can customize the route.

In turn, customer has to pay for the capacity used. It is also possible to turn off the capacity at any time.

Mobile NaaS

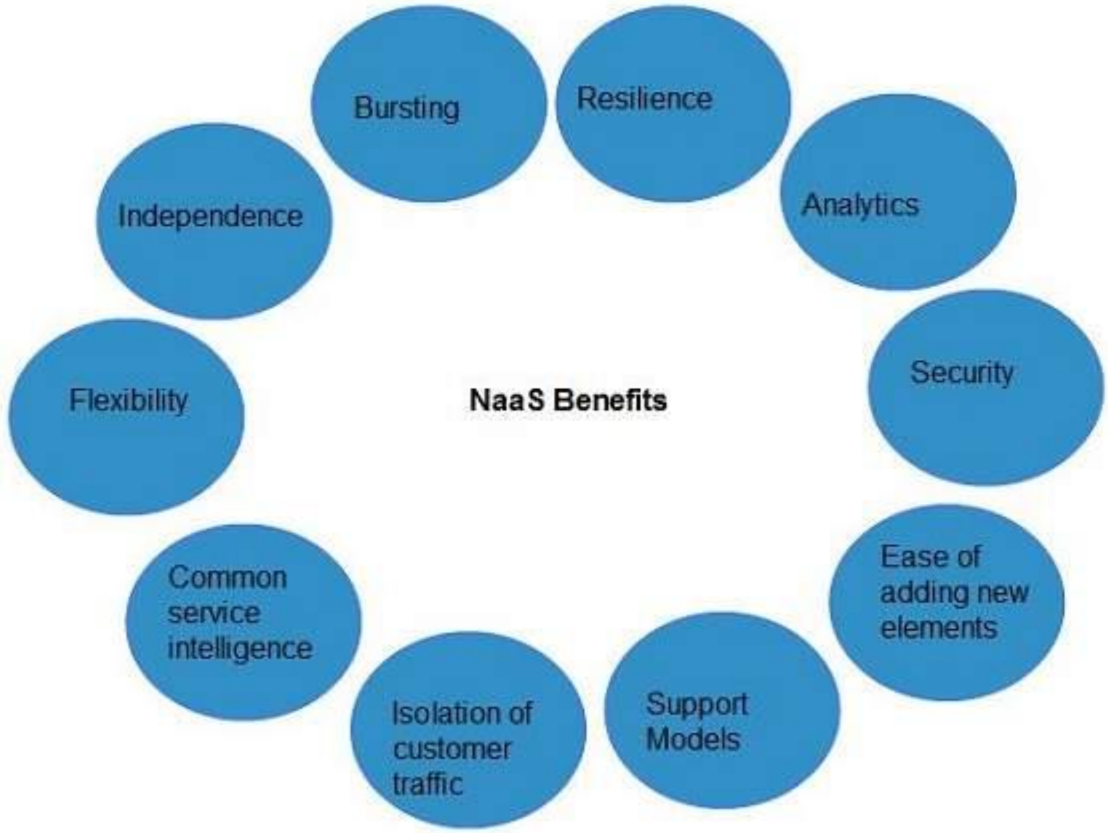
Mobile NaaS offers more efficient and flexible control over mobile devices. It uses virtualization to simplify the architecture thereby creating more efficient processes.

Following diagram shows the Mobile NaaS service elements:


Active Service Catalog
Secure Multitenant portal
Service Elements
Generic interface LAN
Pocket core
Broadband Access Topologies
Common storage and Compute
Functional Virtualization

NaaS Benefits

NaaS offers a number of benefits as discussed below:



Independence

Each customer is independent and can segregate the network.

Bursting

The customer pays for high-capacity network only on requirement.

Resilience

The reliability treatments are available, which can be applied for critical applications.

Analytics

The data protection solutions are available, which can be applied for highly sensitive applications.

Ease of Adding New Service Elements

It is very easy to integrate new service elements to the network.

Support Models

A number of support models are available to reduce operation cost.

Isolation of Customer Traffic

The customer traffic is logically isolated.

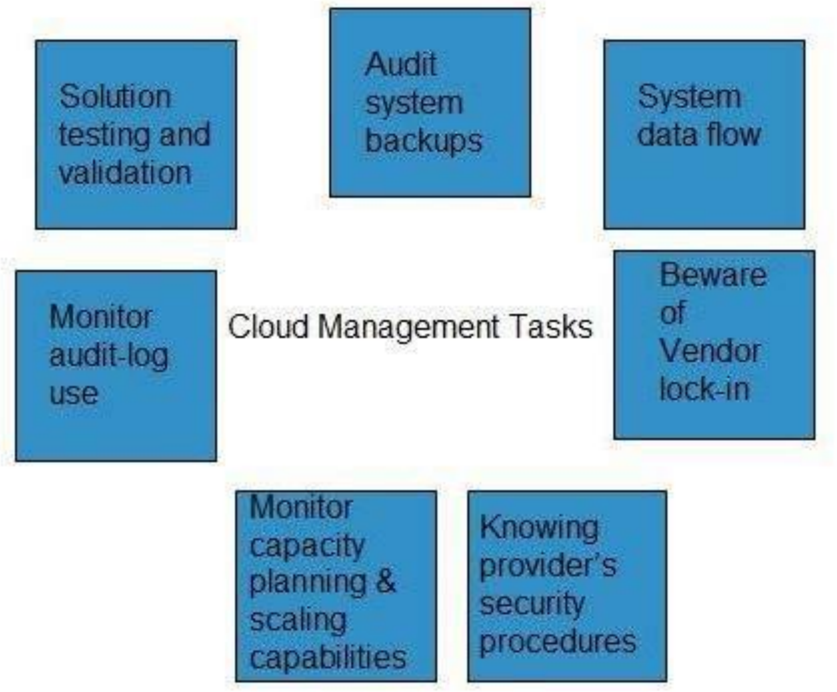
CLOUD ADVANCED CONCEPTS

Cloud Computing Management

It is the responsibility of cloud provider to manage resources and their performance. Management of resources includes several aspects of cloud computing such as load balancing, performance, storage, backups, capacity, deployment, etc. The management is essential to access full functionality of resources in the cloud.

Cloud Management Tasks

The cloud provider performs a number of tasks to ensure efficient use of cloud resources. Here, we will discuss some of them:


Solution testing and validation
Audit system backups
System data flow
Monitor audit-log use
Cloud Management Tasks
Beware of Vendor lock-in
Monitor capacity planning & scaling capabilities
Knowing provider's security procedures

Audit System Backups

It is required to audit the backups timely to ensure restoring of randomly selected files of different users. Backups can be performed in following ways:

- Backing up files by the company, from on-site computers to the disks that reside within the cloud.
- Backing up files by the cloud provider.

It is necessary to know if cloud provider has encrypted the data, who has access to that data and if the backup is taken at different locations then the user must know the details of those locations.

Data Flow of the System

The managers are responsible to develop a diagram describing a detailed process flow. This process flow describes the movement of data belonging to an organization throughout the cloud solution.

Vendor Lock-In Awareness and Solutions

The managers must know the procedure to exit from services of a particular cloud provider. The procedures must be defined to enable the cloud managers to export data of an organization from their system to another cloud provider.

Knowing Provider's Security Procedures

The managers should know the security plans of the provider for the following services:

- Multitenant use
- E-commerce processing
- Employee screening
- Encryption policy

Monitoring Capacity Planning and Scaling Capabilities

The managers must know the capacity planning in order to ensure whether the cloud provider is meeting the future capacity requirement for his business or not.

The managers must manage the scaling capabilities in order to ensure services can be scaled up or down as per the user need.

Monitor Audit Log Use

In order to identify errors in the system, managers must audit the logs on a regular basis.

Solution Testing and Validation

When the cloud provider offers a solution, it is essential to test it in order to ensure that it gives the correct result and it is error-free. This is necessary for a system to be robust and reliable.

Cloud Computing Data Storage

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a **web services API.**

Storage Devices

Storage devices can be broadly classified into two categories:

- Block Storage Devices
- File Storage Devices

Block Storage Devices

The **block storage devices** offer raw storage to the clients. These raw storage are partitioned to create volumes.

File Storage Devices

The **file Storage Devices** offer storage to clients in the form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

Cloud Storage Classes

Cloud storage can be broadly classified into two categories:

- Unmanaged Cloud Storage
- Managed Cloud Storage

Unmanaged Cloud Storage

Unmanaged cloud storage means the storage is preconfigured for the customer. The customer can neither format, nor install his own file system or change drive properties.

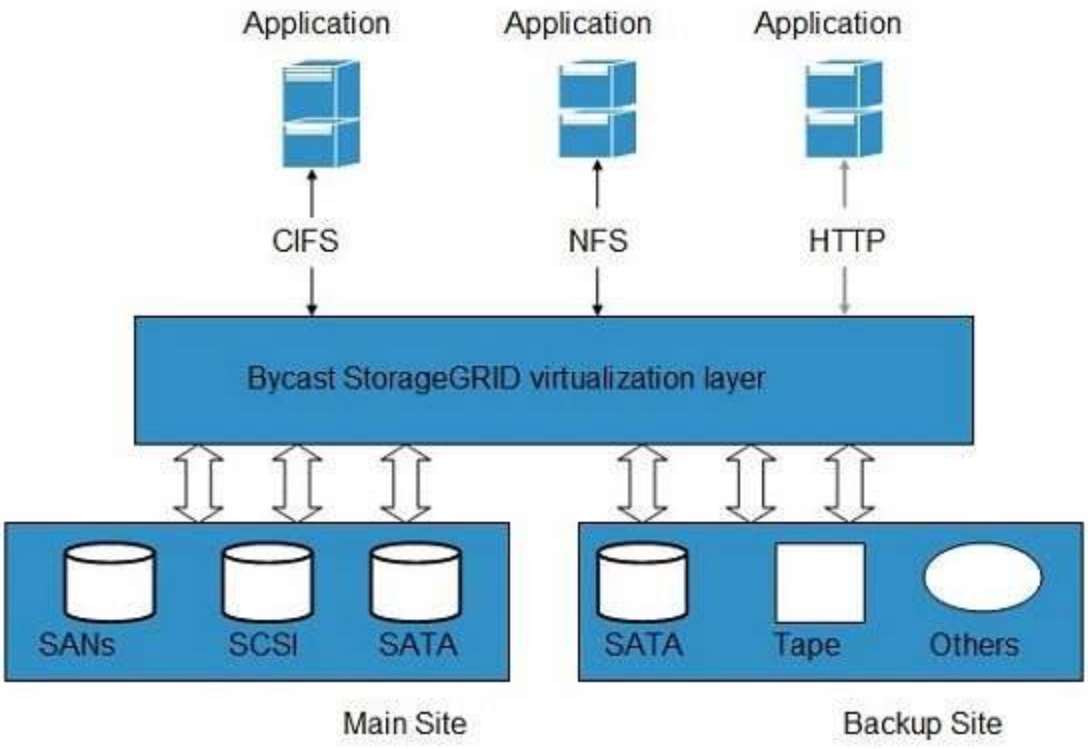
Managed Cloud Storage

Managed cloud storage offers online storage space on-demand. The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

Creating Cloud Storage System

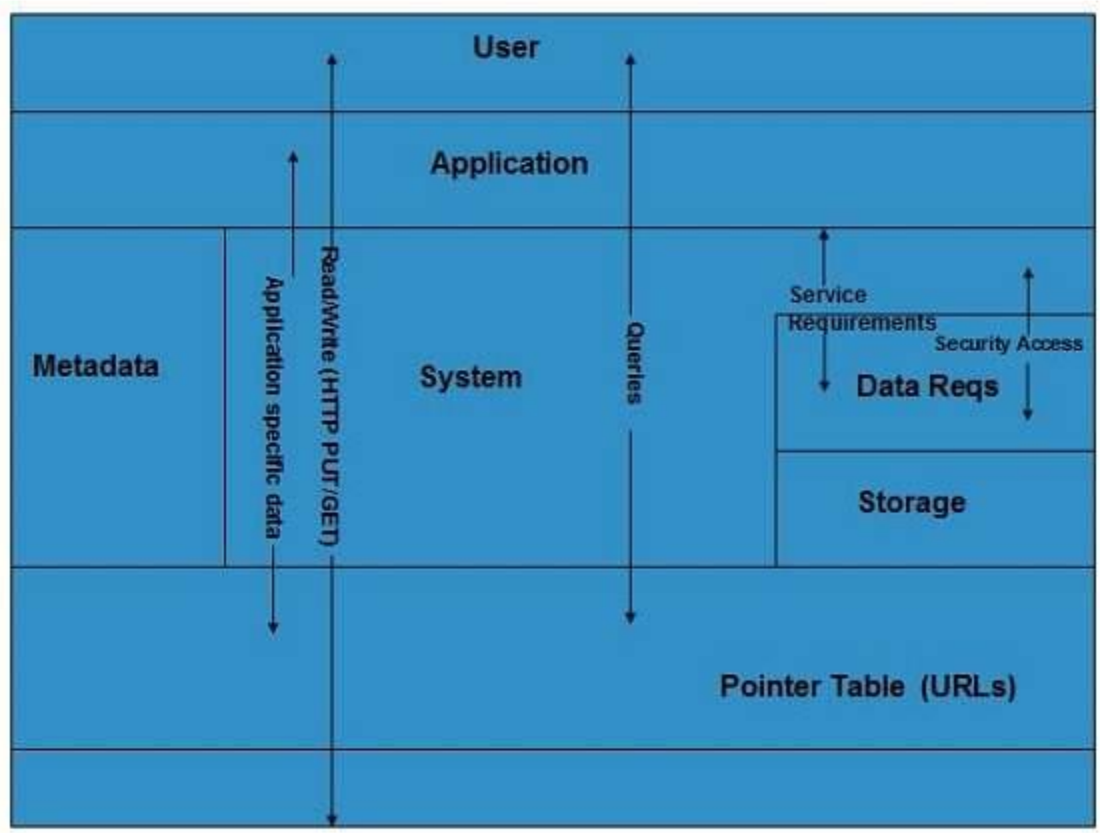
The cloud storage system stores multiple copies of data on multiple servers, at multiple locations. If one system fails, then it is required only to change the pointer to the location, where the object is stored.

To aggregate the storage assets into cloud storage systems, the cloud provider can use storage virtualization software known as **StorageGRID.** It creates a virtualization layer that fetches storage from different storage devices into a single management system. It can also manage data from **CIFS** and **NFS** file systems over the Internet. The following diagram shows how StorageGRID virtualizes the storage into storage clouds:



Virtual Storage Containers

The **virtual storage containers** offer high performance cloud storage systems. **Logical Unit Number (LUN)** of device, files and other objects are created in virtual storage containers. Following diagram shows a virtual storage container, defining a cloud storage domain:



Challenges

Storing the data in cloud is not that simple task. Apart from its flexibility and convenience, it also has several challenges faced by the customers. The customers must be able to:

- Get provision for additional storage on-demand.
- Know and restrict the physical location of the stored data.
- Verify how data was erased.
- Have access to a documented process for disposing of data storage hardware.
- Have administrator access control over data.

Cloud 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 so by **assigning a logical name** to a physical resource and providing a **pointer to that physical resource** on demand.

Virtualization Concept

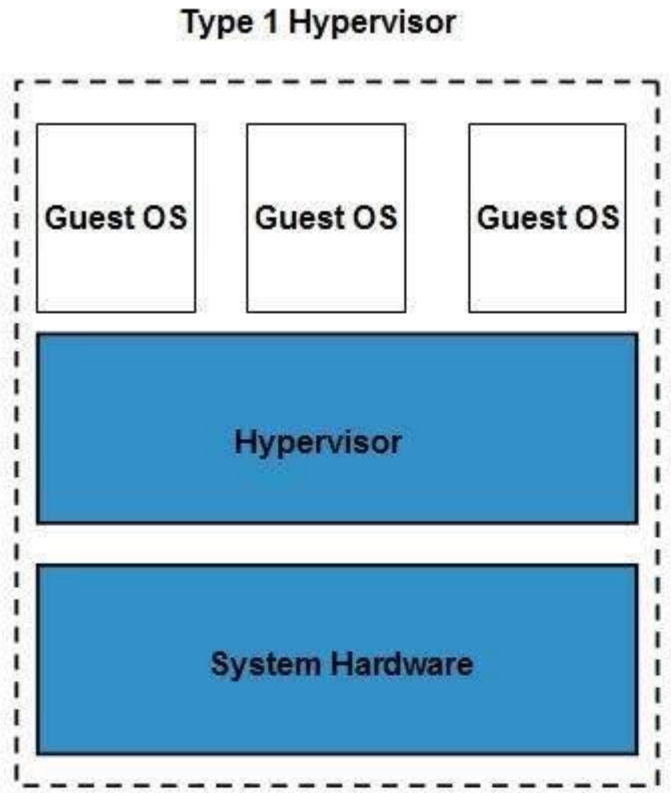
Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is created is known as **host machine** and **virtual machine** is referred as a **guest machine.** This virtual machine is managed by a software or firmware, which is known as **hypervisor.**

Hypervisor

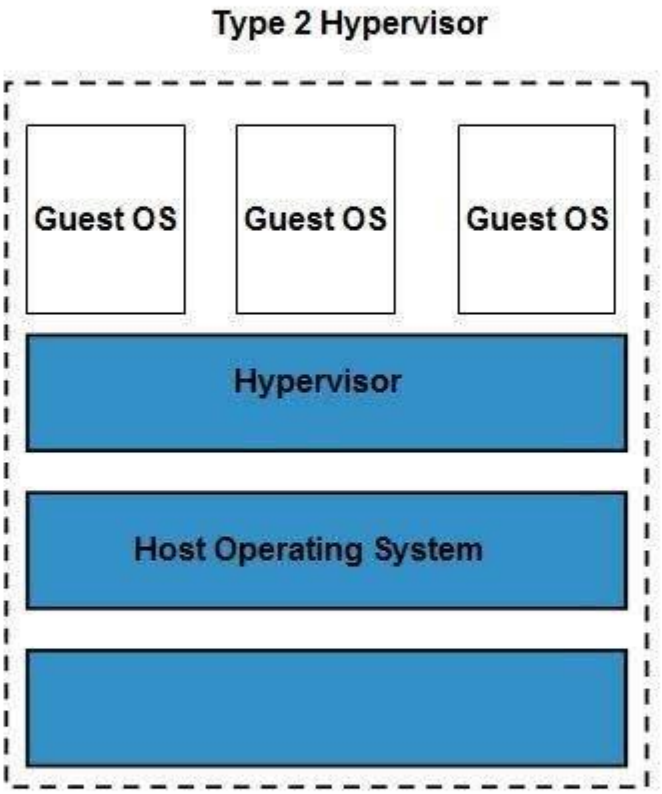
The **hypervisor** is a firmware or low-level program that acts as a Virtual Machine Manager. There are two types of hypervisor:

Type 1 hypervisor executes on bare system. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogic VLX are examples of Type 1 hypervisor. The following diagram shows the Type 1 hypervisor.



The **type1 hypervisor** does not have any host operating system because they are installed on a bare system.

Type 2 hypervisor is a software interface that emulates the devices with which a system normally interacts. Containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC and **VMWare workstation 6.0** are examples of Type 2 hypervisor. The following diagram shows the Type 2 hypervisor.



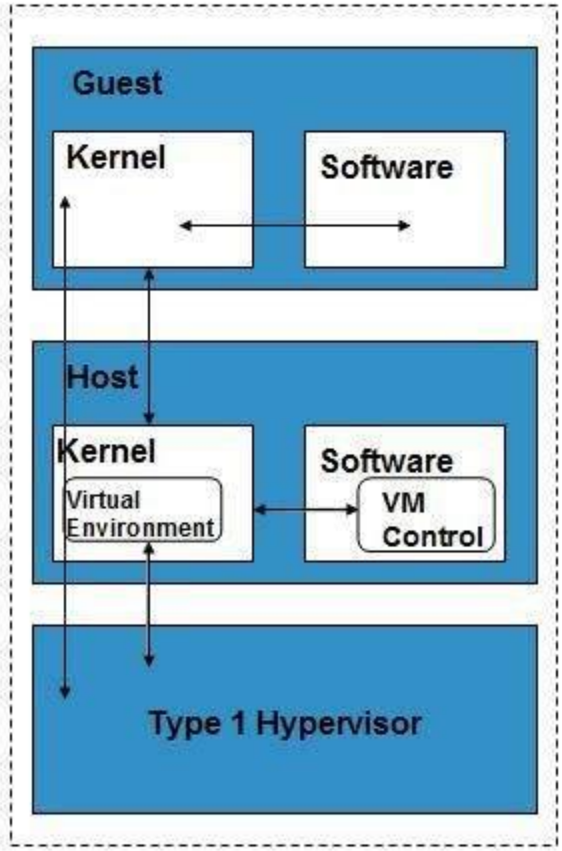
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

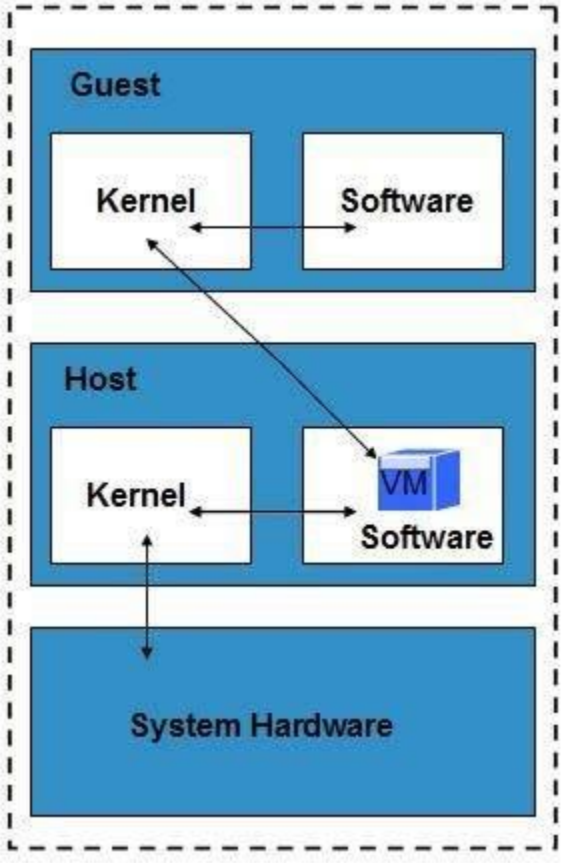
Full Virtualization

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



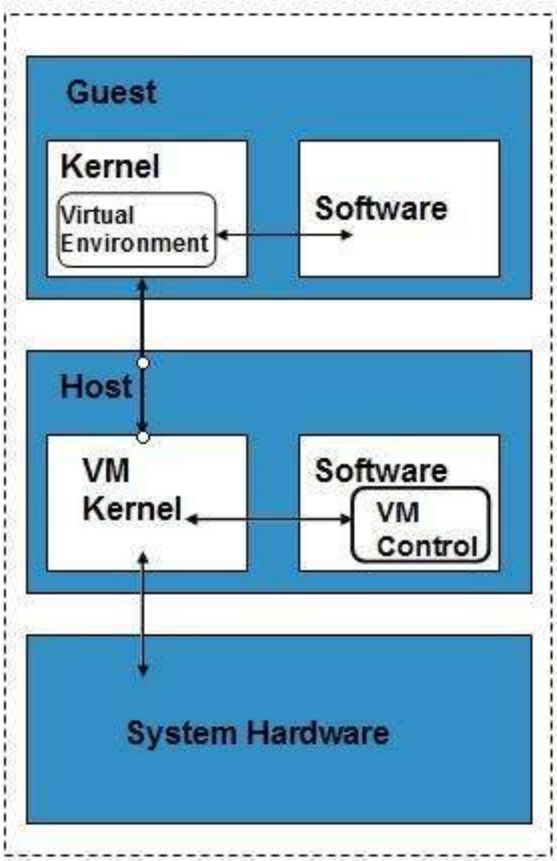
Emulation Virtualization

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.



VMware vSphere is highly developed infrastructure that offers a management infrastructure framework for virtualization. It virtualizes the system, storage and networking hardware.

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:

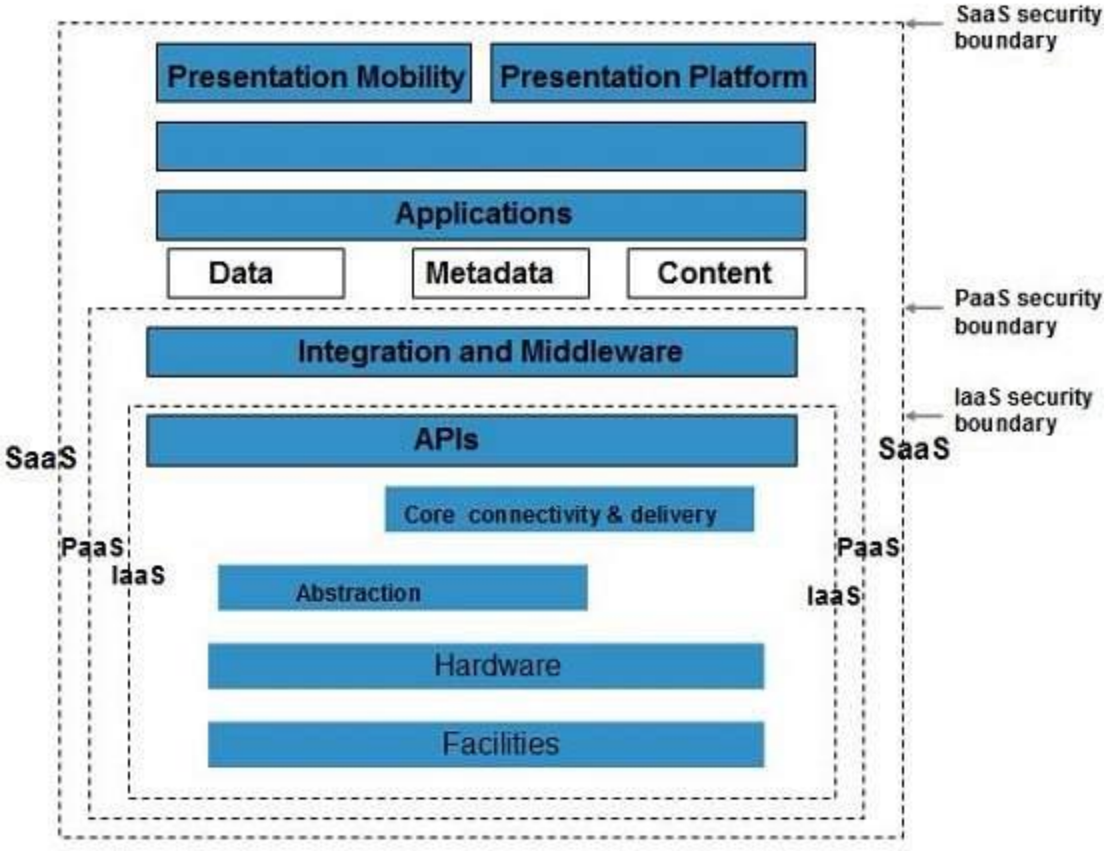
- Select resource that needs to move to the cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS,** and **SaaS.** These models require customer to be responsible for security at different levels of service.
- Consider the cloud type to be used such as **public, 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 Security of Cloud

Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and customer. **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the **CSA stack model:**



Key Points to CSA Model

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
- Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

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:

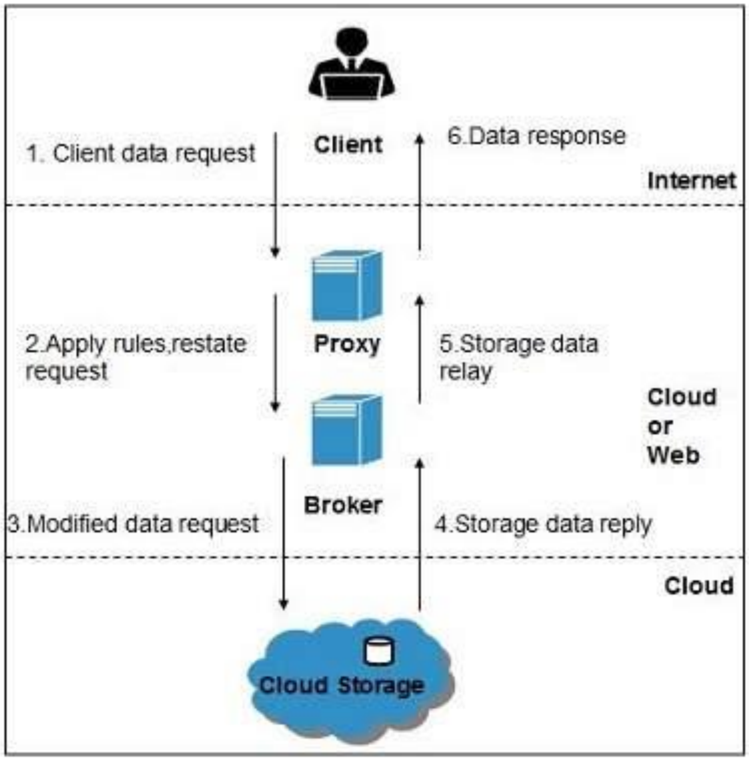
- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

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:



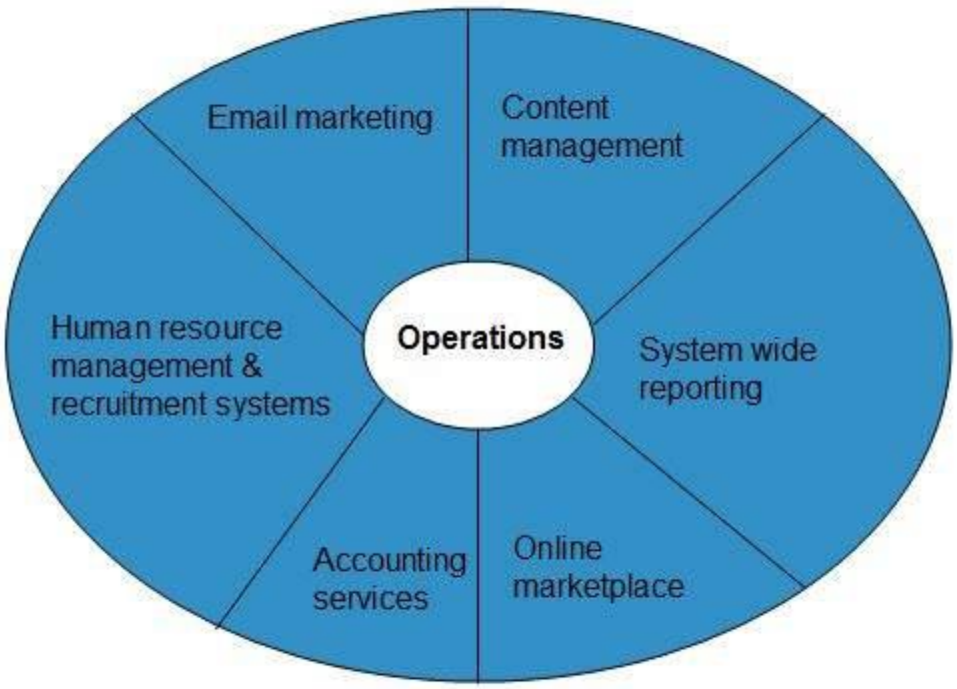
Encryption

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 Computing Operations

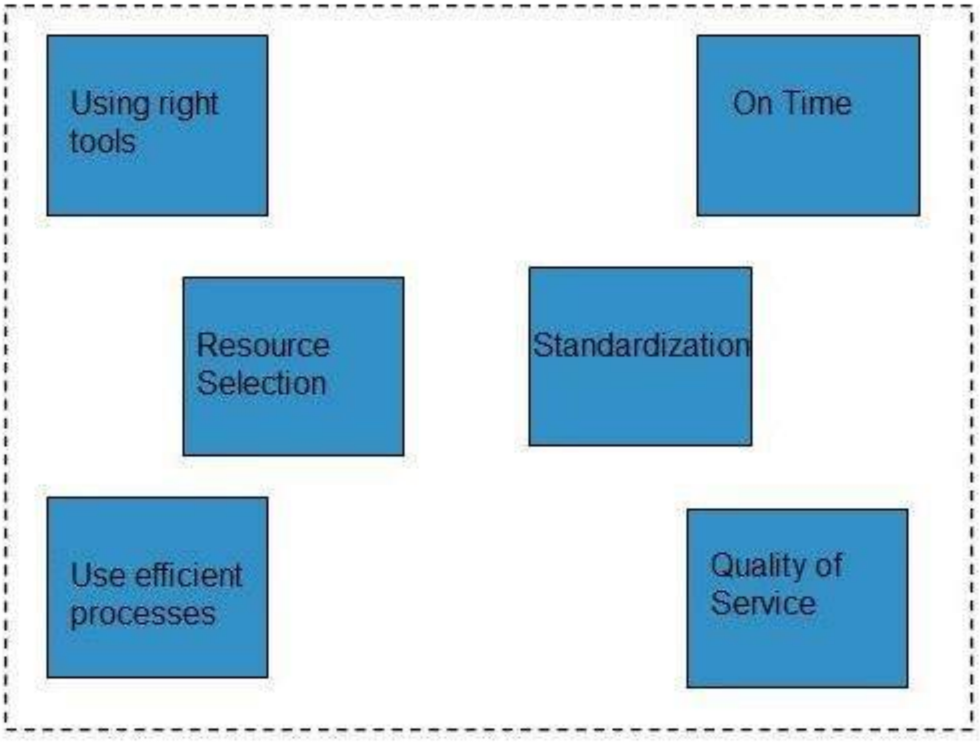
Cloud computing operation refers to delivering superior cloud service. Today, cloud computing operations have become very popular and widely employed by many of the organizations just because it allows to perform all business operations over the Internet.

These operations can be performed using a web application or mobile based applications. There are a number of operations performed in cloud. Some of them are shown in the following diagram:



Managing Cloud Operations

There are several ways to manage day-to-day cloud operations, as shown in the following diagram:



- Always employ right tools and resources to perform any function in the cloud.
- Things should be done at right time and at right cost.
- Selecting an appropriate resource is mandatory for operation management.
- The process should be standardized and automated to manage repetitive tasks.
- Using efficient process will eliminate the waste of efforts and redundancy.
- One should maintain the quality of service to avoid re-work later.

Cloud Computing Applications

Cloud Computing has its applications in almost all the fields such as business, entertainment, data storage, social networking, management, entertainment, education, art and **global positioning system,** etc. Some of the widely famous cloud computing applications are discussed here in this tutorial:

Business Applications

Cloud computing has made businesses more collaborative and easy by incorporating various apps such as **MailChimp, Chatter, Google Apps for business,** and **Quickbooks.**

SN	Application Description
1	**MailChimp** It offers an **e-mail publishing platform.** It is widely employed by the businesses to design and send their e-mail campaigns.
2	**Chatter** **Chatter app** helps the employee to share important information about organization in real time. One can get the instant feed regarding any issue.
3	**Google Apps for Business** **Google** offers **creating text documents, spreadsheets, presentations,** etc., on **Google Docs** which allows the business users to share them in collaborating manner.
4	**Quickbooks** It offers **online accounting solutions** for a business. It helps in **monitoring cash flow, creating VAT returns** and **creating business reports.**

Data Storage and Backup

Box.com, Mozy, Joukuu are the applications offering data storage and backup services in cloud.

SN	Application Description

1	**Box.com** **Box.com** offers drag and drop service for files. The users need to drop the files into Box and access from anywhere.
2	**Mozy** **Mozy** offers online backup service for files to prevent data loss.
3	**Joukuu** **Joukuu** is a web-based interface. It allows to display a single list of contents for files stored in **Google Docs, Box.net and Dropbox.**

Management Applications

There are apps available for management task such as **time tracking, organizing notes.** Applications performing such tasks are discussed below:

SN	Application Description
1	**Toggl** It helps in tracking time period assigned to a particular project.
2	**Evernote** It organizes the sticky notes and even can read the text from images which helps the user to locate the notes easily.
3	**Outright** It is an accounting app. It helps to track income, expenses, profits and losses in real time.

Social Applications

There are several social networking services providing websites such as Facebook, Twitter, etc.

SN	Application Description
1	**Facebook** It **offers** social networking service. One can share photos, videos, files, status and much more.
2	**Twitter** It **helps** to interact with the public directly. One can follow any celebrity, organization and any person, who is on twitter and can have latest updates regarding the same.

Entertainment Applications

SN	Application Description
1	**Audio box.fm** It offers streaming service. The music files are stored online and can be played from cloud using the own media player of the service.

Art Applications

SN	Application Description
1	**Moo** It offers art services such as designing and printing **business cards, postcards** and **mini cards.**

Cloud Computing Providers

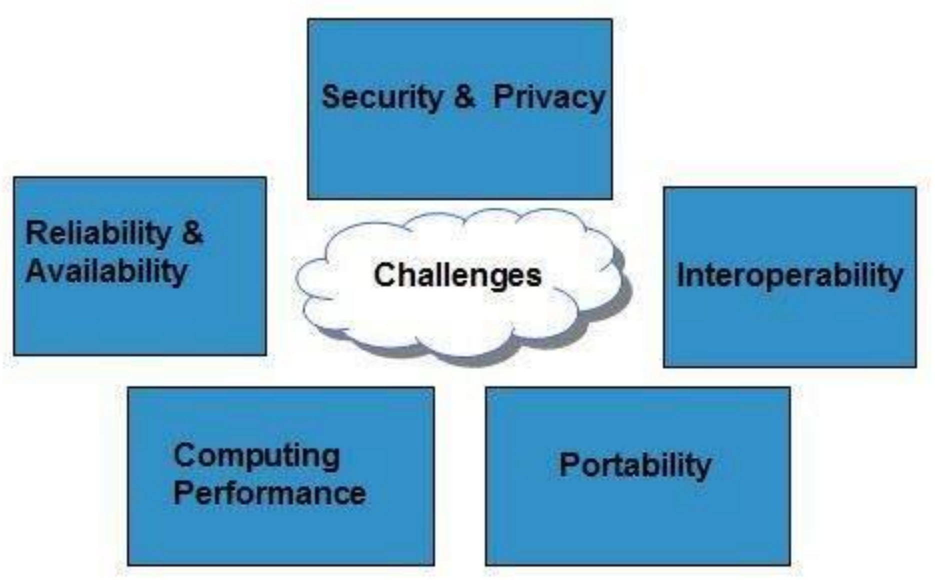
Various Cloud Computing platforms are available today. The following table contains the popular Cloud Computing platforms:

SN	Platform Description
1	**Salesforce.com** This is a Force.com development platform. This provides a simple user interface and lets users log in, build an app, and push it in the cloud.
2	**Appistry** The Appistry's CloudIQ platform is efficient in delivering a runtime application. This platform is very useful to create scalable and service oriented applications.
3	**AppScale** The AppScale is an open source platform for App Engine of Google applications.
4	**AT&T** The AT&T allows access to virtual servers and manages the virtualization infrastructure. This virtualization infrastructure includes network, server and storage.
5	**Engine Yard** The Engine Yard is a rails application on cloud computing platform.
6	**Enomaly** Enomaly provides the Infrastructure-as-a-Service platform.
7	**FlexiScale** The FlexiScale offers a cloud computing platform that allows flexible, scalable and automated cloud infrastructure.
8	**GCloud3**

	The GCloud3 offers private cloud solution in its platform.
9	**Gizmox** The Gizmox Visual WebGUI platform is best suited for developing new web apps and modernize the legacy apps based on ASP.net, DHTML, etc.
10	**GoGrid** The GoGrid platform allows the users to deploy web and database cloud services.
11	**Google** The Google's App Engine lets the users build, run and maintain their applications on Google infrastructure.
12	**LongJump** The LongJump offers a business application platform, a Platform-as-a-Service (PaaS).
13	**Microsoft** The Microsoft Windows Azure is a cloud computing platform offering an environment to create cloud apps and services.
14	**OrangeScape** OrangeScape offers a Platform-as-a-Service (Paas) for non-programmers. Building an app is as easy as spreadsheet.
15	**RackSpace** The RackSpace provides servers-on-demand via a cloud-driven platform of virtualized servers.
16	**Amazon EC2** The Amazon EC2 (Elastic Compute Cloud) lets the users configure and control computing resources while running them on Amazon environment.

Cloud Computing Challenges

Cloud computing, an emergent technology, has placed many challenges in different aspects of data and information handling. Some of these are shown in the following diagram:



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.

Mobile Cloud Computing

Cloud Computing offers such smartphones that have rich Internet media support, require less processing and consume less power. In terms of Mobile Cloud Computing (MCC), processing is done in cloud, data is stored in cloud, and the mobile devices serve as media for display.

Today smartphones are employed with rich cloud services by integrating applications that consume web services. These web services are deployed in cloud.

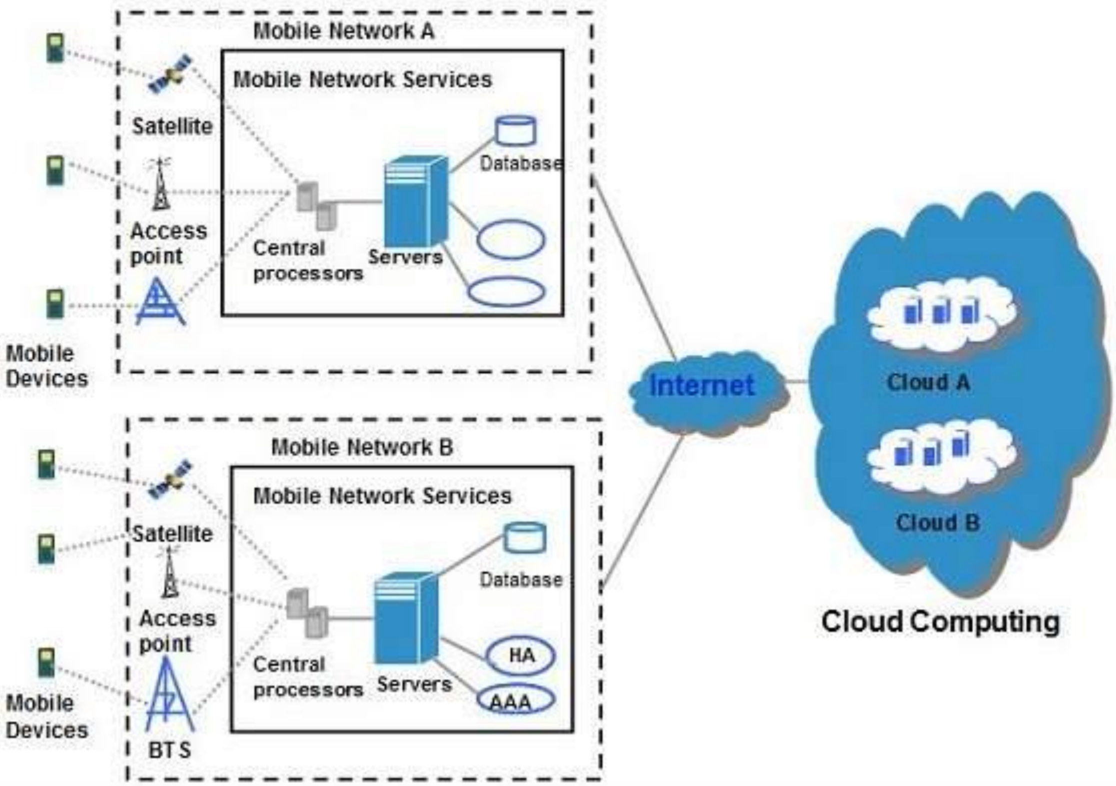
There are several Smartphone operating systems available such as Google's Android, Apple's iOS, RIM BlackBerry, Symbian, and Windows Mobile Phone. Each of these platforms support third-party applications that are deployed in cloud.

Architecture

MCC includes four types of cloud resources:

- Distant mobile cloud
- Distant immobile cloud
- Proximate mobile computing entities
- Proximate immobile computing entities
- Hybrid

The following diagram shows the framework for mobile cloud computing architecture:



Issues

Despite of having significant development in field of mobile cloud computing, still many issues remain unsorted such as:

Emergency Efficient Transmission

There should be a frequent transmission of information between cloud and the mobile devices.

Architectural Issues

Mobile cloud computing is required to make architectural neutral because of heterogeneous environment.

Live VM Migration

It is challenging to migrate an application, which is resource-intensive to cloud and to execute it via Virtual Machine.

Mobile Communication Congestion

Due to continuous increase in demand for mobile cloud services, the workload to enable smooth communication between cloud and mobile devices has been increased.

Security and Privacy

This is one of the major issues because mobile users share their personal information over the cloud.