CHAPTER

1

Cloud Computing - Overview

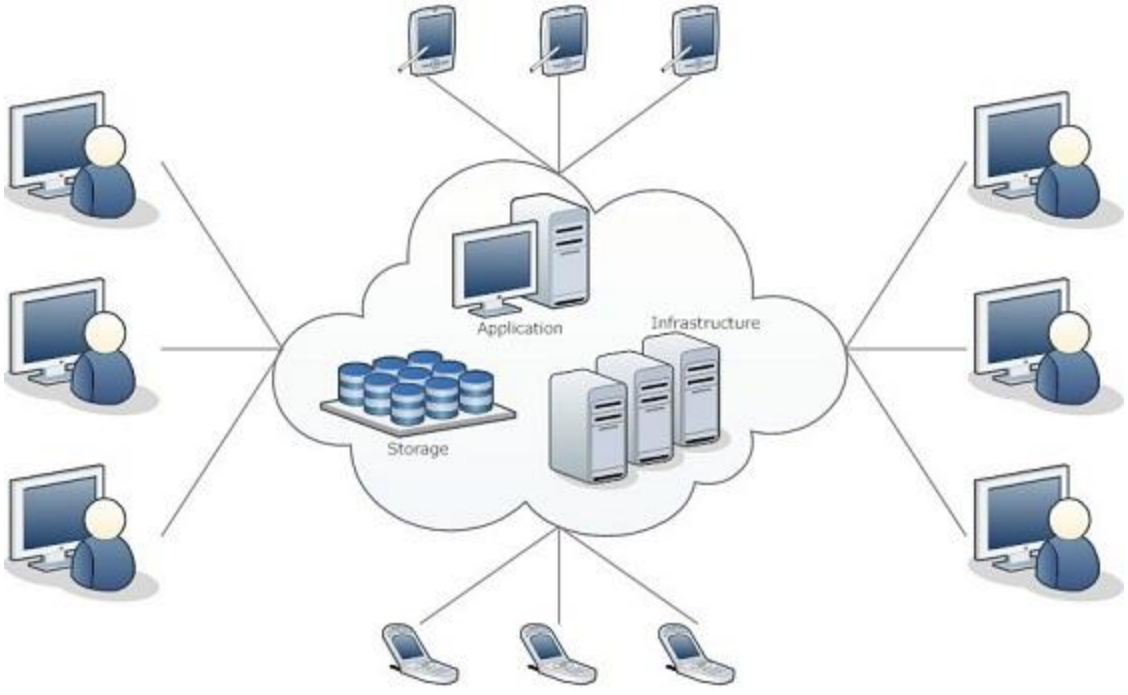
Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online.

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 network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN.
Applications such as **e-mail, web conferencing, customer relationship management (CRM),**all run in cloud.

What is Cloud Computing?

Cloud Computing refers to **manipulating, configuring,** and **accessing** the applications online. It offers online data storage, infrastructure and application.



We need not to install a piece of software on our local PC and this is how the cloud computing overcomes **platform dependency issues**. Hence, the Cloud Computing is making our business application **mobile** and **collaborative**.

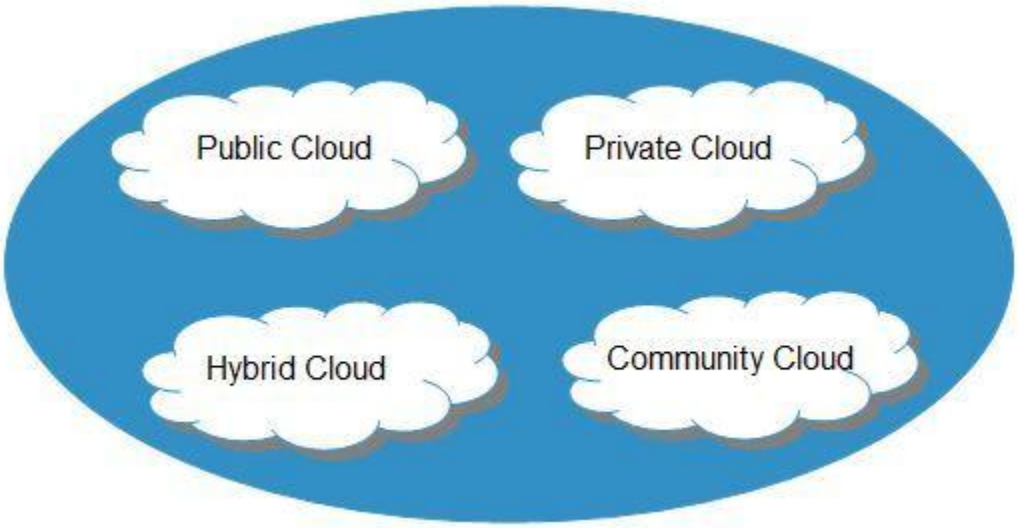
Basic Concepts

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, e.g., e-mail.

PRIVATE CLOUD

The **Private Cloud** allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

COMMUNITY CLOUD

The **Community Cloud** allows systems and services to be accessible by group of organizations.

HYBRID CLOUD

The **Hybrid Cloud** is mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

SERVICE MODELS

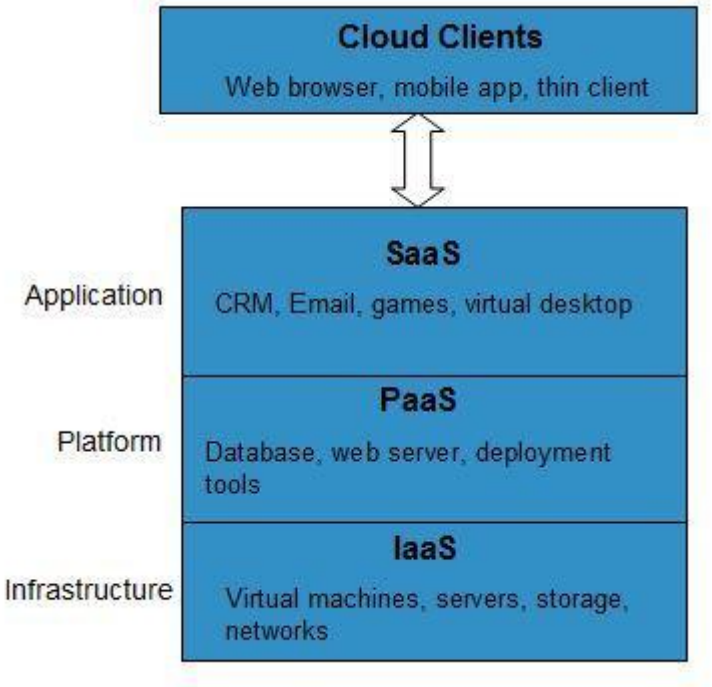
Service Models are the reference models on which the Cloud Computing is based. These can be categorized into three basic service models as listed below:

1. Infrastructure as a Service (IaaS)

2. Platform as a Service (PaaS)

3. Software as a Service (SaaS)

There are many other service models all of which can take the form like **XaaS**, i.e., **Anything as a Service**. This can be **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 make use of the underlying service model, i.e., each inherits the security and management mechanism from the underlying model, as shown in the following diagram:



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)

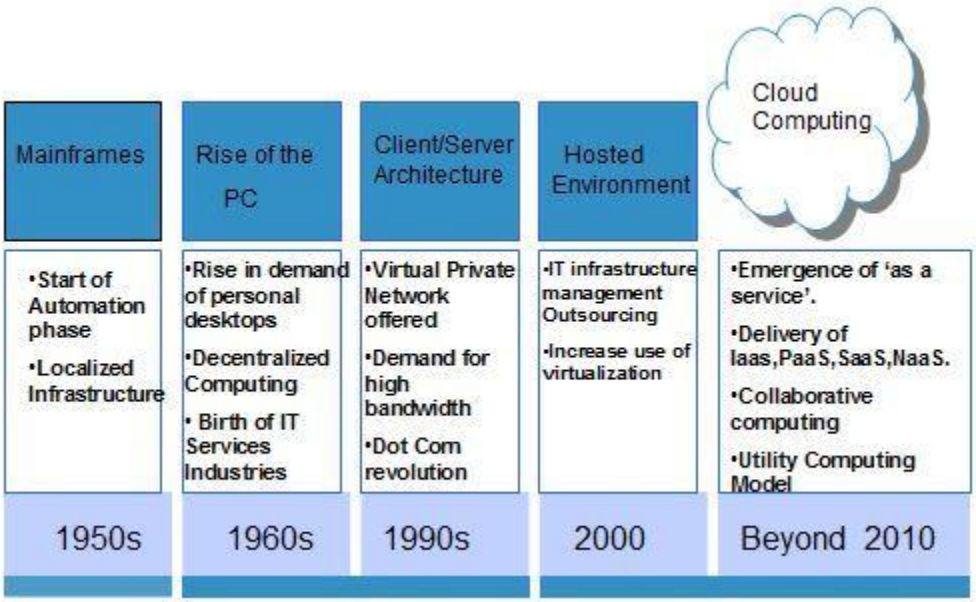
PaaS provides the runtime environment for applications, development & deployment tools, etc.

SOFTWARE AS A SERVICE (SAAS)

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

History

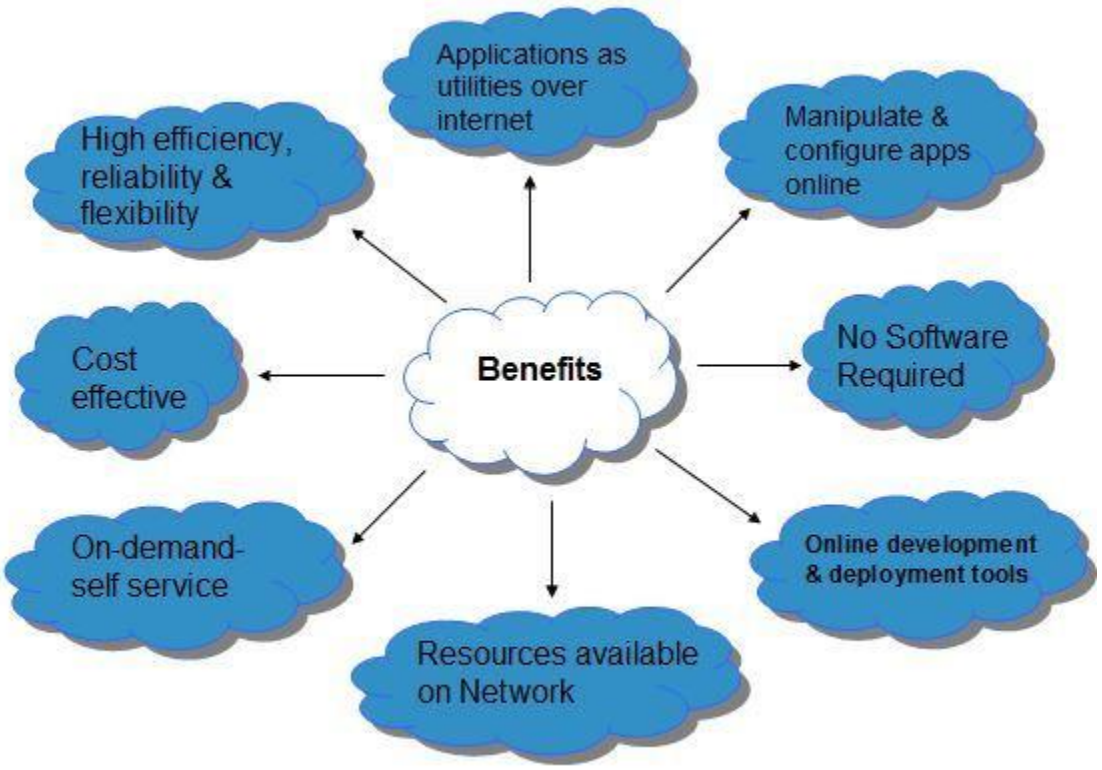
The concept of **Cloud Computing** came into existence in 1950 with implementation of mainframe computers, accessible via **thin/static clients**. Since then, cloud computing has been evolved from static clients to dynamic ones from software to services. The following diagram explains the evolution of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



Benefits

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

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through **Platform as a Service model**.
- Cloud resources are available over the network in a manner that provides 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 higher efficiencies with greater utilization. It just requires an Internet connection.
- Cloud Computing offers load balancing that makes it more reliable.



Risks

Although Cloud Computing is a great innovation in the world of computing, there also exist downsides of cloud computing. Some of them are discussed below:

SECURITY & 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 such providers.

Although the cloud computing vendors ensure more secure password protected accounts, any sign of security breach would result in loss of clients 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, routing between the different tenants.

MANAGEMENT INTERFACE COMPROMISE

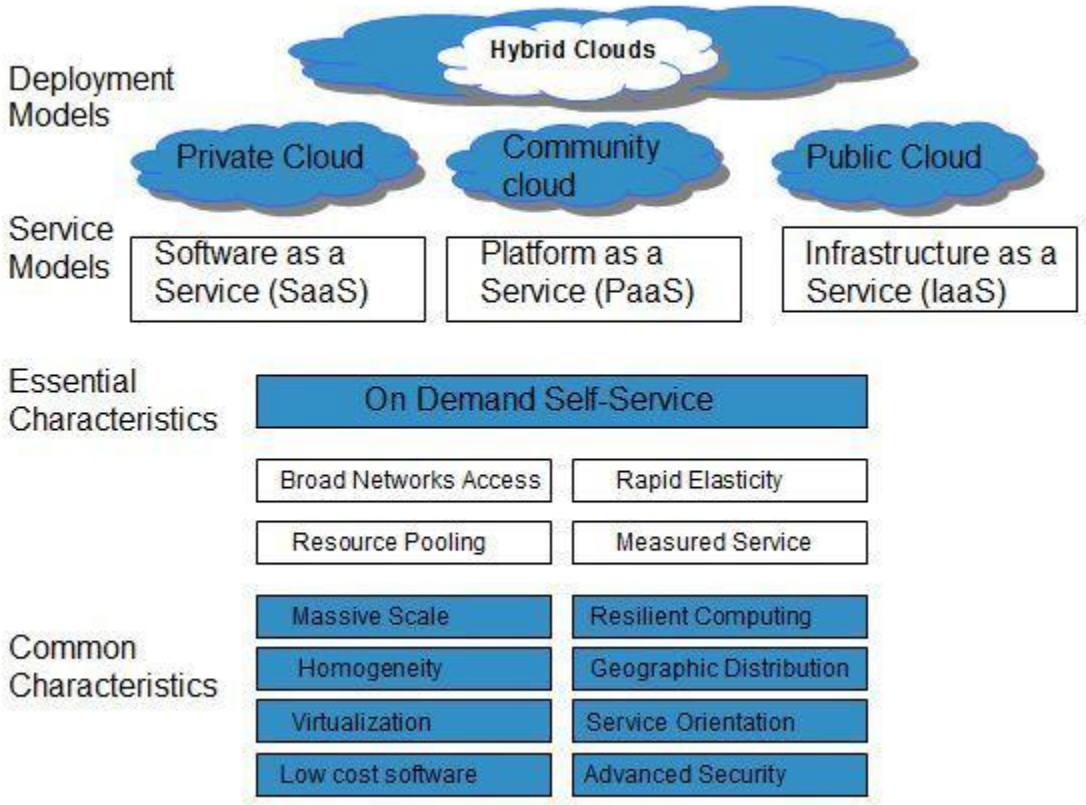
In case of public cloud provider, the customer management interfaces are accessible through the Internet.

INSECURE OR INCOMPLETE DATA DELETION

It is possible that the data requested for deletion may not get deleted. It happens either because extra copies of data are stored but are not available or disk destroyed also stores data from other tenants.

Characteristics

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 up or down the resources at any time.

Resources used by the customers or currently assigned to customers are automatically monitored and resources. It make it possible

MEASURED SERVICE

Service Models & Deployment Models are described in above section.

CHAPTER

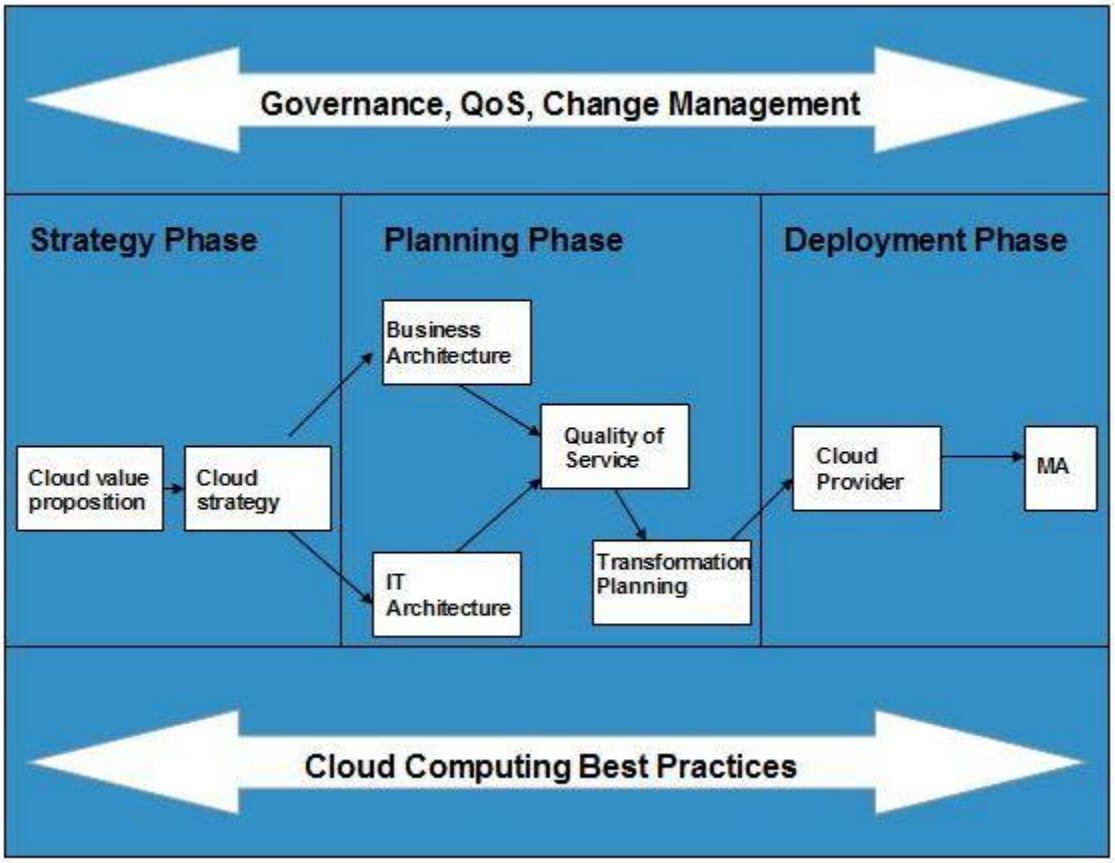
2

Cloud Computing - Planning

Beforedeploying applications to cloud, it is necessary to consider your business requirements. Following are the issues one must have to think about:

- 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. Here 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 Planning Phase

In this, 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.

Cloud Computing Tactics Planning Phase

This step performs analysis of problems and risks in the cloud application to ensure the customers that the cloud computing successfully meet 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.

Cloud Computing Deployment Phase

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

- Cloud Computing Provider
- Maintenance and Technical Service

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 must have to ensure the quality of services.

CHAPTER

3

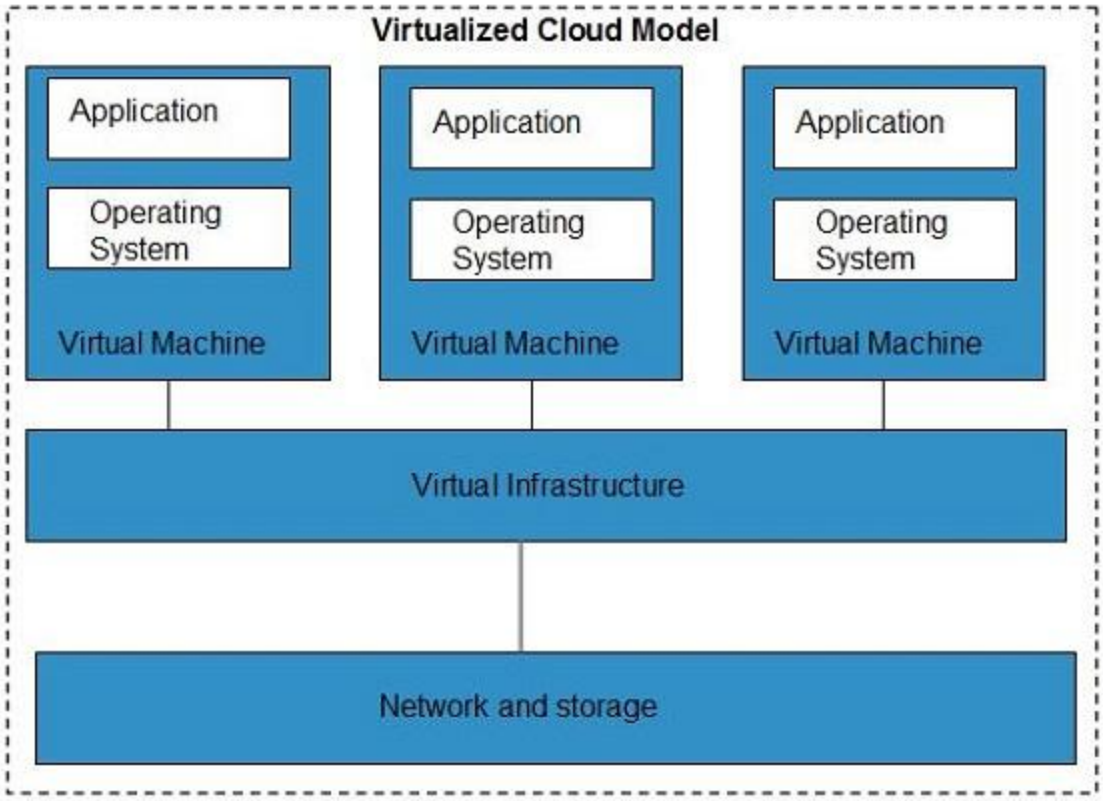
Cloud Computing-Technologies

Thereare certain technologies that are working behind the cloud computing platforms making cloud computing flexible, reliable, 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 so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

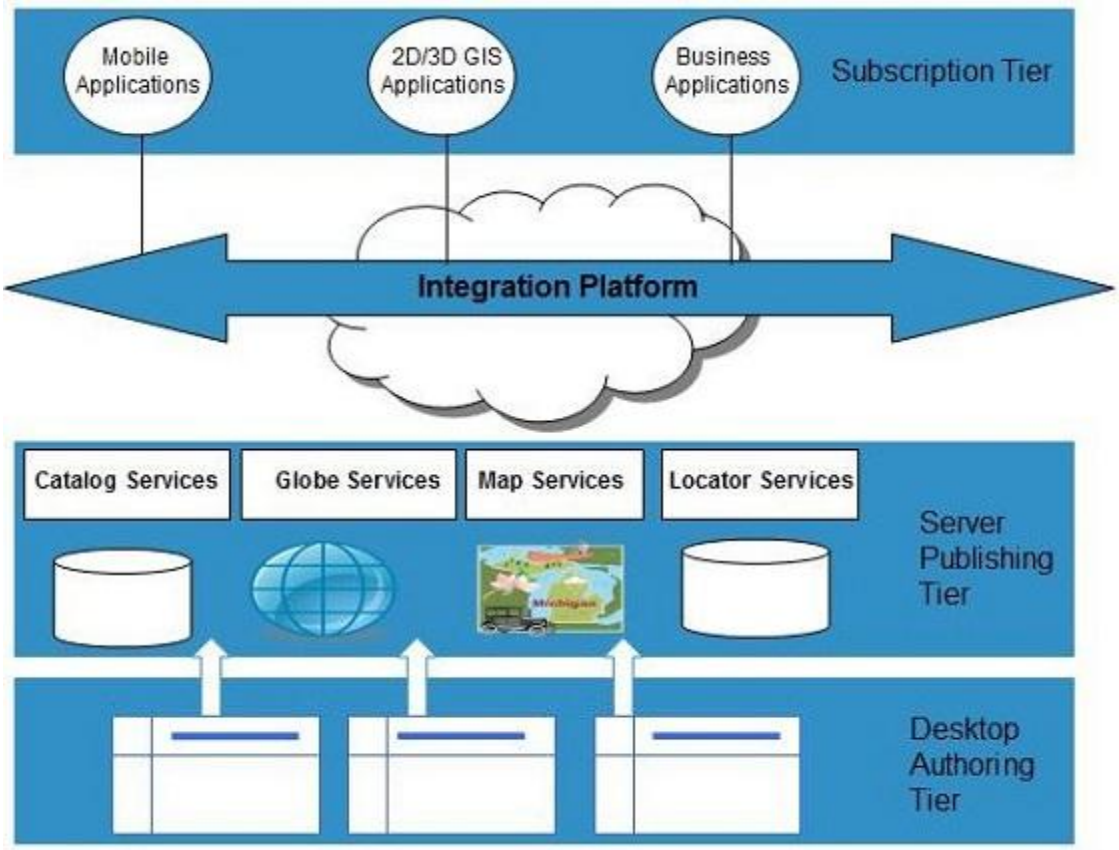


The **Multitenant** architecture offers **virtual isolation** among the multiple tenants and therefore the organizations can use and customize the application as though they each have its own instance running.

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

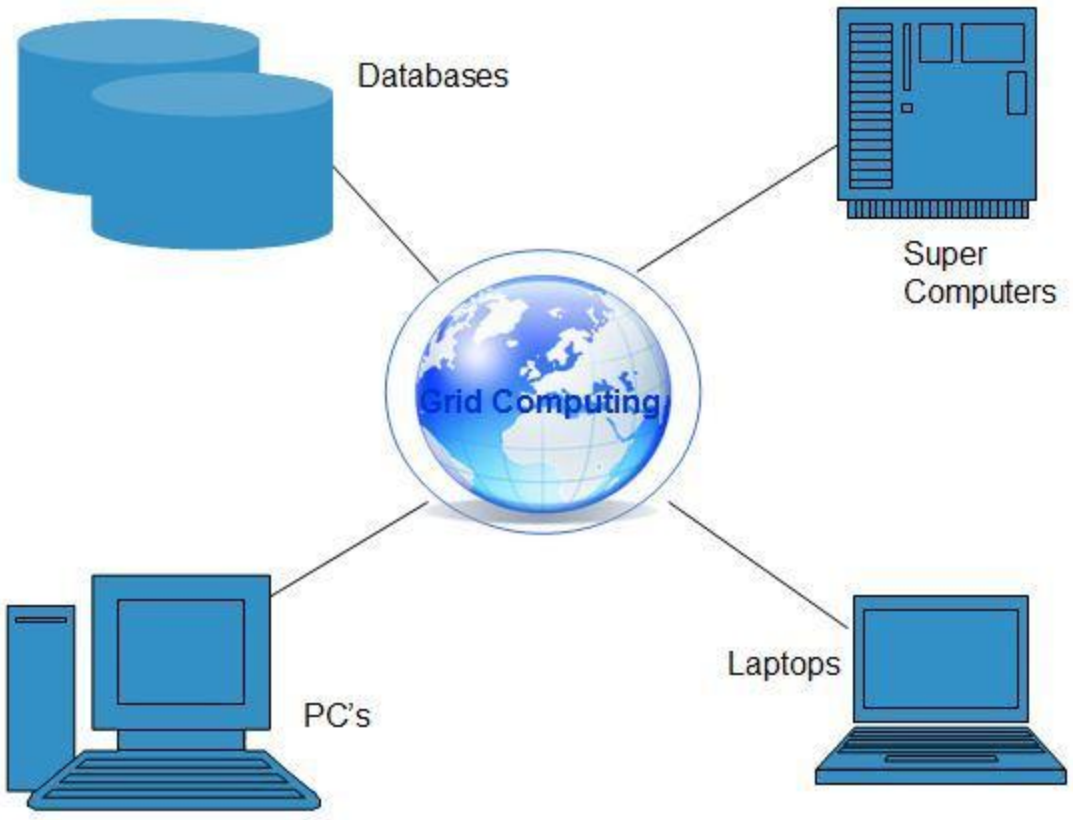
cloud_computing-service_oriented_architecture



Grid Computing

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

Grid Computing breaks complex task into smaller pieces. These smaller pieces 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.

CHAPTER

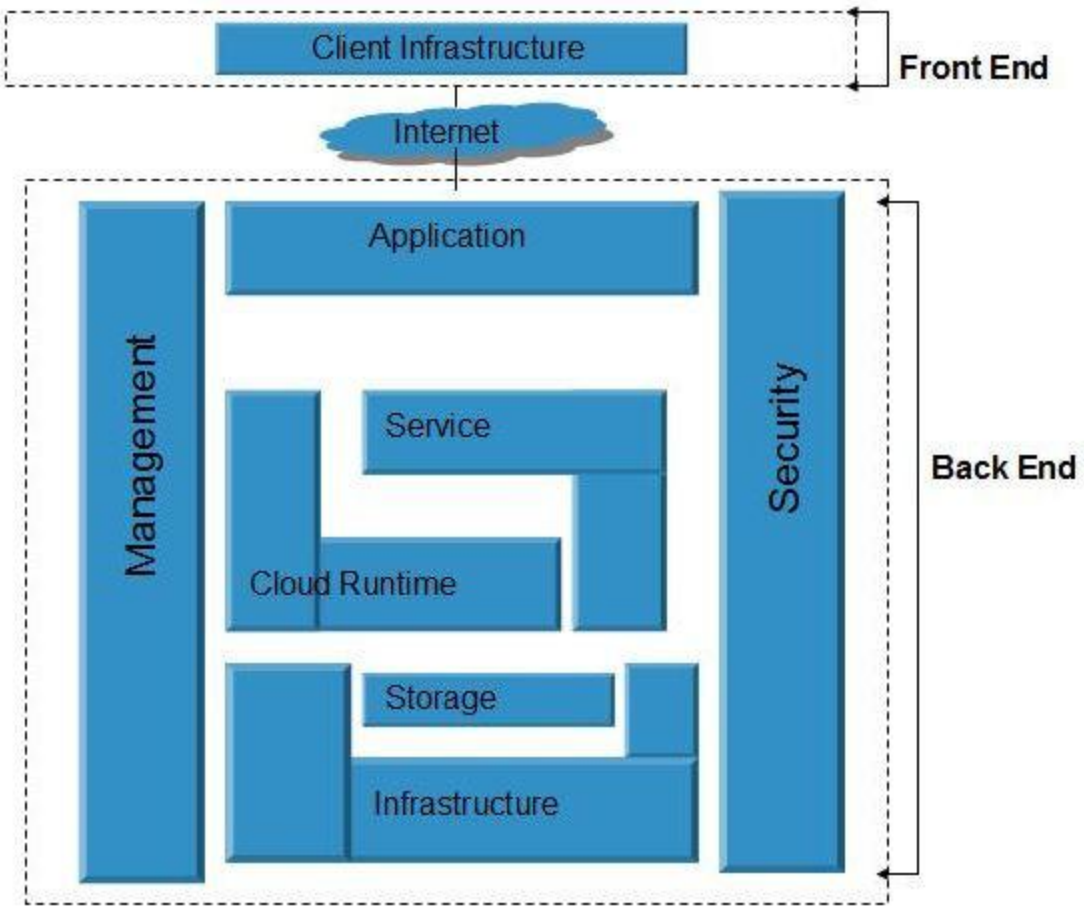
4

Cloud Computing-Architecture

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

- Front End
- Back End

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



FRONT END

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, e.g., Web Browser.

BACK END

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.

Important Points

- 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, helps the connected devices to communicate with each other.

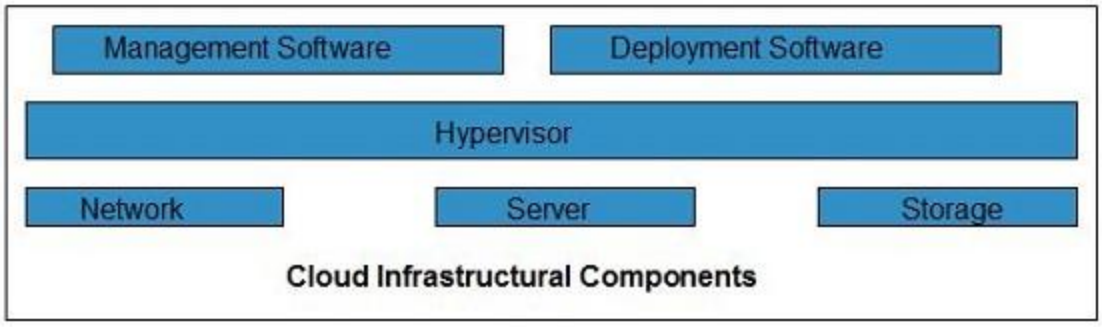
CHAPTER

5

Cloud Computing Infrastructure

Cloud Infrastructure Components

Cloud **infrastructure** consists of servers, storage, network, management software, and 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

Management Software helps to maintain and configure the infrastructure.

DEPLOYMENT SOFTWARE

Deployment software helps to deploy and integrate the application on the cloud.

NETWORK

Network 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, i.e., the consumer can customize the network route and protocol.

SERVER

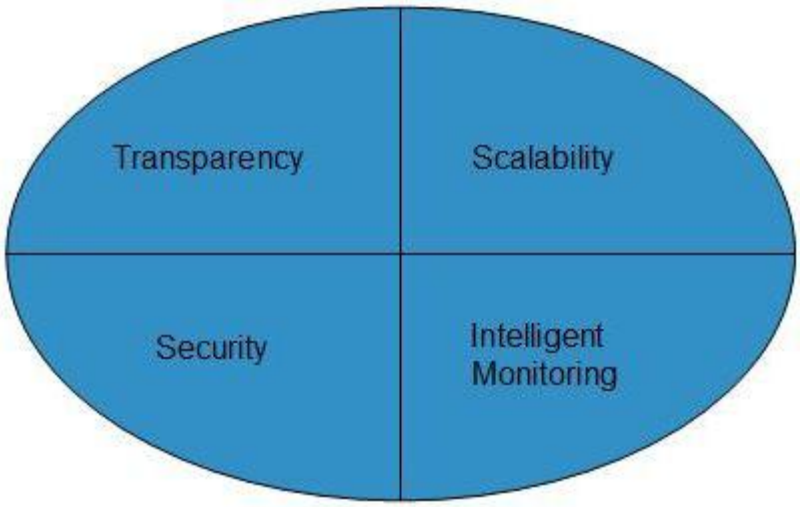
Server helps to compute the resource sharing and offer other services such as resource allocation and deallocation, monitoring resources, security, etc.

STORAGE

Cloud uses distributed file system for storage purpose. If one of the storage resource 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

Since 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, a entry point in mega data center also needs to be secure.

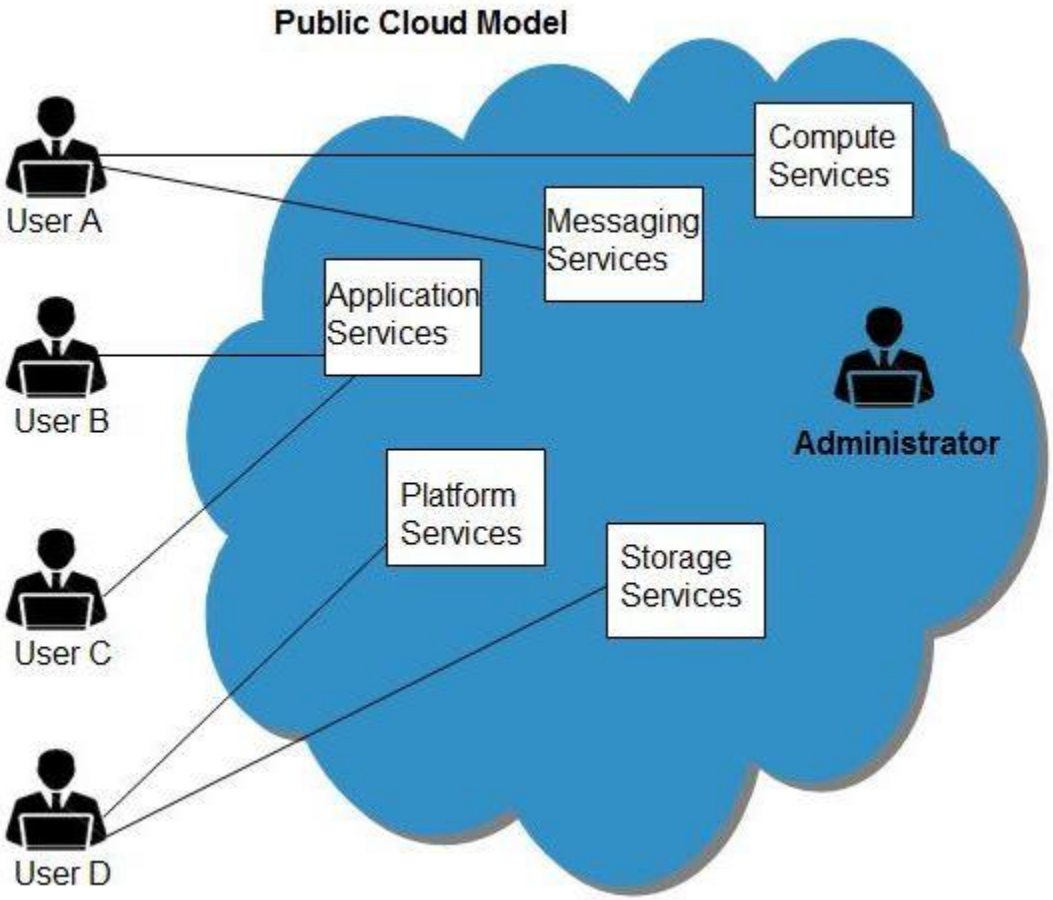
CHAPTER

6

Public Cloud Model

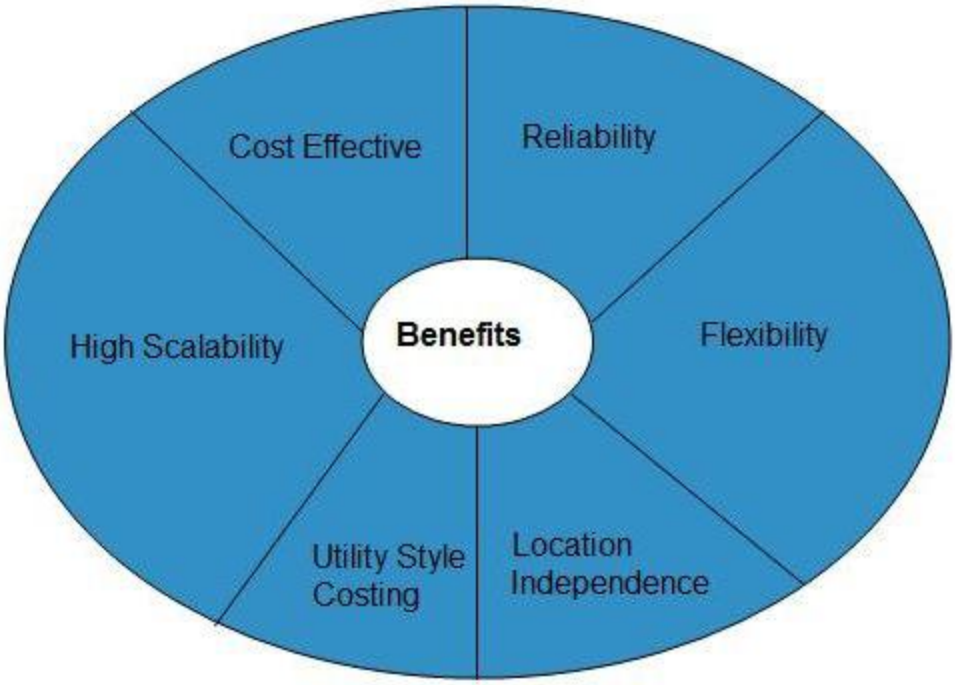
Public Cloud

The**Public Cloud** allows systems and services to be easily accessible to general public, e.g., **Google, Amazon, Microsoft** offers cloud services via Internet.



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** share same resources with large number of consumer, it has low cost.

RELIABILITY

Since **public cloud** employs large number of resources from different locations, if any of the resource fail, public cloud can employ another one.

FLEXIBILITY

It is also very easy to integrate public cloud with private cloud, hence gives consumers a flexible approach.

LOCATION INDEPENDENCE

Since, **public cloud** services are delivered through Internet, therefore ensures location independence.

UTILITY STYLE COSTING

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

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 the 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.

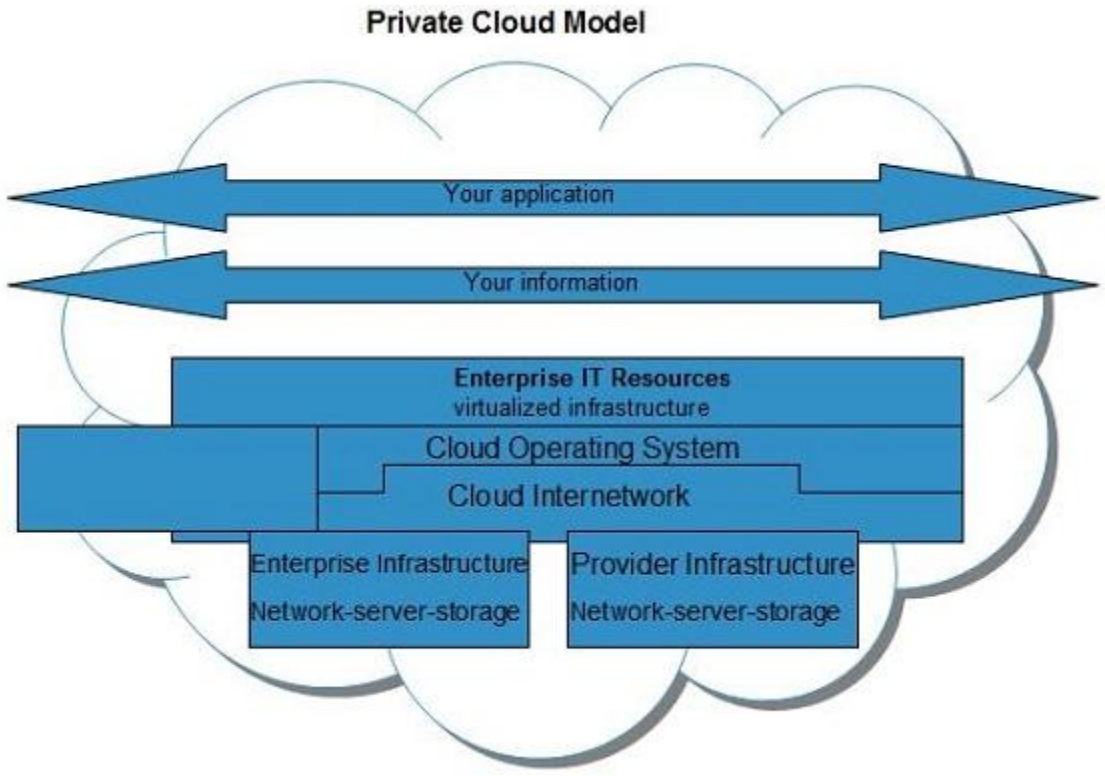
CHAPTER

7

Private Cloud Model

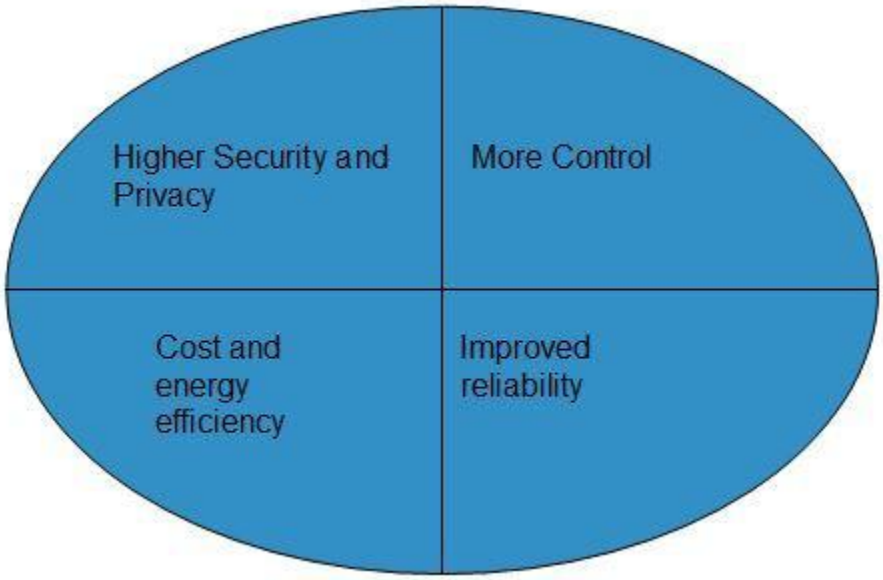
Private Cloud

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



Benefits

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



HIGHER SECURITY AND PRIVACY

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

MORE CONTROL

Private clouds have more control on its resources and hardware than public cloud because it is accessed only within an organization.

COST AND ENERGY EFFICIENCY

Private cloud resources are not as cost effective as public clouds but they offer more efficiency than public cloud.

Disadvantages

Here are the disadvantages of using private cloud model:

RESTRICTED AREA

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

INFLEXIBLE PRICING

In order to fulfill demand, purchasing new hardware is very costly.

LIMITED SCALABILITY

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

ADDITIONAL SKILLS

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

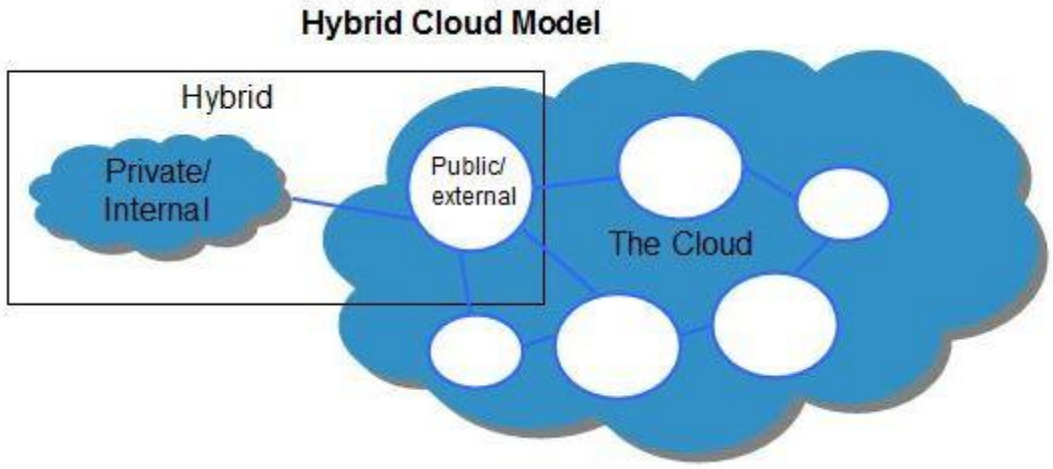
CHAPTER

8

Hybrid Cloud Model

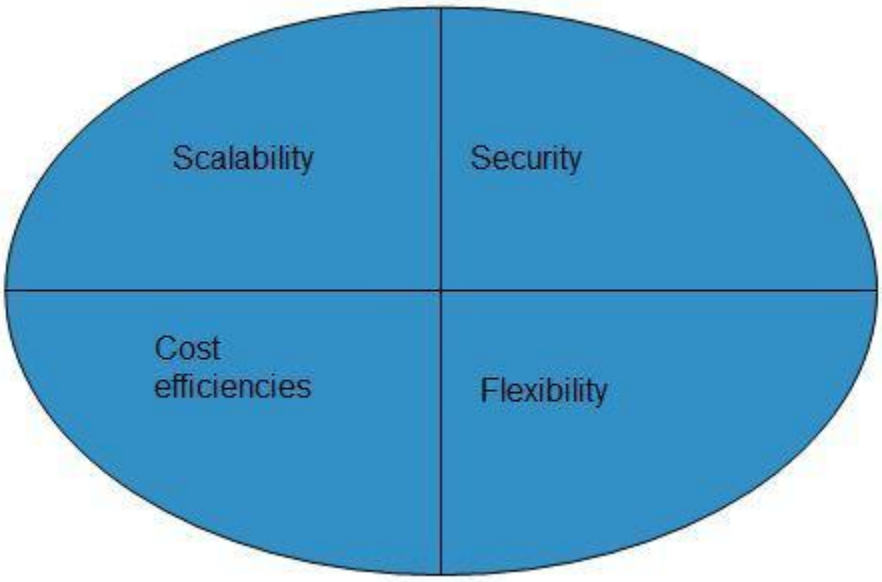
Hybrid Cloud

The**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.



Benefits

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



SCALABILITY

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

FLEXIBILITY

It offers both secure resources and scalable public resources.

COST EFFICIENCIES

Public cloud are more cost effective than private, therefore hybrid cloud can have this saving.

SECURITY

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 organization's security policies.

INFRASTRUCTURAL DEPENDENCY

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

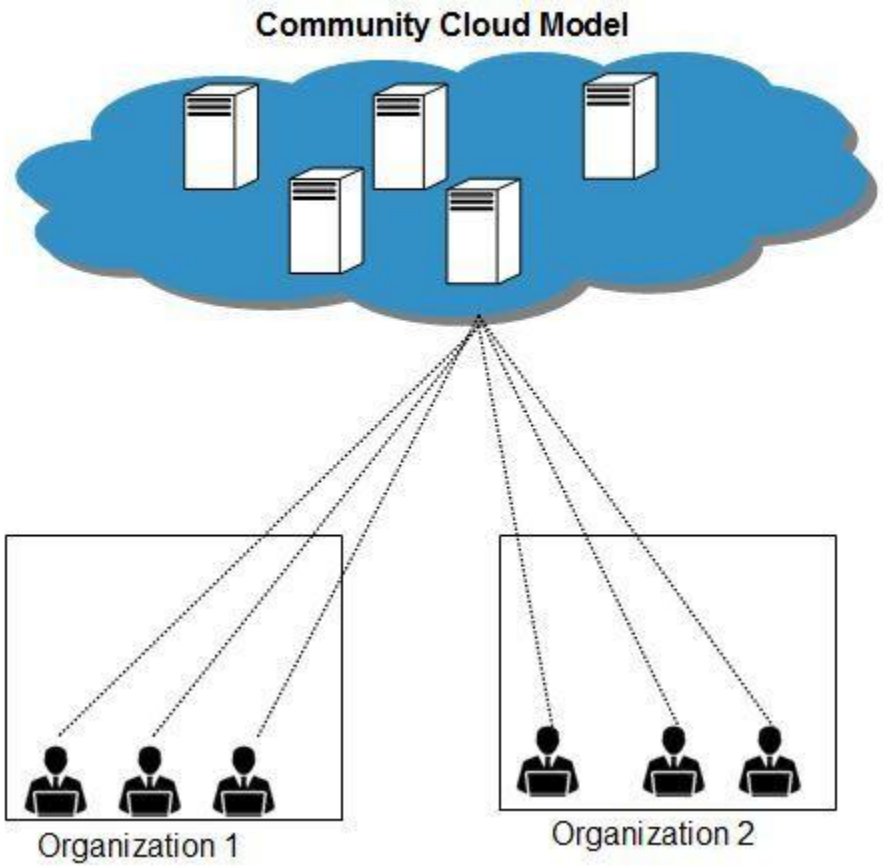
CHAPTER

9

Community Cloud Model

Community Cloud

The**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 or by the third-party.



Benefits

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

COST EFFECTIVE

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

Sharing Between Organizations

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

SECURITY

Community cloud is comparatively more secure than the public cloud.

ISSUES

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

CHAPTER

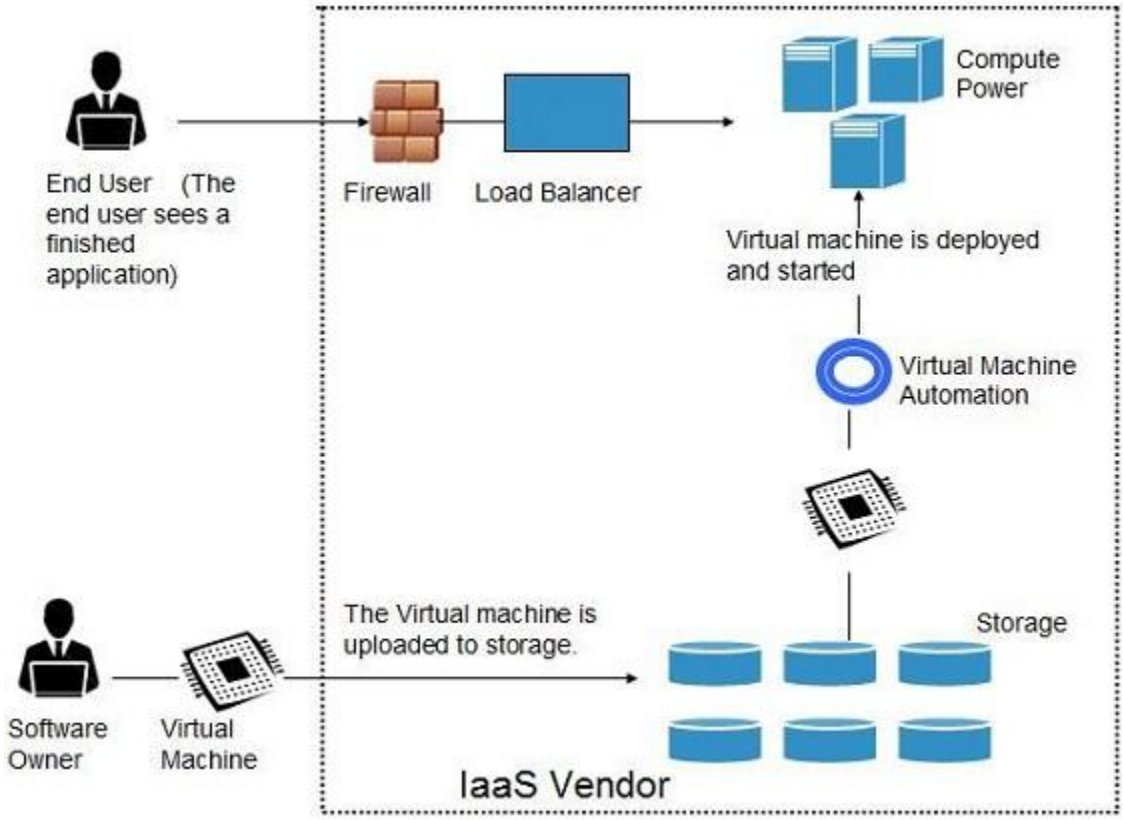
10

Infrastructure-as-a-service

IaaSprovides 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.



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 consumer to access computing resources through administrative access to virtual machines in the following manner:

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

FLEXIBLE AND EFFICIENT RENTING OF COMPUTER HARDWARE

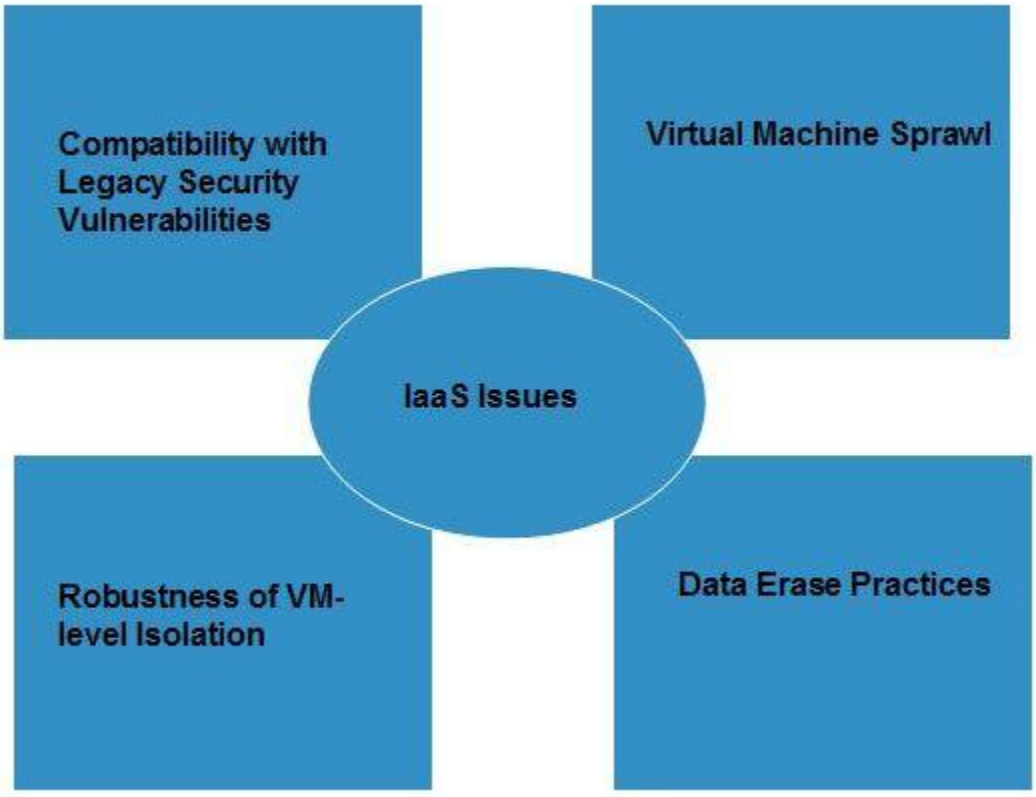
IaaS resources such as virtual machines, storages, bandwidth, IP addresses, monitoring services, firewalls, etc., all are made available to the consumers on rent. The consumer has to pay based the length of time a consumer retains a resource. Also with administrative access to virtual machines, the consumer can also 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, e-mail server that normally runs on consumer-owned server hardware can also be run from VMs in IaaS cloud.

Issues

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



COMPATIBILITY WITH LEGACY SECURITY VULNERABILITIES

Because IaaS offers the consumer to run legacy software in provider's infrastructure, therefore it exposes consumers 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 consumer 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 consumers 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 consumer uses virtual machines that in turn uses the common disk resources provided by the cloud provider. When the consumer releases the resource, the cloud provider must ensure that next consumer to rent the resource does not observe data residue from previous consumer.

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 in different locations.
- The computing resources can be easily scaled up and down.

CHAPTER

11

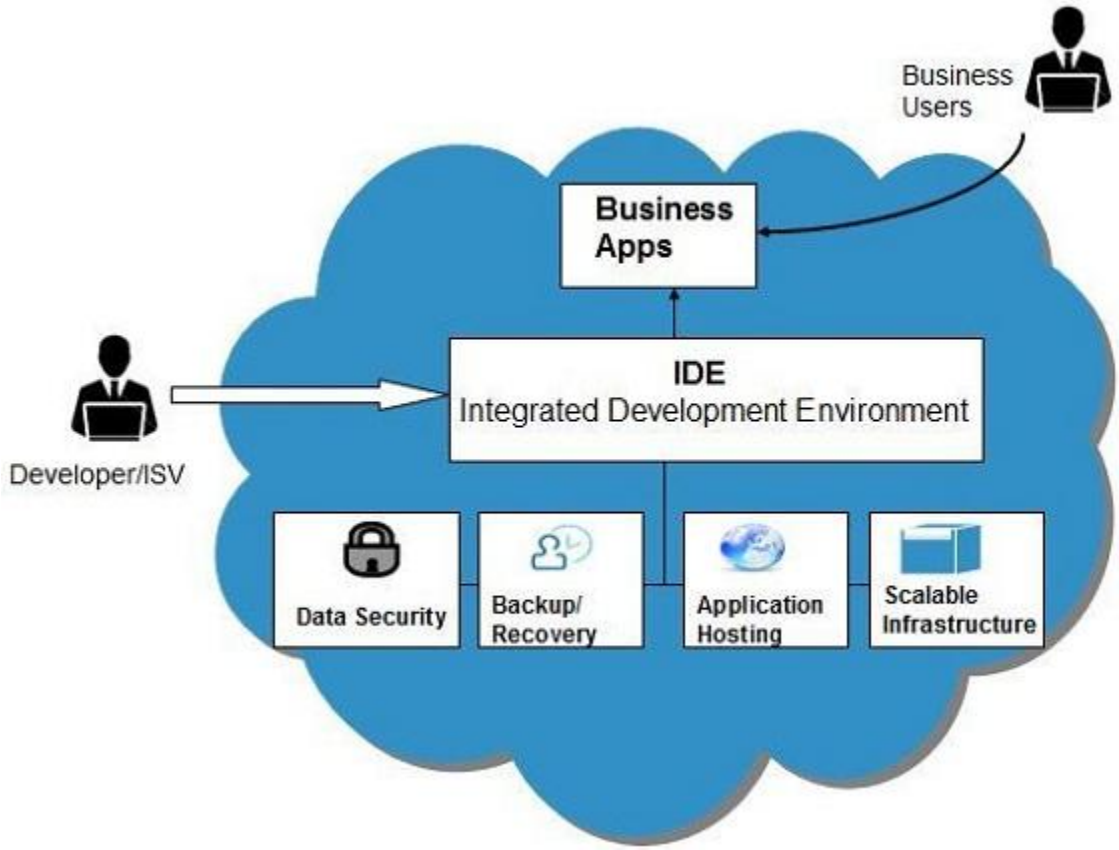
Platform-as-a-Service

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

Google's App Engine, 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.

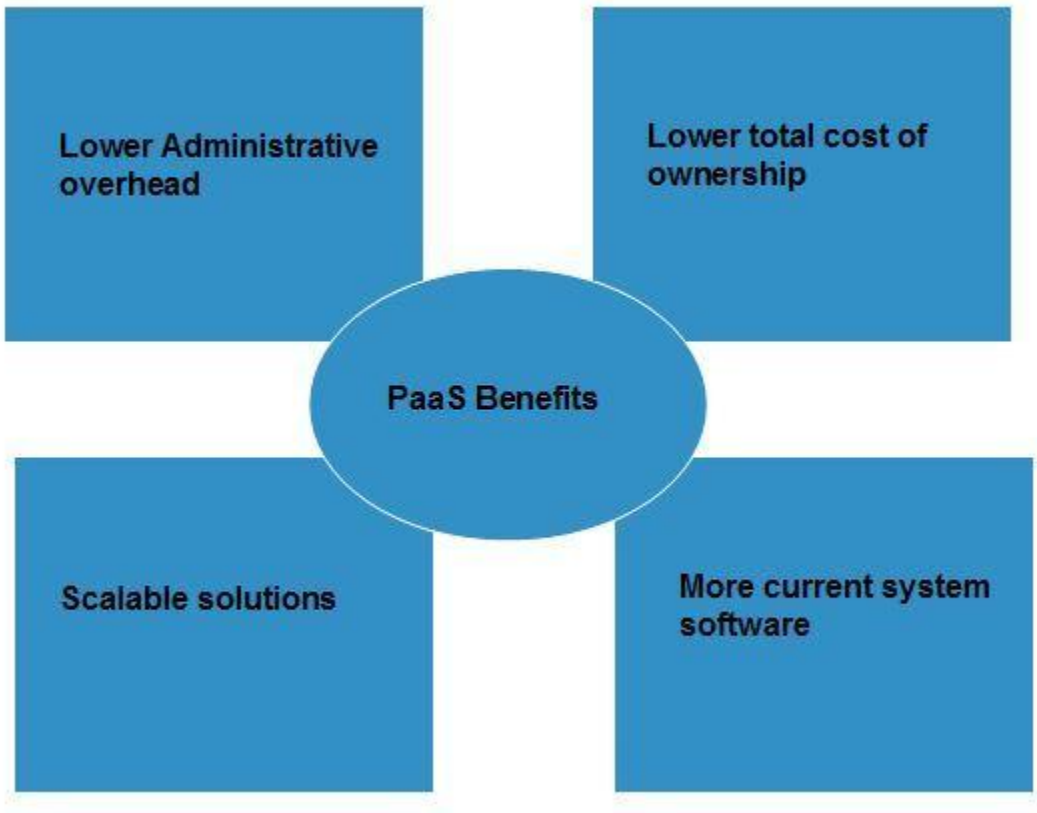
But the disadvantage of using PaaS is that the developer **lock-in** with a particular vendor. For example, an application written in Python against Google's API using Google's App Engine is likely to work only in that environment. Therefore, the vendor lock-in is the biggest problem in PaaS.

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

Consumer need not to bother much about the administration because it's the responsibility of cloud provider.

LOWER TOTAL COST OF OWNERSHIP

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

SCALABLE SOLUTIONS

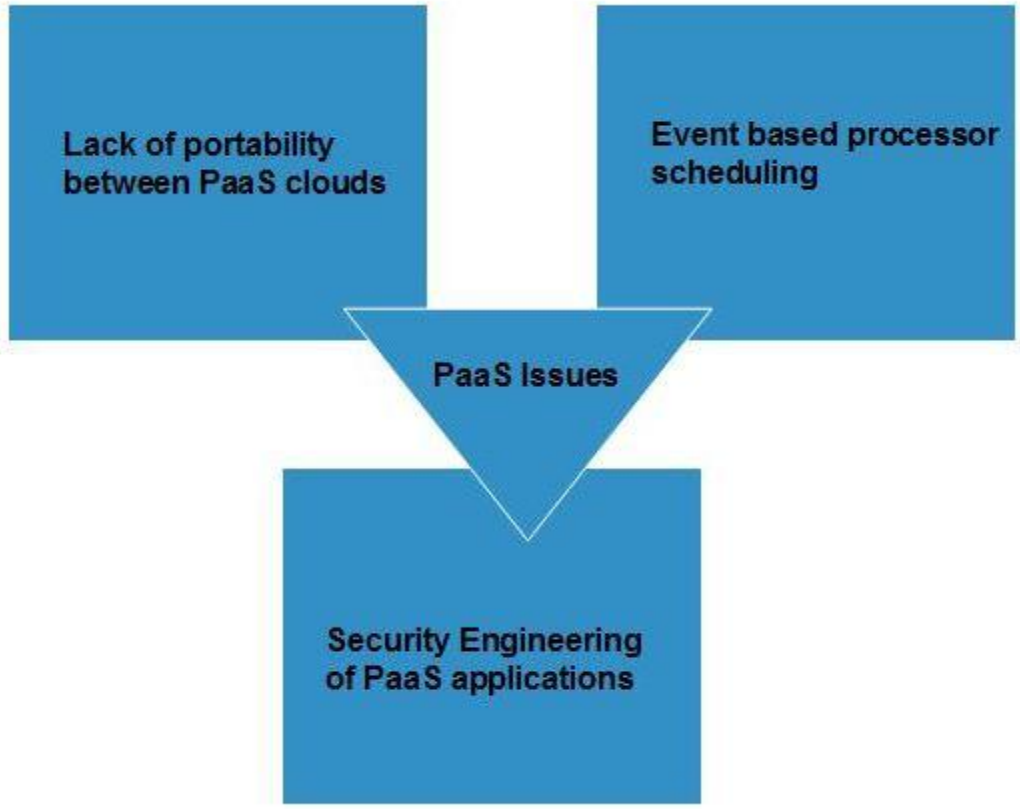
It is very easy to scale up or down automatically based on application resource demands.

MORE CURRENT SYSTEM SOFTWARE

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

Issues

Like **SaaS**, **PaaS** also place significant burdens on consumer's browsers to maintain reliable and secure connections to the provider 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

Although standard languages are used yet the implementations of platforms services may vary. For example, file, queue, or hash table interfaces of one platform may differ from another, making it difficult to transfer 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 the PaaS applications are dependent on network, PaaS applications must explicitly use cryptography and manage security exposures.

Characteristics

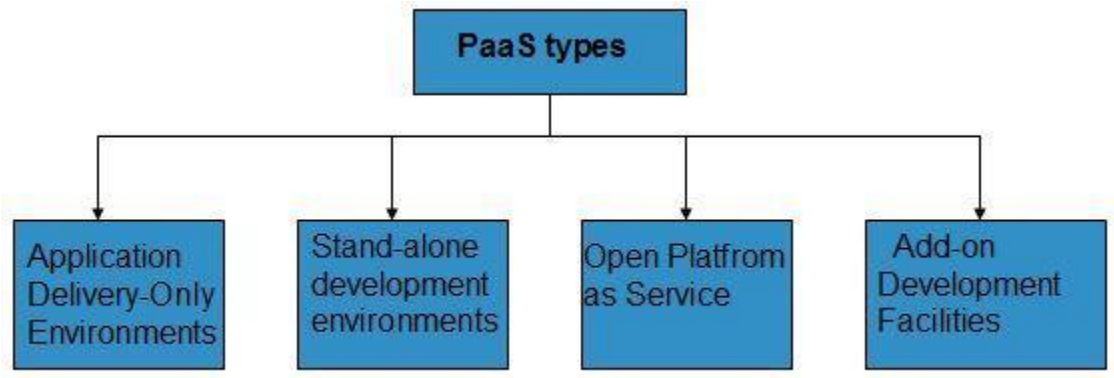
Here are the characteristics of PaaS service model:

- 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 and approval processes** and defining business rules.
- It is easy to integrate 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, the PaaS can be classified into four types as shown in the following diagram:



STAND-ALONE DEVELOPMENT ENVIRONMENTS

The **Stand-alone PaaS** works as an independent entity for a specific function. It does not include licensing, 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.

CHAPTER

12

Software-as-a-Service

Softwareas 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 hosted service and is accessible via Internet. There are several SaaSapplications, some of them are 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 an **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 are maintained by the vendor rather than where they are running.
- 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 share 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 are running same version of the software.

Benefits

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

- Modest Software Tools
- Efficient use of Software Licenses
- Centralized Management & 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 client 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 & DATA

The data stored by the cloud provider is centralized. However, the cloud providers may store data in a decentralized manner for 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 consumer need not to bother about them.

MULTITENANT SOLUTIONS

Multitenancy allows multiple users to share single instance of resources in virtual isolation. Consumers 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 consumer visits malicious website and browser becomes infected, and the subsequent access to SaaS application might compromise the consumer's data.

To avoid such risks, the consumer 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 the consumer.

LACK OF PORTABILITY BETWEEN SAAS CLOUDS

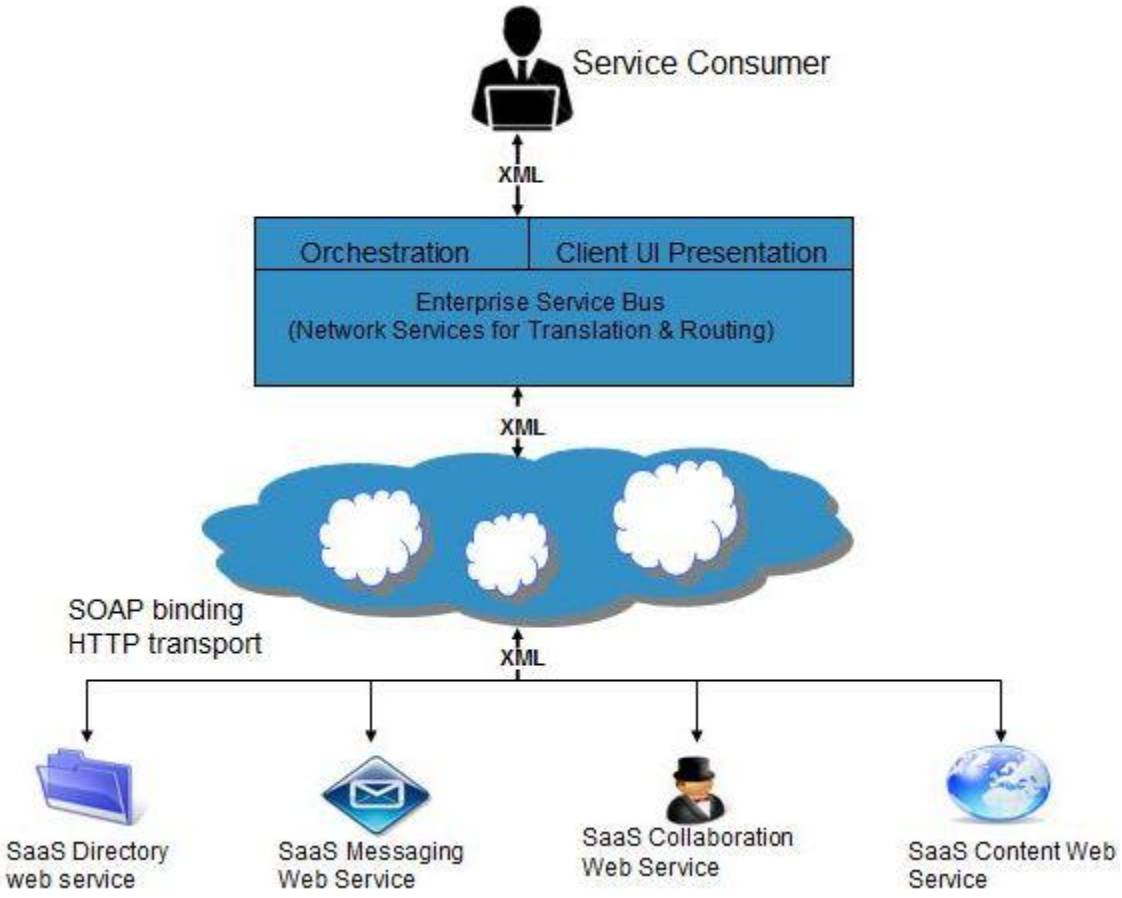
Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.

OPEN SAAS AND SOA

Open SaaS uses SaaS applications that 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, some of these are 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:


Service Consumer
XML
Orchestration
Client UI Presentation
Enterprise Service Bus
(Network Services for Translation & Routing)
XML
SOAP binding
HTTP transport
XML
SaaS Directory
web service
SaaS Messaging
Web Service
SaaS Collaboration
Web Service
SaaS Content Web
Service

CHAPTER

13

Identity-as-a-Service

Overview

Employees in a company require to login into 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's required to ensure that each of the user's account has been 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

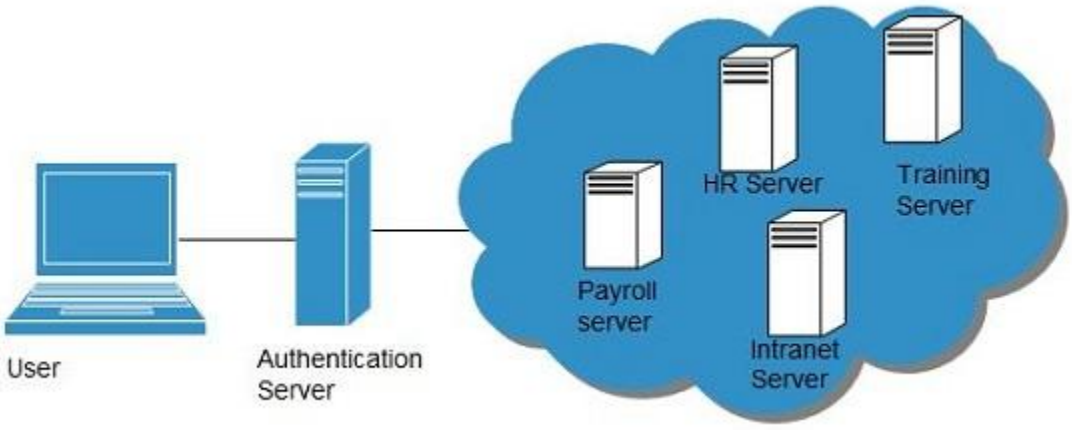
Identity refers to set of attributes associated with something and make it recognizable. All objects may have same attributes, but their identity cannot be the same. This unique identity is assigned through unique identification attribute.
There are several **identity services** that have been deployed 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)

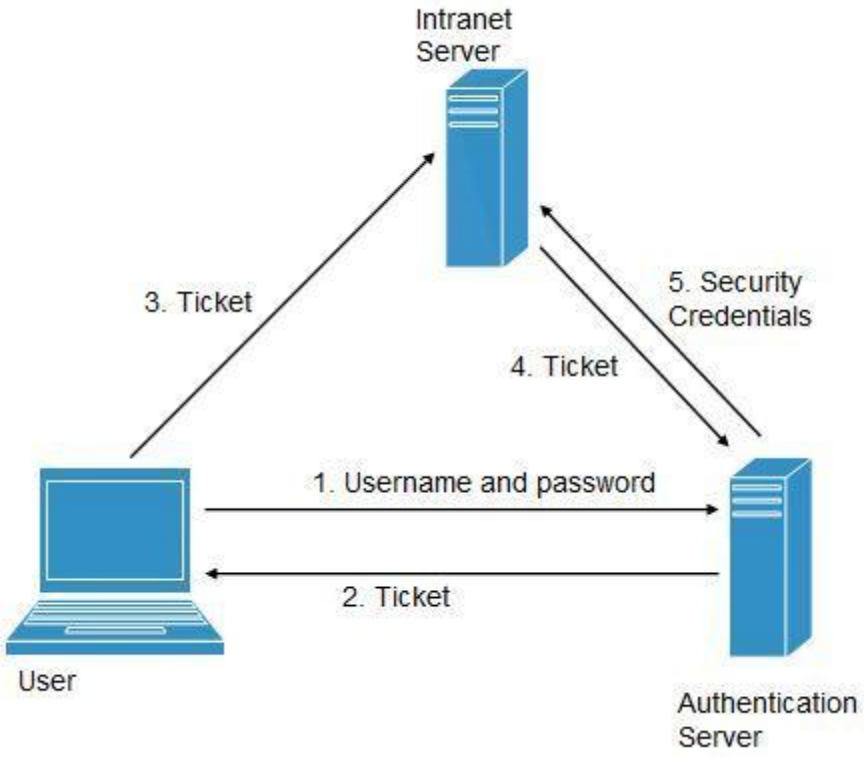
To solve the problem of using different username & password combination for different servers, companies now employ Single Sign-On software, which allows the user to login only one time and manages the user's access to other systems.

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 will discuss the common working of SSO:



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

1. User logs into the authentication server using a username and password.

2. The authentication server returns the user's ticket.

3. User sends the ticket to intranet server.

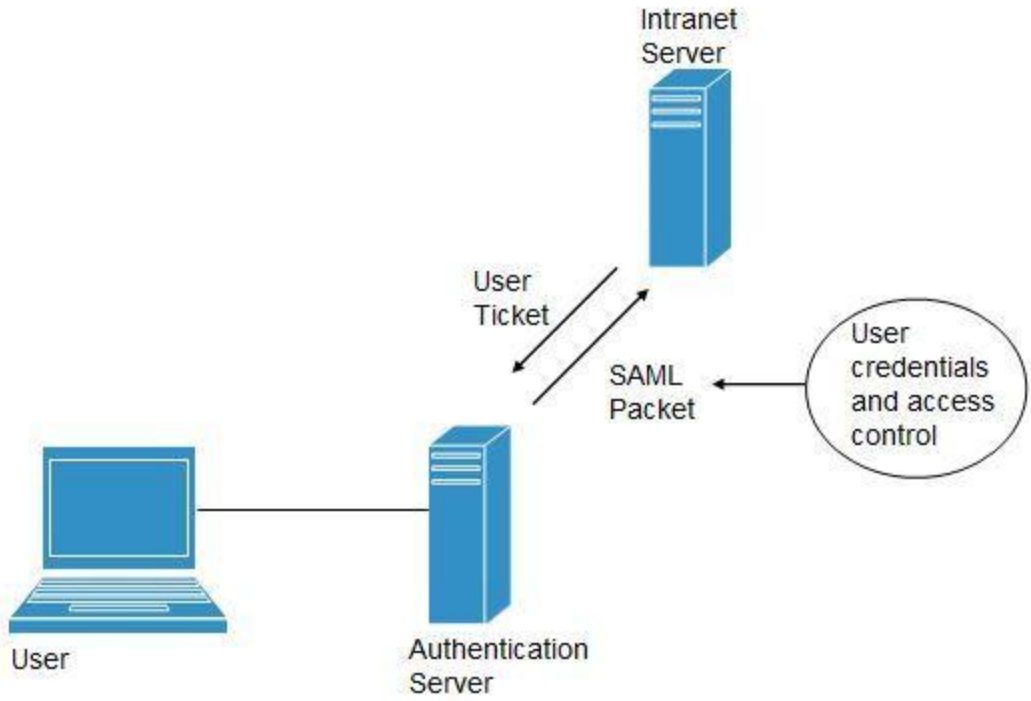
4. Intranet server sends the ticket to the authentication server.

5. Authentication server sends the user's security credentials for that server back to the intranet server.

If an employee leaves the company, then it just required to disable the user at the authentication server, which in turn disables 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.

CHAPTER

14

Network-as-a-Service

Overview

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 consumer. It is the responsibility of NaaS provider to maintain and manage the network resources which decreases the workload from the consumer. Moreover, NaaS offers **network as a utility**.
NaaS is also based on **pay-per-use** model.

How NaaS is delivered?

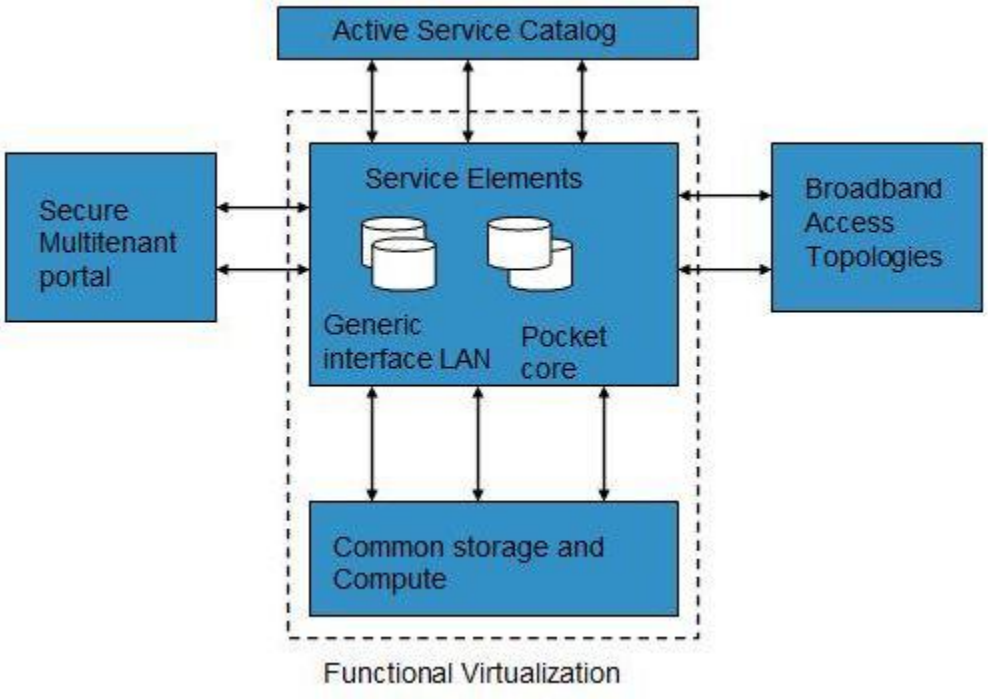
To use NaaS model, the consumer is required to logon to the web portal, where he can get online API. Here, the consumer can customize the route.

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

Mobile NaaS

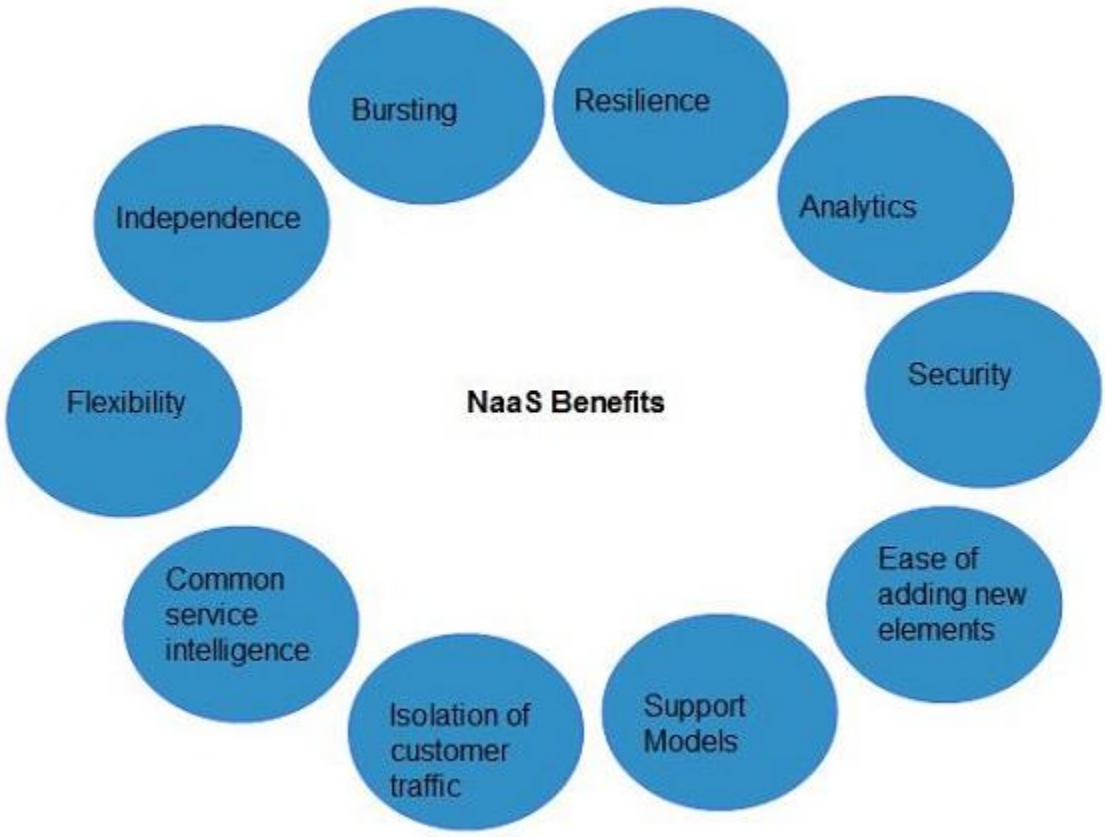
Mobile NaaS offers more efficient and flexible control over mobile devices. It uses virtualization to simplify the architecture to create more efficient processes.

Following diagram shows the Mobile NaaS service elements:



NaaS Benefits

NaaS offers a number of benefits, some of them are discussed below:



INDEPENDENCE

Each consumer is independent and can segregate the network.

BURSTING

Customers have to pay for high-capacity network only when needed.

RESILIENCE

There exists reliability treatments that can be applied for critical applications.

ANALYTICS

There exists data protection solution for highly sensitive applications.

EASE OF ADDING NEW SERVICE ELEMENTS

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

SUPPORT MODELS

There exists more open support models, which help to reduce the operation cost.

ISOLATION OF CUSTOMER TRAFFIC

The customer traffic is logically isolated.

CHAPTER

15

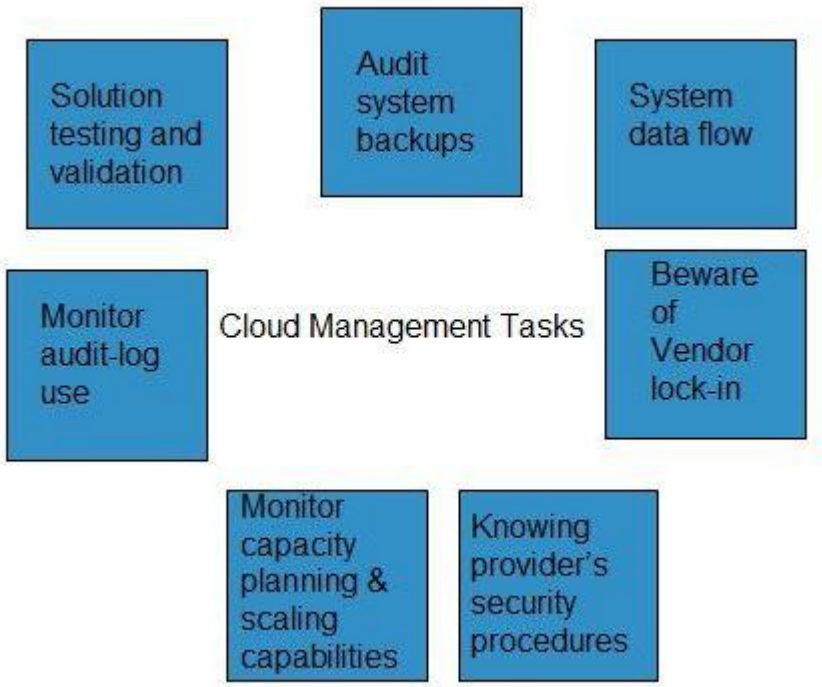
Cloud Computing Management

Overview

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

Cloud Management Tasks

Cloud Management involves a number of tasks to be performed by the cloud provider to ensure efficient use of cloud resources. Here, we will discuss some of these tasks:



AUDIT SYSTEM BACKUPS

It is required to timely audit the backups to ensure you can successfully restore 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, you must know where.

SYSTEM'S DATA FLOW

The managers should develop a diagram describing a detailed process flow. This process flow will describe the movement of company's data throughout the cloud solution.

BEWARE OF VENDOR LOCK-IN

The managers must know the procedure to exit from services of a particular cloud provider. There must exist procedures, enabling the managers to export company's data to a file and importing it to another provider.

KNOWING PROVIDER'S SECURITY PROCEDURES

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

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

MONITOR CAPACITY PLANNING AND SCALING CAPABILITIES

The managers should know the capacity planning in order to ensure whether the cloud provider will meet the future capacity requirement for his business or not.

It is also required to manage 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 the errors in the system, managers must audit the logs on a regular basis.

SOLUTION TESTING AND VALIDATION

It is necessary to test the solutions provided by the provider in order to validate that it gives the correct result and is error-free. This is necessary for a system to be robust and reliable.

CHAPTER

16

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

Block Storage Devices offer raw storage to the clients. This raw storage can be partitioned to create volumes.

FILE STORAGE DEVICES

File Storage Devices offers storage to clients in 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 that the storage is preconfigured for the consumer. The consumer cannot format nor the consumer can install own file system or change drive properties.

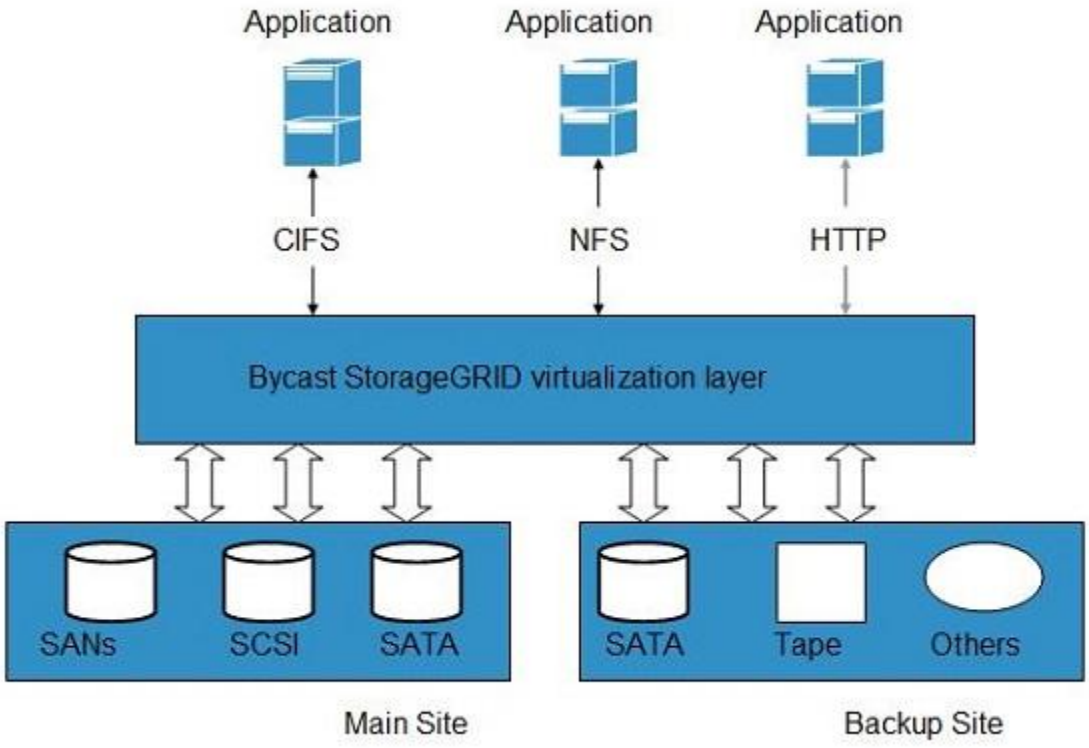
MANAGED CLOUD STORAGE

Managed Cloud Storage offers online storage space on demand. Managed cloud storage system presents what appears to the user to be a raw disk that the user can partition and format.

Creating Cloud Storage System

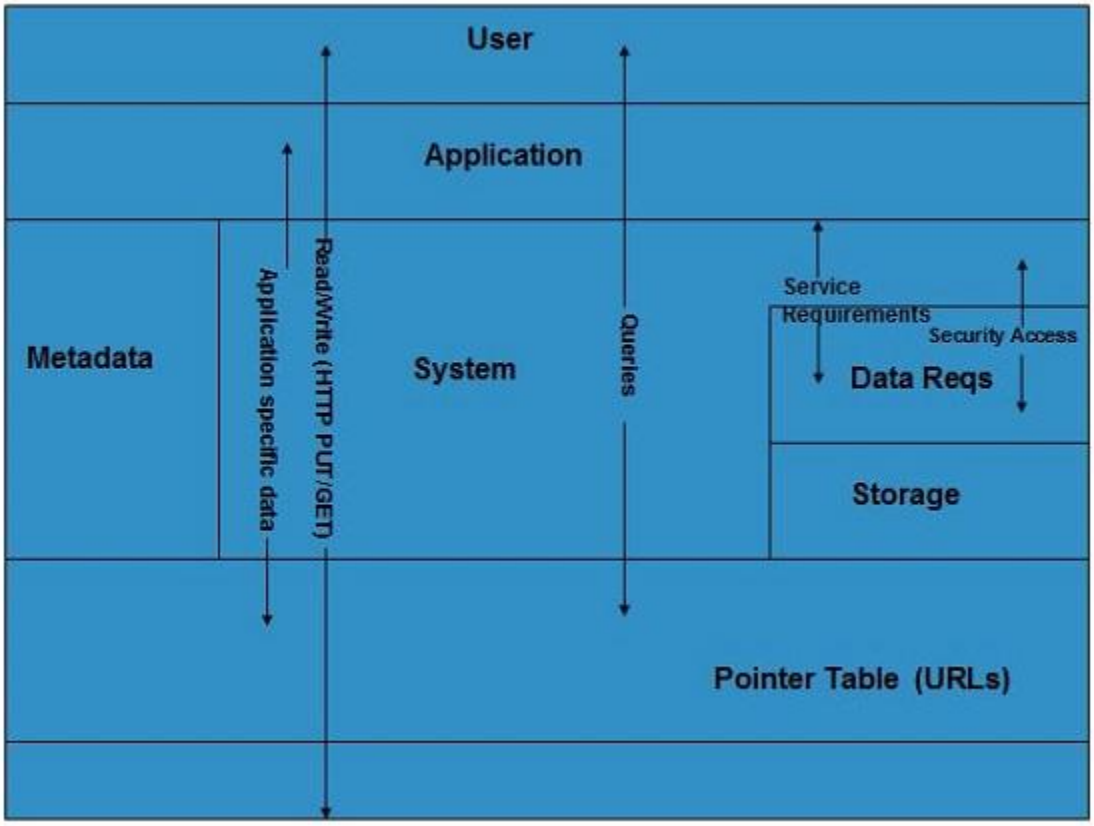
The cloud storage system stores multiple copies of data on multiple servers and in multiple locations. If one system fails, then it only requires to change the pointer to stored object's location.

To aggregate storage assets into cloud storage systems, the cloud provider can use storage virtualization software, **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 system over the Internet. The following diagram shows how SystemGRID virtualizes the storage into storage clouds:



Virtual Storage Containers

Virtual storage containers offer high performance cloud storage systems. **Logical Unit Number (LNU)**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 consumers. The consumers require ability to:

- Provision 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 surely disposing of data storage hardware.
- Administrator access control over data.

CHAPTER

17

Cloud Computing Virtualization

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** when demanded.

Virtualization Concept

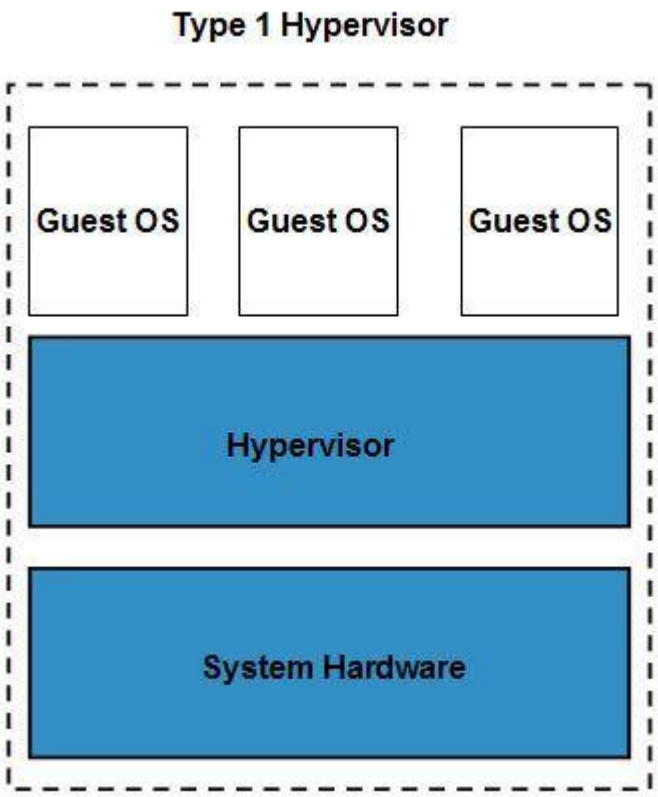
Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware.

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**.

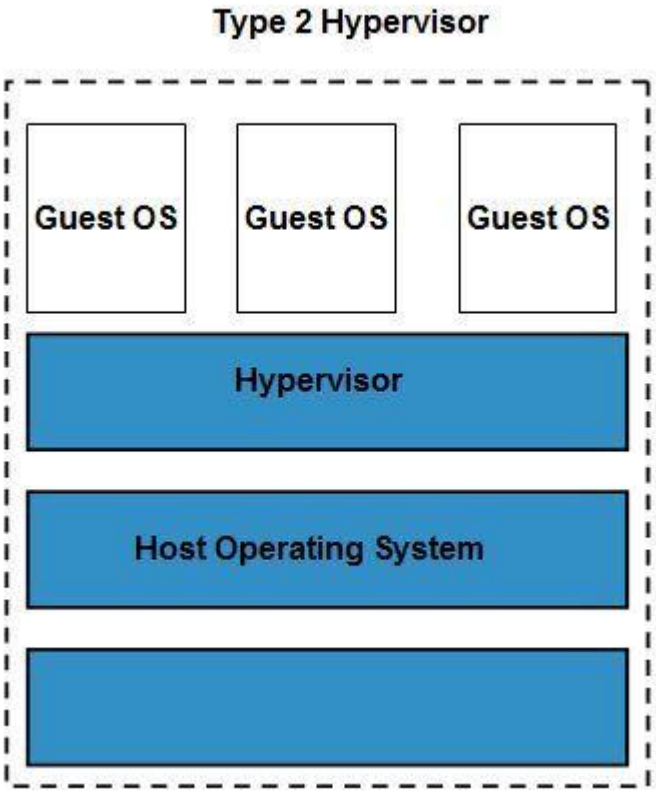
HYPERVISOR

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

Type 1 hypervisor runs 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.



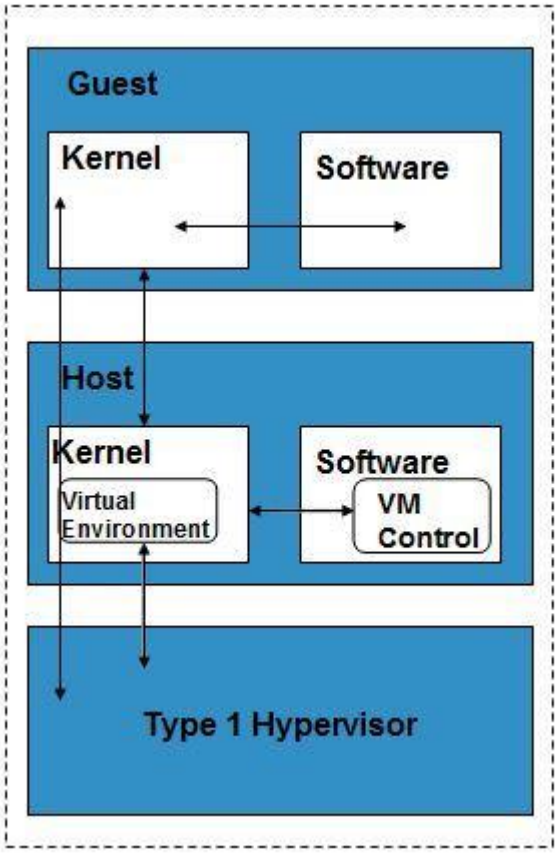
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

1. Full Virtualization
2. Emulation Virtualization
3. Paravirtualization

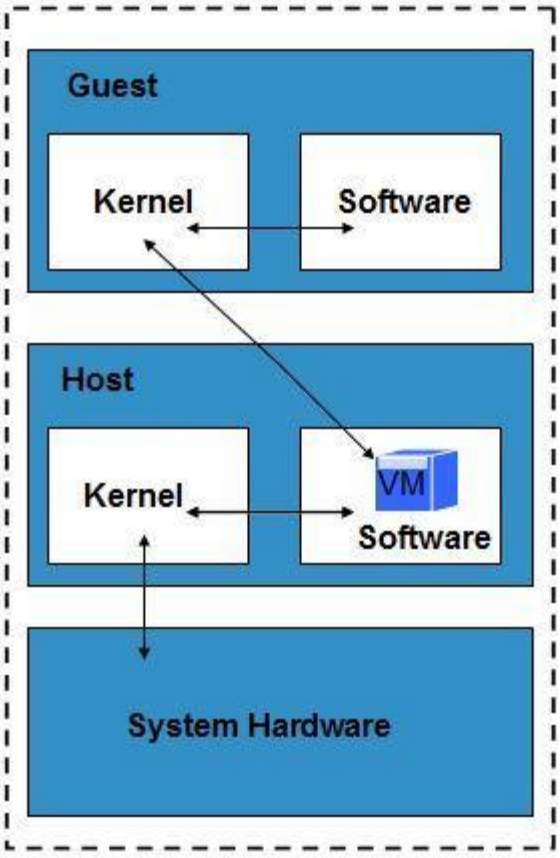
FULL VIRTUALIZATION

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



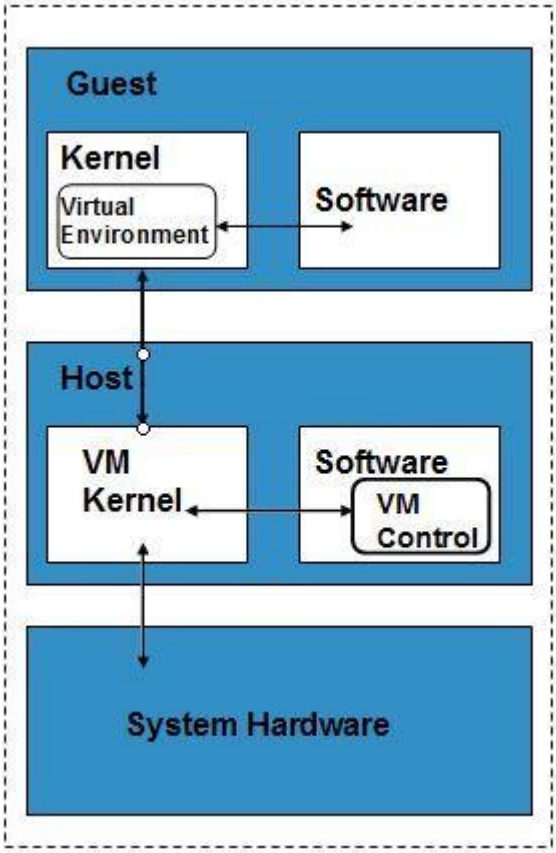
EMULATION VIRTUALIZATION

In **Emulation**, the virtual machine simulates the hardware and hence become independent of the 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.

CHAPTER

18

Cloud Computing Security

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

Security Planning

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

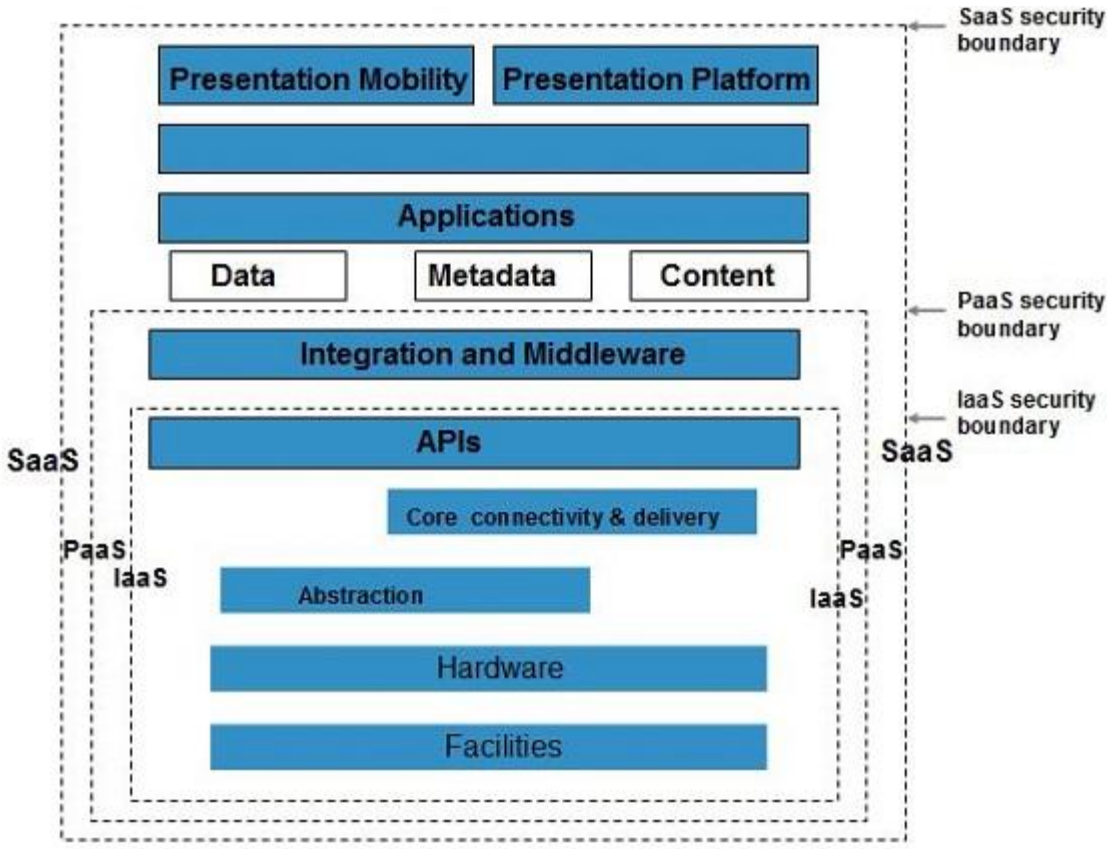
- Select which resources he is going to move to cloud and analyze its sensitivity to risk.
- Consider cloud service models such as **IaaS, PaaS**, and **SaaS**. These models require consumer to be responsible for security at different levels of service.
- Consider which cloud type such as **public, private, community** or **hybrid**.
- Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud.

Mainly the risk in cloud deployment 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 consumer. **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 service.
- 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 responsibility ends and the consumer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and above should me maintained by the consumer.

Although each service model has security mechanism but security needs also depends 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 cloud. Here are key mechanisms for protecting data mechanisms listed below:

- 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, therefore to protect the data, we must have a mechanism to isolate data from direct client access.

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

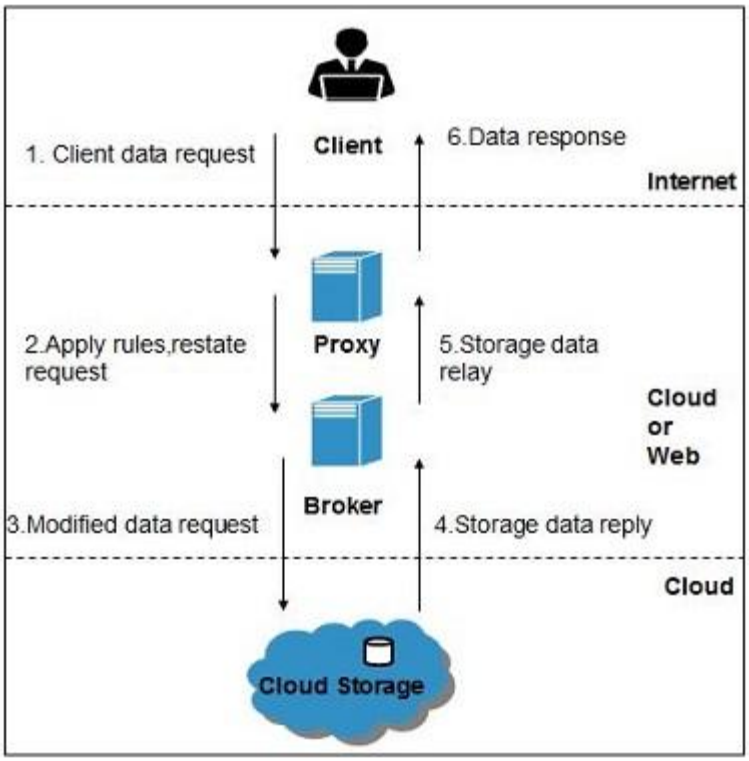
- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

WORKING OF BROKERED CLOUD STORAGE ACCESS SYSTEM

When the client issue request to access data:

- The client data request goes to proxy's external service interface.
- 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 from data loss.

CHAPTER

19

Cloud Computing Operations

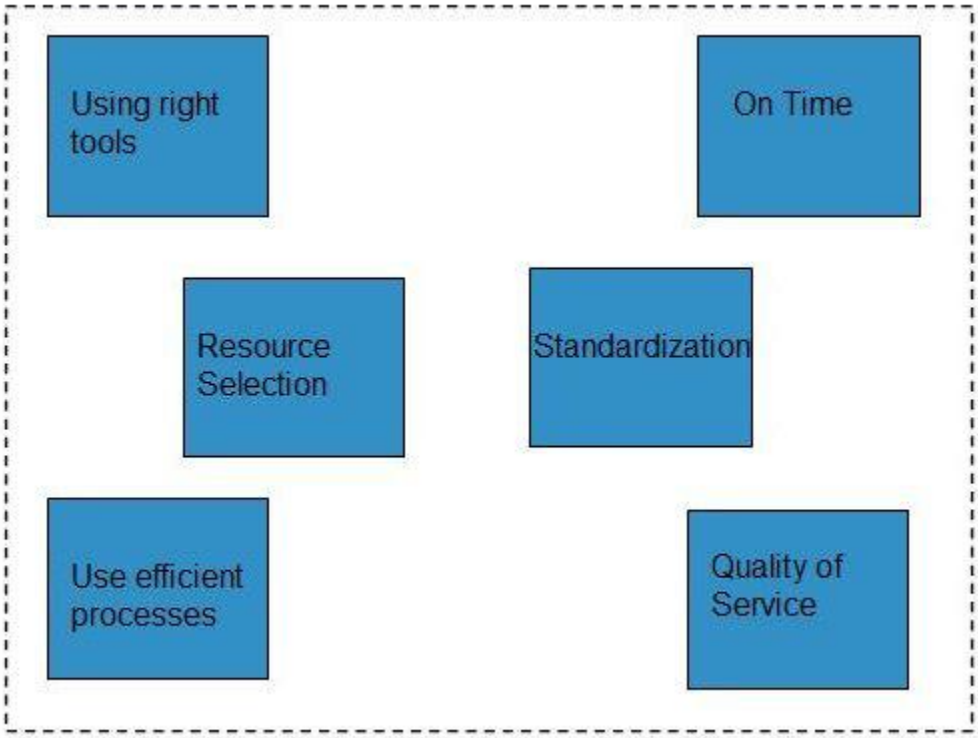
Overview

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 that are 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 avoid repetitive tasks.
- Using efficient process will eliminate the waste and redundancy.
- One should maintain the quality of service to avoid re-work later.

CHAPTER

20

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. It just required to drop the files into Box and access from anywhere.
2	**Mozy** **Mozy** offers online backup service for files during a 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** Evernote is an application that 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** **Facebook** offers social networking service. One can share photos, videos, files, status and much more.
2	**Twitter** **Twitter** helps to interact directly with the public. 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	**Audiobox.fm** It offers streaming service, i.e., music can be stored online and can be played from cloud using service's own media player.

Art Applications

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

CHAPTER

21

Cloud Computing Providers

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

SN	Platform's Description
1	**Salesforce.com** This is a Force.com development platform. This provide a simple user interface and lets users log in, build an app and push it in the cloud.
2	**Appistry** The Appistry'sCloudQ platform is efficient in delivering a runtime application platform. This platform is very useful to create scalable and service oriented applications.
3	**AppScale** The AppScale is an open source platform for Google App Engine 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 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 gPlatform.
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's infrastructure.
12	**LongJump**

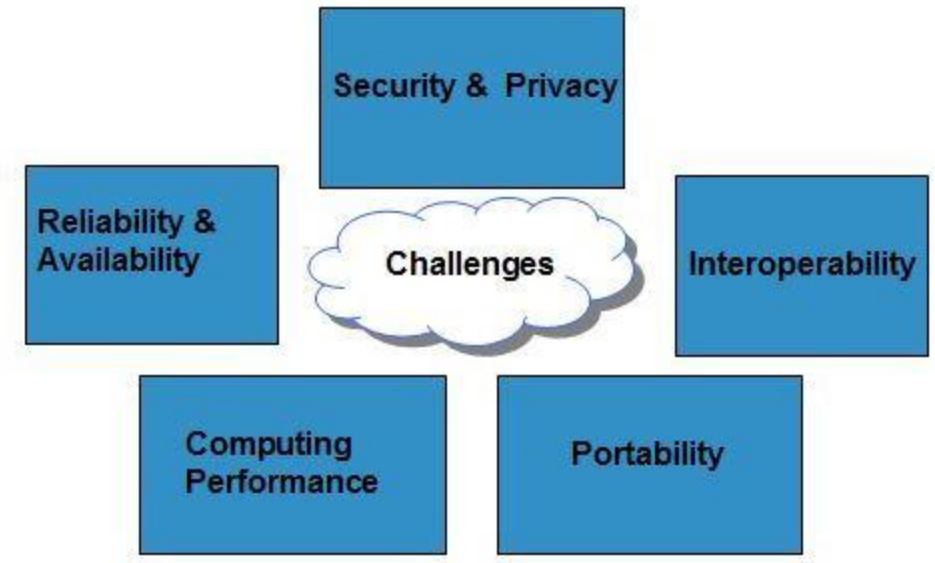
	The LongJump offers a Business Application Platform, a platform-as-a-Service (PaaS).
13	**Microsoft** The Microsoft's Windows Azure is a cloud computing platform offering an environment to create cloud apps and services.
14	**OrangeScape** OrangeScape offers a Platform-as-a-Service (Paas) for non-programmers. Building an app is as easy as spreadsheet.
15	**RackSpace** The RackSpace provide 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's environment.

CHAPTER

22

Cloud Computing Challenges

Cloud Computing, an emergence technology, has placed many challenges in different aspects. Some of these are shown in the following diagram:



SECURITY & 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 should 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

Application on one platform should be able to incorporate services from other platform. It is made possible via web services. But writing such web services is very complex.

COMPUTING PERFORMANCE

To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost. If done at low bandwidth, then it does not meet the required 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.

CHAPTER

23

Mobile Cloud Computing

CloudComputing offers such smartphones that have rich Internet media experience and require less processing, less power. In term of Mobile Cloud Computing, processing is done in cloud, data is stored in cloud. And the mobile devices serve as a 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.

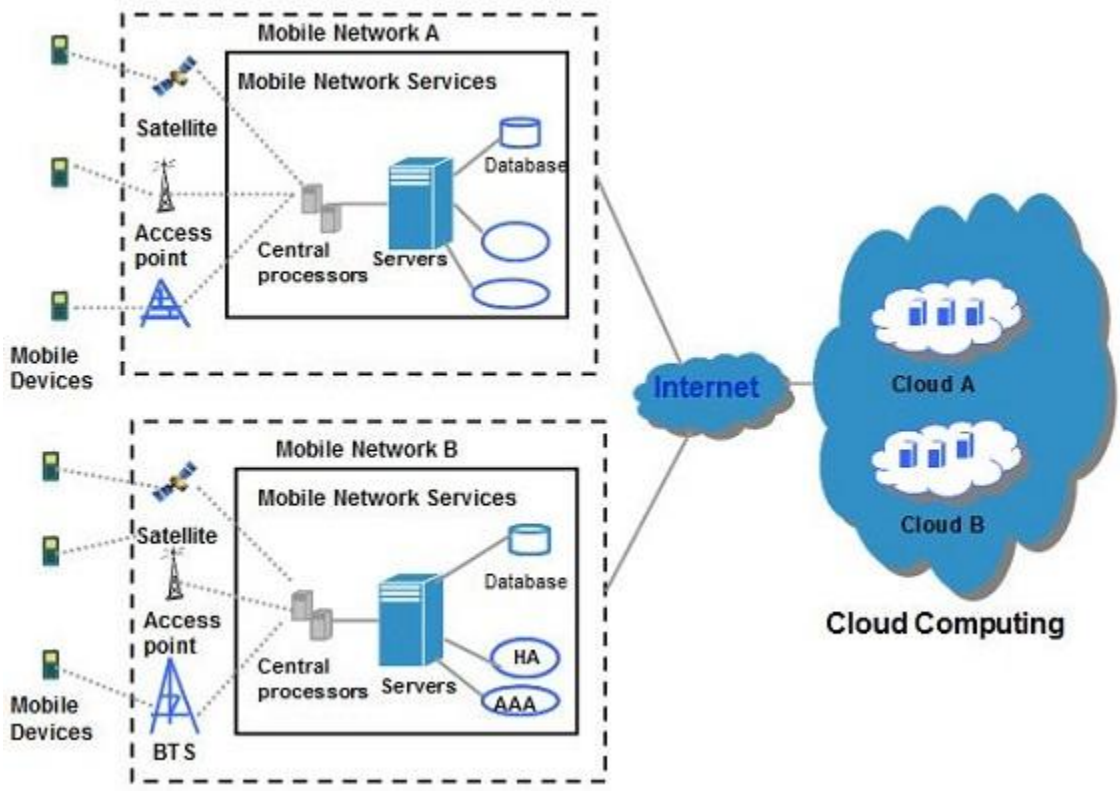
There are several Smartphone operating systems available such as **Google's Android, Apple's iOS, RIM BlackBerry, Symbian,** and **Windows Mobile Phone**. Each of these platforms support third-party applications that are deployed in cloud.

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 computing, there still exists many issues:

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 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.