CLOUD COMPUTING

B.sc CSIT Eighth Semester

DECEMBER 14, 2017

PREPARED BY:
Er. Lok Nath Regmi

Chapter -1

Introduction

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.

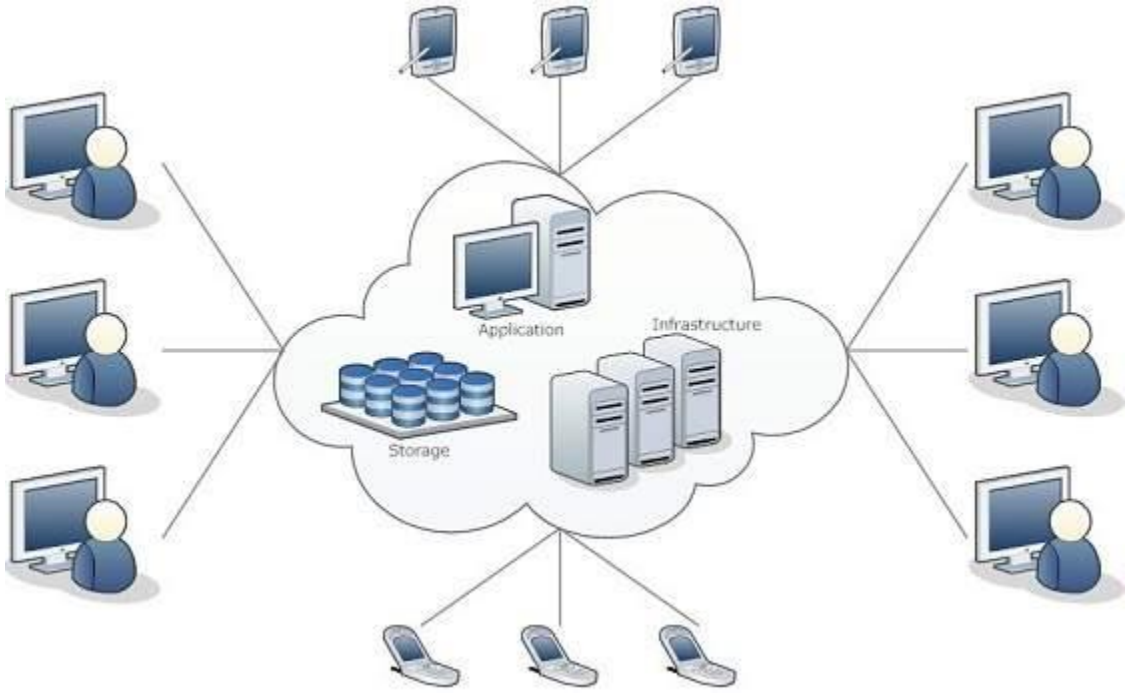
What is Cloud?

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.

Prepared By: Er. Loknath Regmi

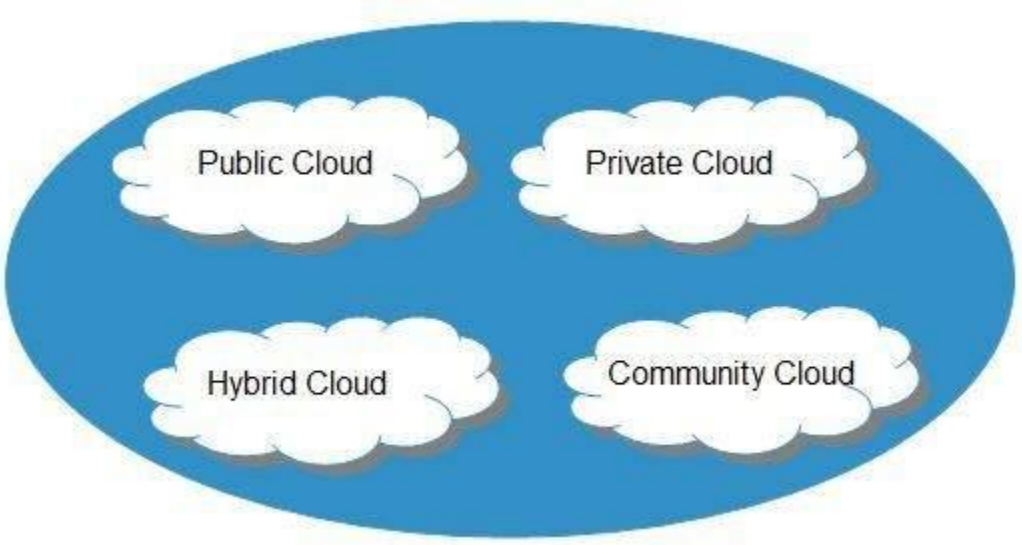
Basic Concepts

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.

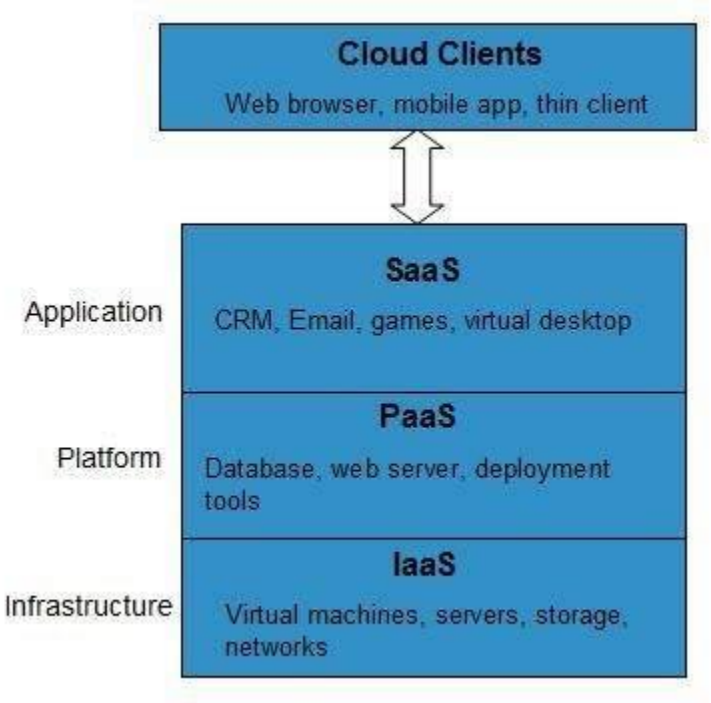
Service Models

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:

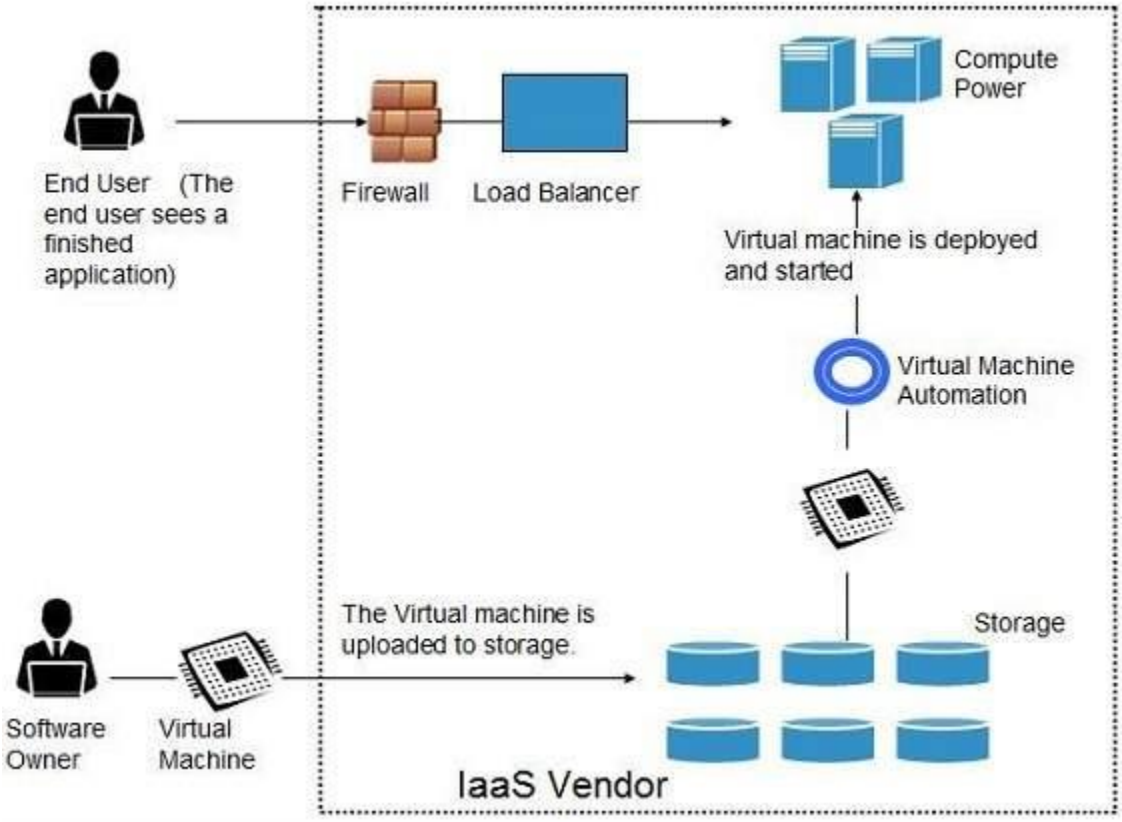


INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc. IaaS refers not to a machine that does all the work, but simply to a facility given to businesses that offers users the leverage of extra storage space in servers and data centers. Examples of IaaS include: Amazon CloudFormation (and underlying services such as Amazon

EC2), Rackspace Cloud, Terremark, Windows Azure Virtual Machines, Google Compute Engine, and Joyent.

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.

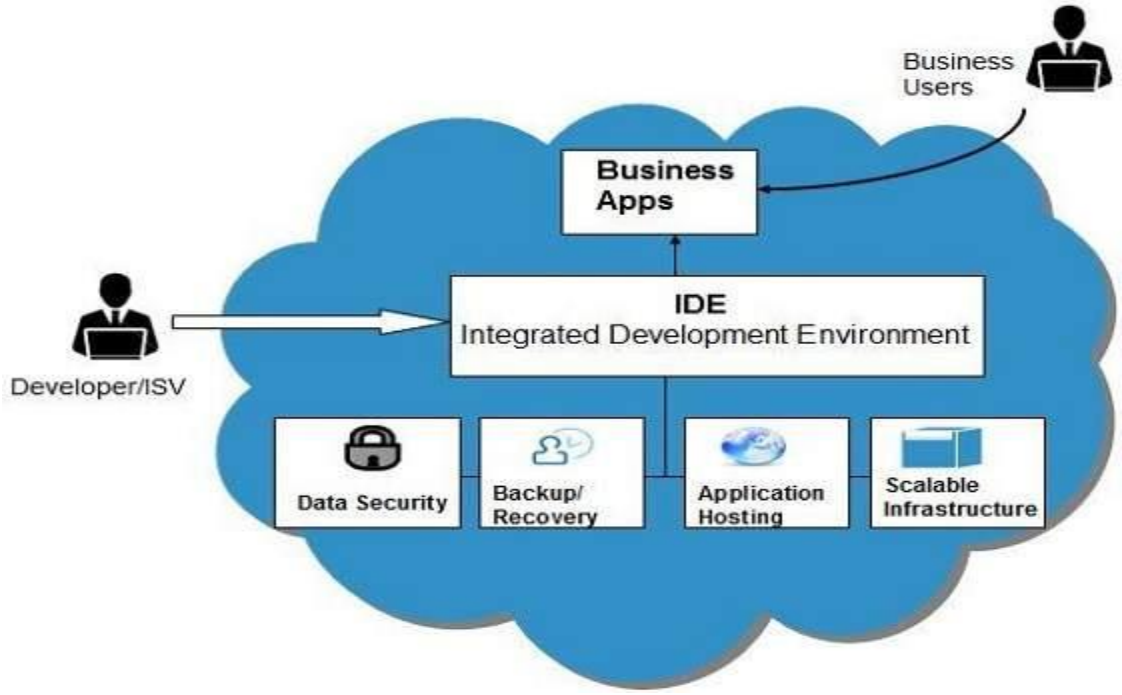
PLATFORM-AS-A-SERVICE (PAAS)

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

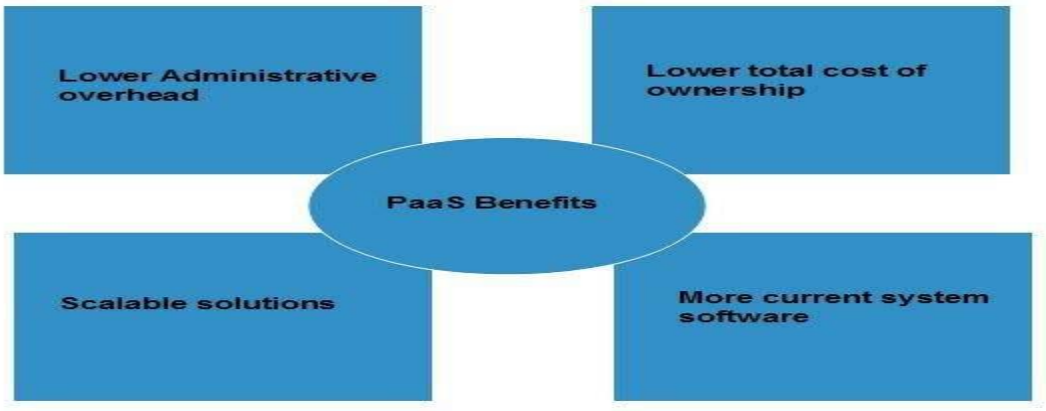
But the disadvantage of using PaaS is that, the developer locks-in with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

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:



1. Lower administrative overhead

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

2. Lower total cost of ownership

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

3. Scalable solutions

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

4. More current system software

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

SOFTWARE-AS-A-SERVICE (SAAS)

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

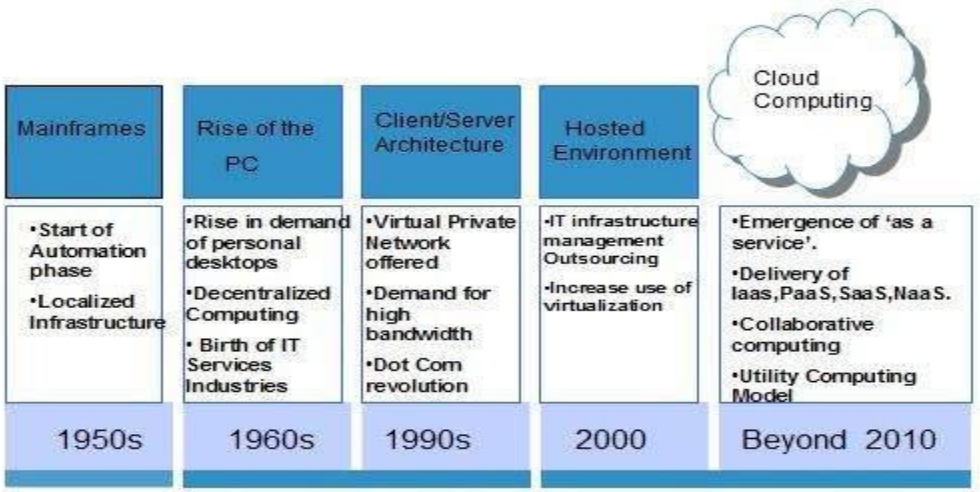
Benefits

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

History of Cloud Computing

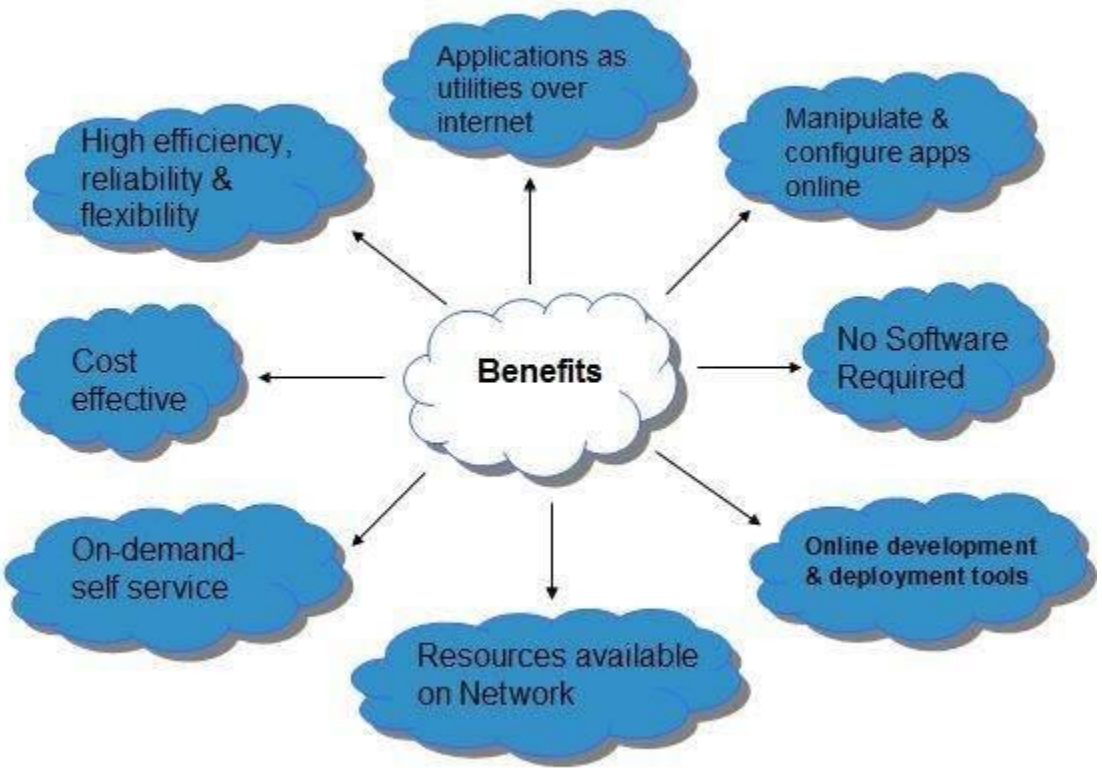
The concept of Cloud Computing came into existence in the year 1950 with implementation of mainframe computers, accessible via thin/static clients. Since then, cloud computing has been evolved from static clients to dynamic ones and from software to services. The following diagram explains the evolution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



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.



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:

1. 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.

2. 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.

3. Isolation Failure

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

4. Management Interface Compromise

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

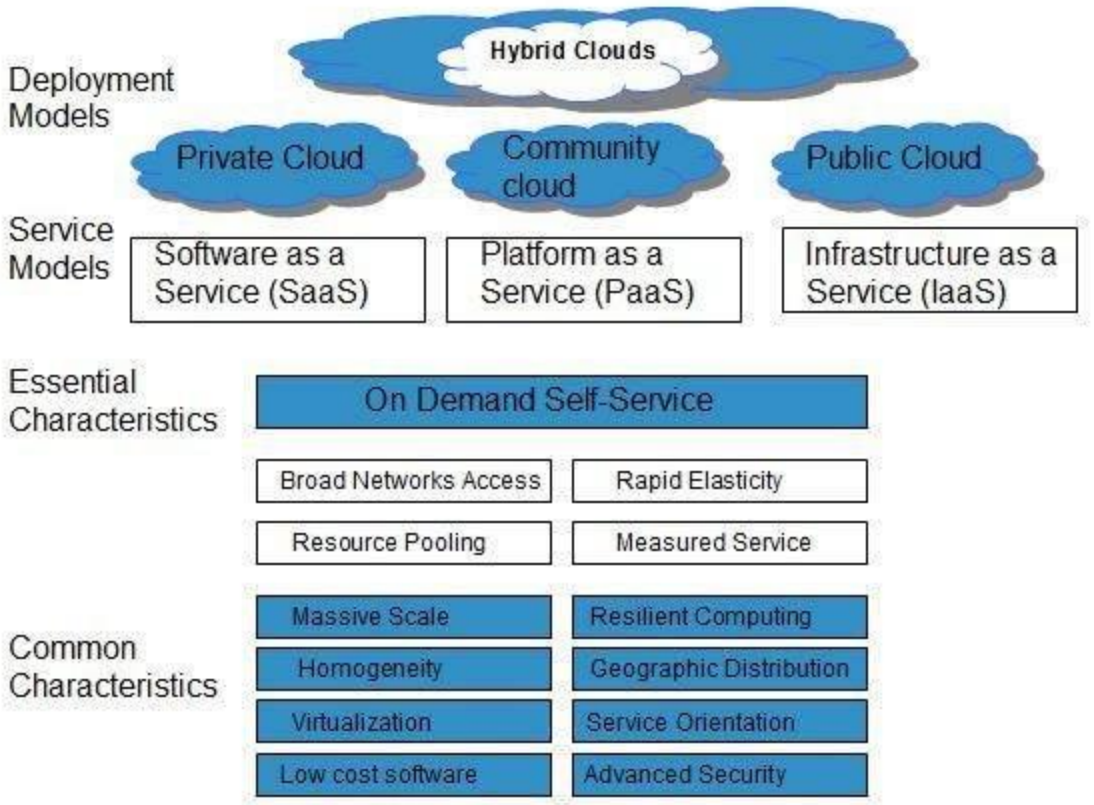
5. Insecure or Incomplete Data Deletion

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:



1. 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.

2. 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.

3. 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.

4. 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.

Emergence of Cloud Computing:

The origin of the term *cloud computing* is obscure, but it appears to derive from the practice of using drawings of stylized clouds to denote networks in diagrams of computing and communications systems. The word *cloud* is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network on telephony schematics and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. The cloud symbol was used to represent the Internet as early as 1994.

In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service but at a much lower cost. By switching traffic to balance utilization as they saw fit, they were able to utilize their overall network bandwidth more effectively. The cloud symbol was used to denote the demarcation point between that which was the responsibility of the provider and that which was the responsibility of the users. Cloud computing extends this boundary to cover servers as well as the network infrastructure.

The underlying concept of cloud computing dates back to the 1950s; when large-scale mainframe became available in academia and corporations, accessible via thin clients /terminal computers. Because it was costly to buy a mainframe, it became important to find ways to get the greatest return on the investment in them, allowing multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time, eliminating periods of inactivity, which became known in the industry as time-sharing.

As in the earliest stages, the term "cloud" was used to represent the computing space between the provider and the end user. In 1997, Professor Ramnath Chellapa of Emory University and the University of South California defined cloud computing as the new "computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone." This has become the basis of what we refer to today when we discuss the concept of cloud computing. Some people think cloud computing is the next big thing in the world of IT. Others believe it is just another variation of the utility computing model that has been repackaged in this decade as something new and cool.

One of the first milestones for cloud computing was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet.

The next development was Amazon Web Services in 2002, which provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk. Then in 2006, Amazon launched its Elastic Compute cloud (EC2) as a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications.

Evolution of cloud computing:

Cloud computing can be seen as an innovation in different ways. From a technological perspective it is an advancement of computing, applying virtualization concepts to utilize hardware more efficiently. Yet a different point of view is to look at cloud computing from an IT deployment perspective. In this sense cloud computing has the potential to revolutionize the way, how computing resources and applications are provided, breaking up traditional value chains and making room for new business models. In the following section we are going to describe the emergence of cloud computing from both perspectives.

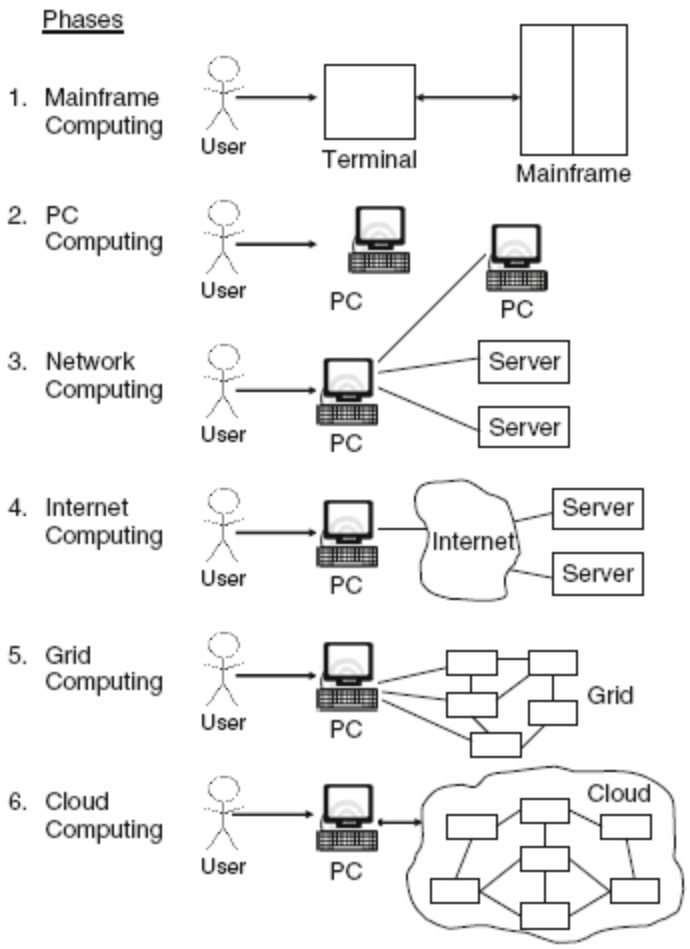


Fig: Evolution of Computing Paradigms from mainframe to cloud computing

Distributed Computing in Grid and Cloud:

Distributed computing is a field of computer science that studies distributed systems. A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. The word *distributed* in terms such as "distributed system", "distributed programming", and "distributed algorithm" originally referred to computer networks where individual computers were physically distributed within some geographical area. The terms are nowadays used in a much wider sense, even referring to autonomous processes that run on the same physical computer and interact with each other by message passing. While there is no single definition of a distributed system, the following defining properties are commonly used:

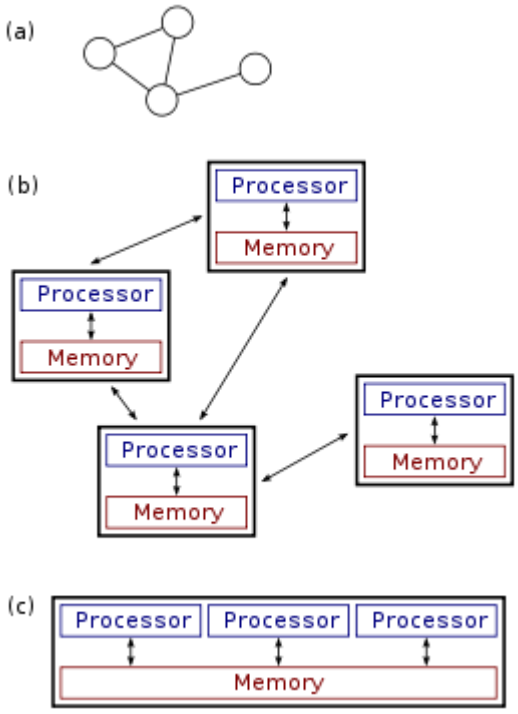
- There are several autonomous computational entities, each of which has its own local memory.
- The entities communicate with each other by message passing

Parallel Vs. Distributed Computing

Distributed systems are groups of networked computers, which have the same goal for their work. The terms "concurrent computing", "parallel computing", and "distributed computing" have a lot of overlap, and no clear distinction exists between them. The same system may be characterized both as "parallel" and "distributed"; the processors in a typical distributed system run concurrently in parallel. Parallel computing may be seen as a particular tightly coupled form of distributed computing, and distributed computing may be seen as a loosely coupled form of parallel computing. Nevertheless, it is possible to roughly classify concurrent systems as "parallel" or "distributed" using the following criteria:

- In parallel computing, all processors may have access to a shared memory to exchange information between processors.
- In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.

The figure below illustrates the difference between distributed and parallel systems. Figure (a) is a schematic view of a typical distributed system; as usual, the system is represented as a network topology in which each node is a computer and each line connecting the nodes is a communication link. Figure (b) shows the same distributed system in more detail: each computer has its own local memory, and information can be exchanged only by passing messages from one node to another by using the available communication links. Figure (c) shows a parallel system in which each processor has a direct access to a shared memory.



The last decade, the term 'Grid' has been a key topic in the field of high performance/distributed computing. The Grid has emerged as a new field of distributed computing, focusing on secure sharing of computational and storage resources among dynamic sets of people and organizations who own these resources. This sharing of resources can give people not only computational capabilities and data storage capabilities that cannot be provided by a single supercomputing center, but it also allows them to share data in a transparent way.

Grid Computing can be defined as applying resources from many computers in a network to a single problem, usually one that requires a large number of processing cycles or access to large amounts of data.

At its core, Grid Computing enables devices-regardless of their operating characteristics-to be virtually shared, managed and accessed across an enterprise, industry or workgroup. This virtualization of resources places all of the necessary access, data and processing power at the fingertips of those who need to rapidly solve complex business problems, conduct compute-intensive research and data analysis, and operate in real-time.

Distributed computing was one of the first real instances of cloud computing. Long before Google or Amazon, there was SETI@Home. Proposed in 1995 and launched in 1999, this program uses the spare capacity of internet connected machines to search for extraterrestrial intelligence. This is sort of the cloud in reverse.

A more recent example would be software like Hadoop. Written in Java, Hadoop is a scalable, efficient, distributed software platform designed to process enormous amounts of data. Hadoop can scale to thousands of computers across many clusters.

Distributed computing is nothing more than utilizing many networked computers to partition (split it into many smaller pieces) a question or problem and allow the network to solve the issue piecemeal.

Another instance of distributed computing, for storage instead of processing power, is bittorrent. A torrent is a file that is split into many pieces and stored on many computers around the internet. When a local machine wants to access that file, the small pieces are retrieved and rebuilt.

As the cloud computing buzzword has evolved, distributed computing has fallen out of that particular category of software. Even though distributed computing might take advantage of the internet, it doesn't follow the other tenants of cloud computing, mainly the automatic and instant scalability of resources.

That's not to say that a distributed system couldn't be built to be a cloud environment. Bittorrent, or any P2P system, comes very close to a cloud storage. It would require some additional protections like file ownership and privacy across all nodes but it could probably be done. Privacy like that is not quite what P2P is all about though.

The Cloud Computing paradigm originates mainly from research on distributed computing and virtualization, as it is based on principles, techniques and technologies developed in these areas.

Ethical issues in cloud computing:

Cloud computing is based on a paradigm shift with profound implications on computing ethics. The main elements of this shift are:

- the control is relinquished to third party services;
- the data is stored on multiple sites administered by several organizations;

- Multiple services interoperate across the network.

Unauthorized access, data corruption, infrastructure failure, or unavailability are some of the risks related to relinquishing the control to third party services; moreover, it is difficult to identify the source of the problem and the entity causing it. Systems can span the boundaries of multiple organizations and cross the security borders, a process called *deperimeterisation*. As a result of de-perimeterisation "not only the border of the organizations IT infrastructure blurs, also the border of the accountability becomes less clear".

The complex structure of cloud services can make it difficult to determine who is responsible in case something undesirable happens. In a complex chain of events or systems, many entities contribute to an action with undesirable consequences, some of them have the opportunity to prevent these consequences, and therefore no one can be held responsible, the so-called "problem of many hands."

Ubiquitous and unlimited data sharing and storage among organizations test the selfdetermination of information, the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal data by others; this tests the confidence and trust in todays evolving information society. Identity fraud and theft are made possible by the unauthorized access to personal data in circulation and by new forms of dissemination through social networks and they could also pose a danger to cloud computing.

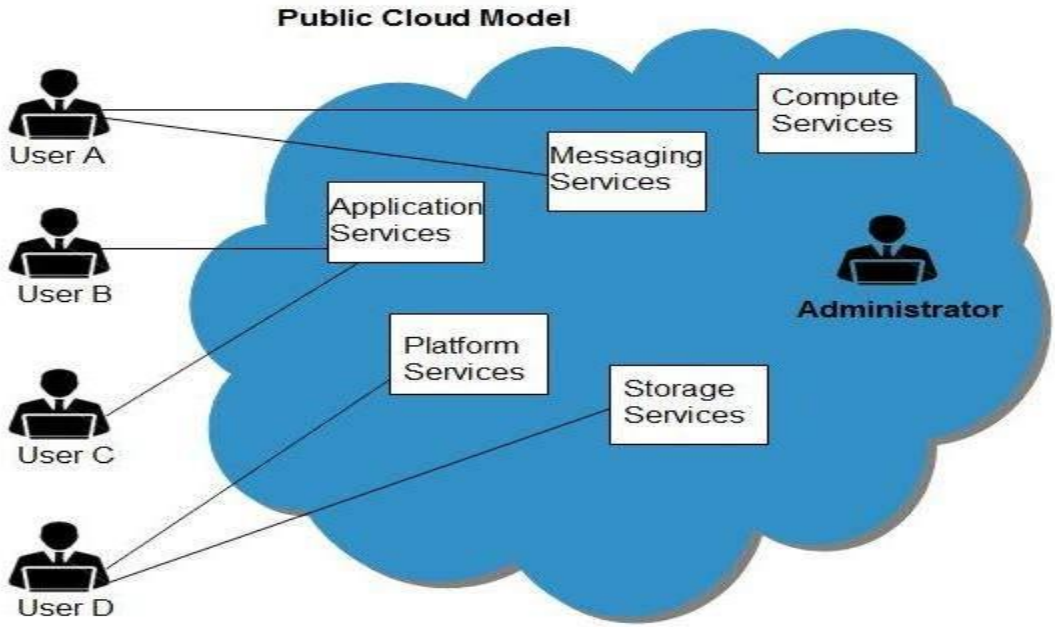
The question of what can be done proactively about ethics of cloud computing does not have easy answers as many undesirable phenomena in cloud computing will only appear in time. But the need for rules and regulations for the governance of cloud computing are obvious. The term *governance* means the manner in which something is governed or regulated, the method of management, the system of regulations. Explicit attention to ethics must be paid by governmental organizations providing research funding; private companies are less constraint by ethics oversight and governance arrangements are more conducive to profit generation.

Accountability is a necessary ingredient of cloud computing; adequate information about how data is handled within the cloud and about allocation of responsibility are key elements to enforcing ethics rules in cloud computing. Recorded evidence allows us to assign responsibility; but there can be tension between privacy and accountability and it is important to establish what is being recorded, and who has access to the records.

Unwanted dependency on a cloud service provider, the so-called *vendor lock-in*, is a serious concern and the current standardization efforts at NIST attempt to address this problem. Another concern for the users is a future with only a handful of companies which dominate the market and dictate prices and policies.

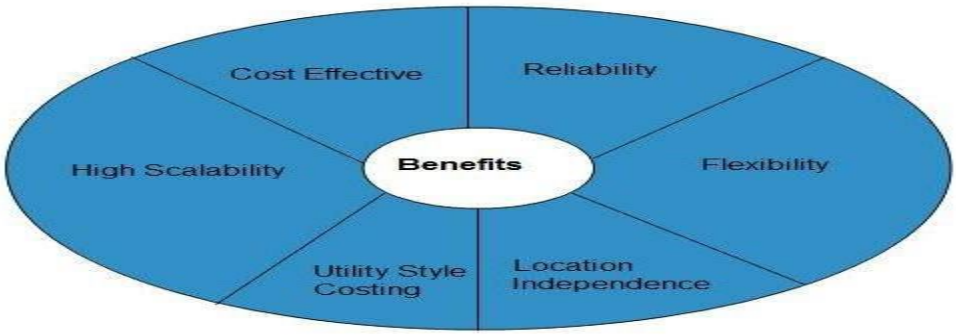
Public Cloud

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:



1. Cost Effective

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

2. Reliability

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

3. Flexibility

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

4. Location Independence

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

5. Utility Style Costing

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

6. 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:

1. Low Security

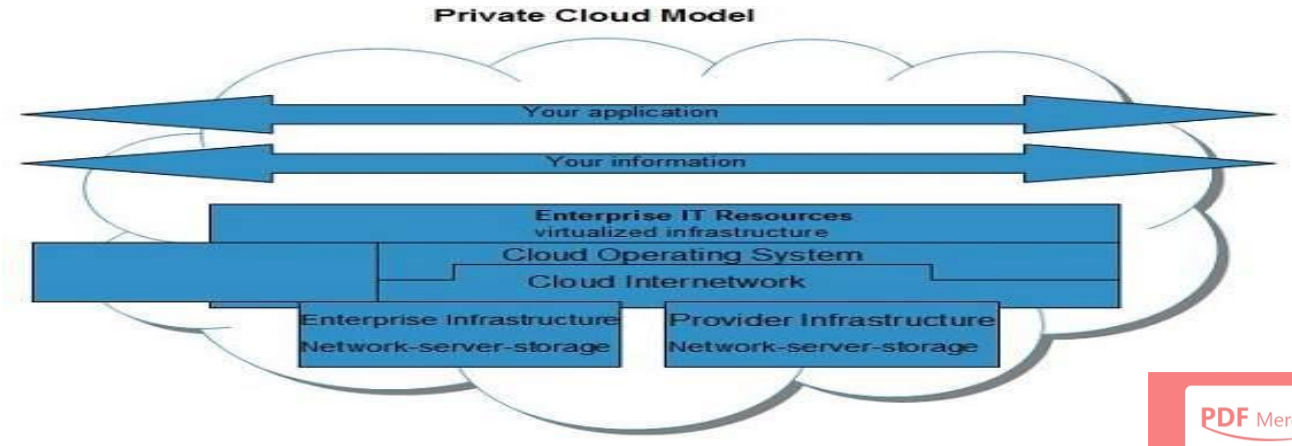
In public cloud model, data is hosted off-site and resources are shared publicly, therefore does not ensure higher level of security.

2. Less Customizable

It is comparatively less customizable than private cloud.

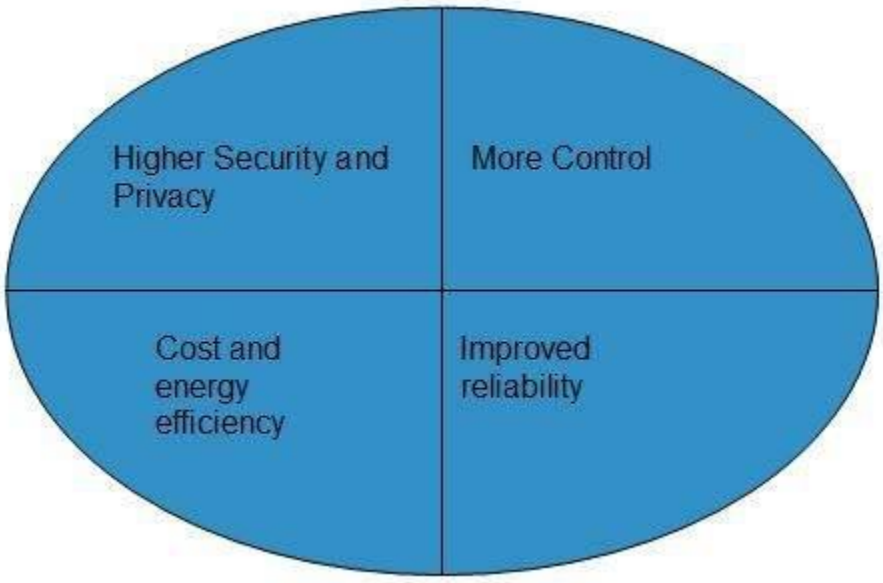
Private Cloud

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:



1. 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.

2. More Control

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

3. 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:

1. Restricted Area of Operation

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

2. High Priced

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

3. Limited Scalability

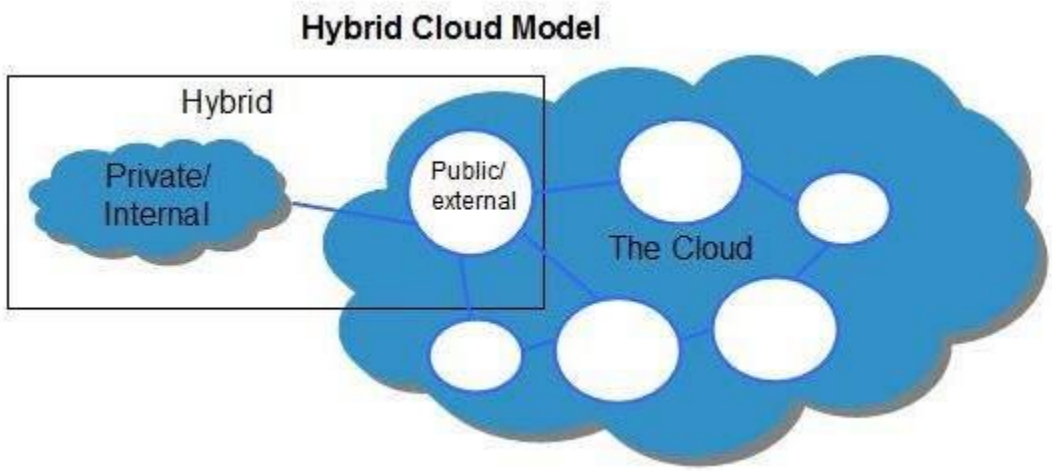
The private cloud can be scaled only within capacity of internal hosted resources.

4. Additional Skills

In order to maintain cloud deployment, organization requires skilled expertise

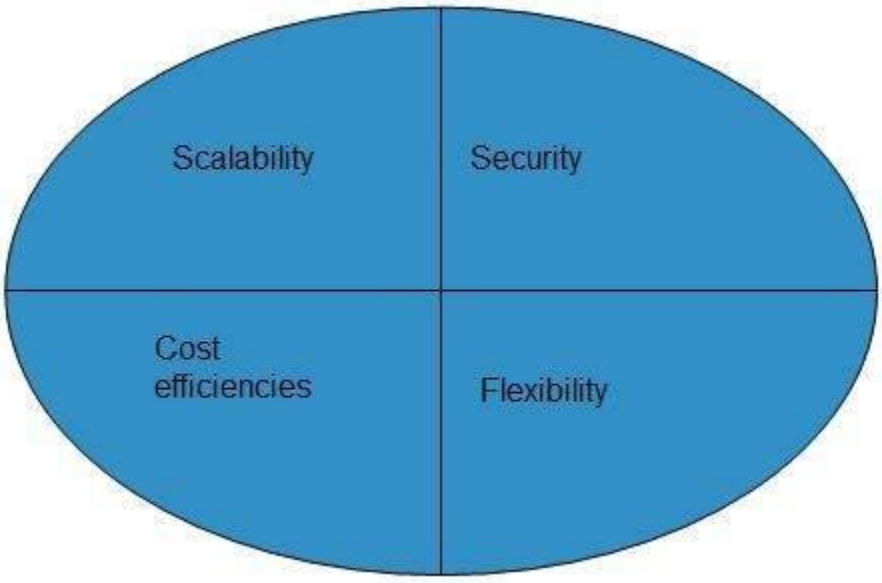
Hybrid Cloud Model

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:



1. Scalability

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

2. Flexibility

It offers secure resources and scalable public resources.

3. Cost Efficiency

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

4. Security

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

Disadvantages

1. Networking Issues

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

2. Security Compliance

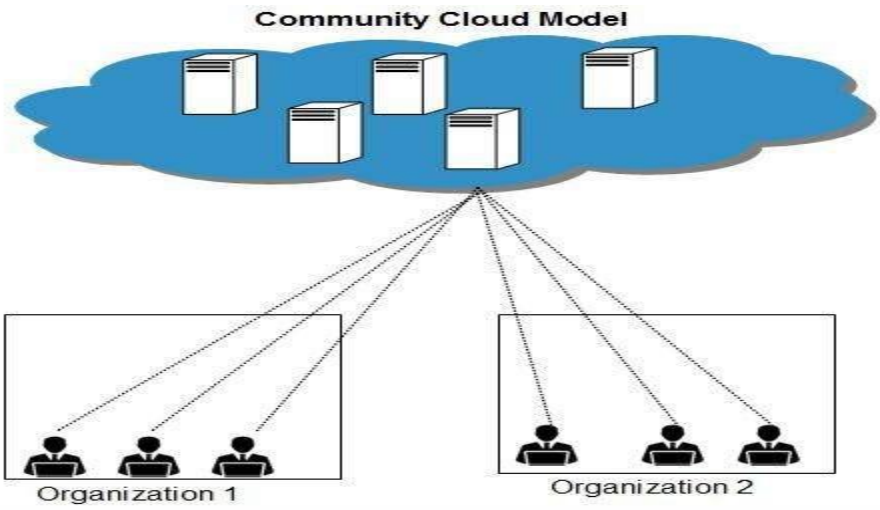
It is necessary to ensure that cloud services are compliant with security policies of the organization.

3. Infrastructure Dependency

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

Community Cloud

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.**

1. Cost Effective

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

2. Sharing Among Organizations

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

3. Security

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

Chapter-2

Cloud Service Models

2.1. Communication as a Service (CaaS):

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

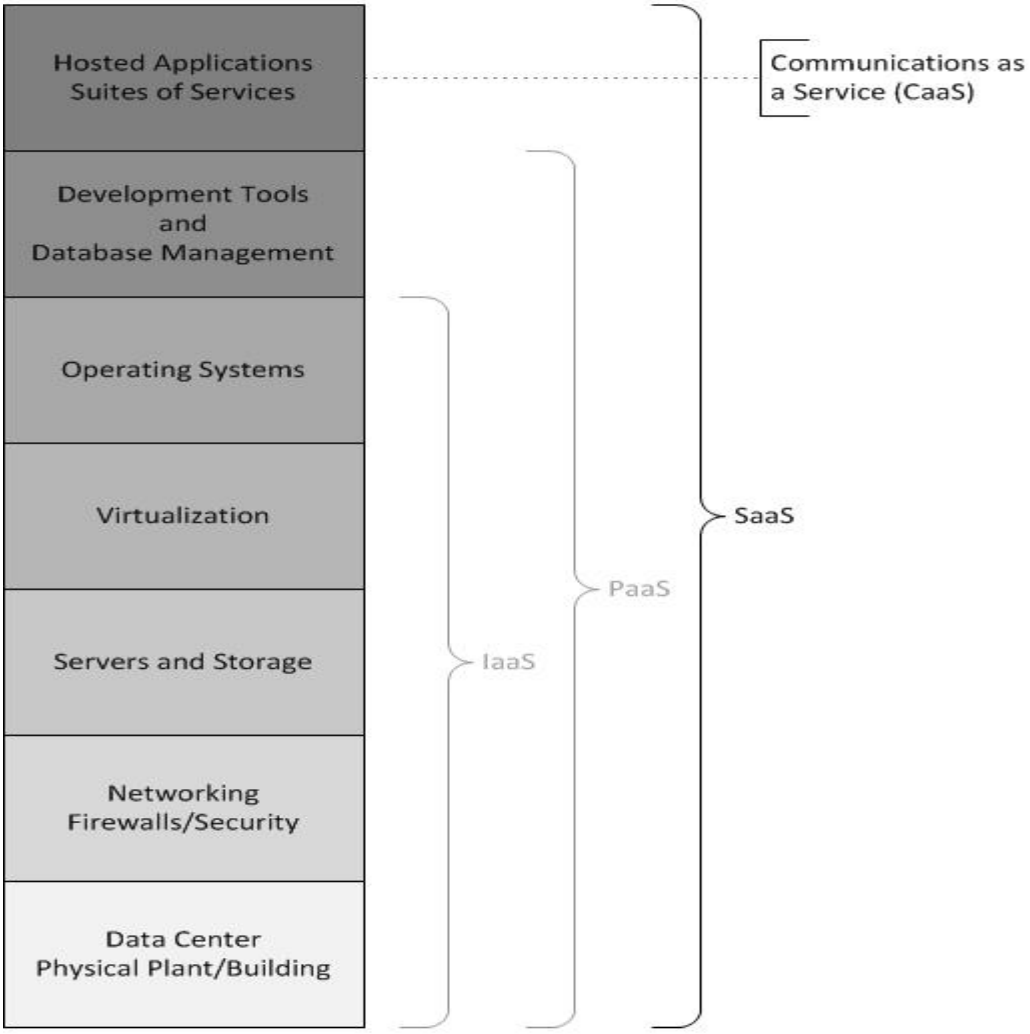


Fig: Cloud Service Models

CaaS brings social networking, cloud computing, and smartphones together, providing cloud technologies that let users communicate via voice, text, and rich media on whatever device they prefer to use. To compete in this marketplace, software vendors, enterprises, and service providers

must introduce communications-enhanced services that meet a surging need for value, efficiency, cost reduction, and convenience.

Through the hosted model, the CaaS provider manages everything, from the telecommunications infrastructure to the software integration platform for delivering communications offered at a guaranteed Quality of Service (QoS). As a result, businesses can selectively deploy communications features, applications, and devices on a pay-as-you-go, as-needed basis, reducing risks while eliminating capital costs associated with new services.

CaaS offers flexibility and expandability that small and medium-sized business might not otherwise afford, allowing for the addition of devices, modes or coverage on demand. The network capacity and feature set can be changed from day to day if necessary so that functionality keeps pace with demand and resources are not wasted. There is no risk of the system becoming obsolete and requiring periodic major upgrades or replacement.

Advantages of Communication as a Service (CaaS):

- **Fully Integrated Enterprise Class Unified Communication**: By managing the LAN/WAN, the vendor can guarantee consistent Quality of Service (QoS) from the desktop across the VoIP backbone and back again. Advanced Unified Communications features such as Outlook integration, soft phones, real-time presence, chat, multimedia conferencing, video calling, unified messaging and mobility are also part of a standard CaaS deployment. And with CaaS, the feature set can continue to evolve. Development and introduction of new features and applications are faster, easier and more economical because the service provider is doing the work for multiple end users across a scalable platform
- **No Upfront Capital Expenses:** Since cloud services are supposed to lower capital expenditure and focus more on operating expenditure, by implementing CaaS, consumers can build up their communication infrastructure without any upfront cost. They just need to pay it as a service.
- **Flexibility in Features:** Since cloud is a multi-tenant architecture, cloud vendors have to manage multiple customers and look after the features that they want. What this allows cloud vendor is to add more advanced features and flexibility in their service model. Economies of scale also mean that the service provider is not tied to a single vendor investment and can leverage bestof-breed providers like Cisco, Microsoft and Nortel much more economically than an independent enterprise.

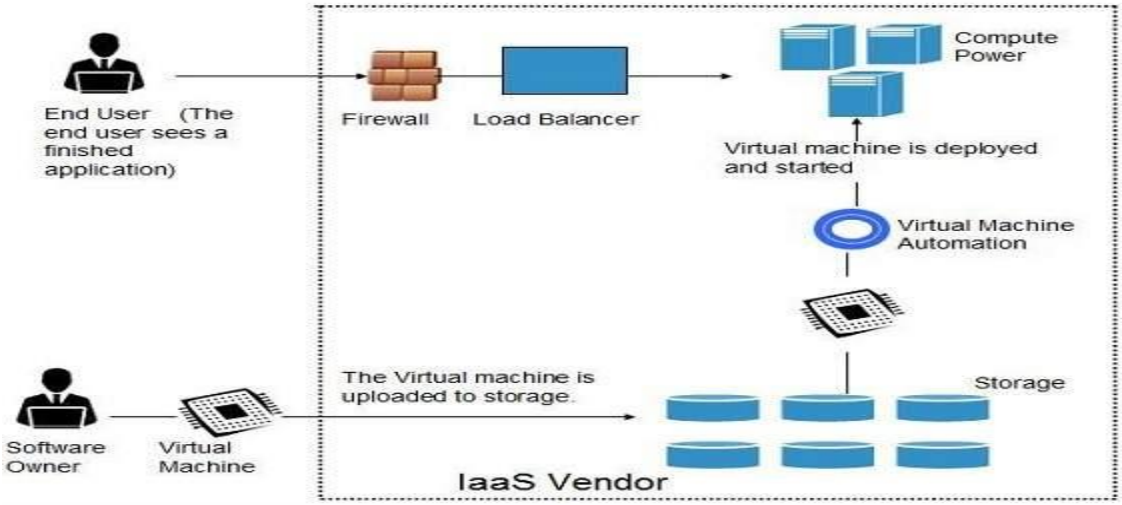
- **No Risk of Obsolescence:** Technology changes rapidly and are obsolete within few years of introduction. With CaaS, companies are always privileged with new technologies as cloud vendors keep on updating their equipment's and technologies to sustain in market.
- **No Data Center Cost:** As a prime advantages of cloud computing, while using CaaS infrastructure, organization need not invest on expensive servers, cooling system and electric equipment. With monthly/ yearly recurring cost, organization can dramatically cut down the management cost of data center as well.
- **Guaranteed Business Continuity:** With CaaS, organization can be hugely benefitted with guaranteed business continuity as cloud service providers proactively plans for Business Continuity Planning for their customers. Service uptime is guaranteed even if any catastrophic disaster strikes.

2.2 Infrastructure-as-a-Service

It 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.



Advantage of IaaS:

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:

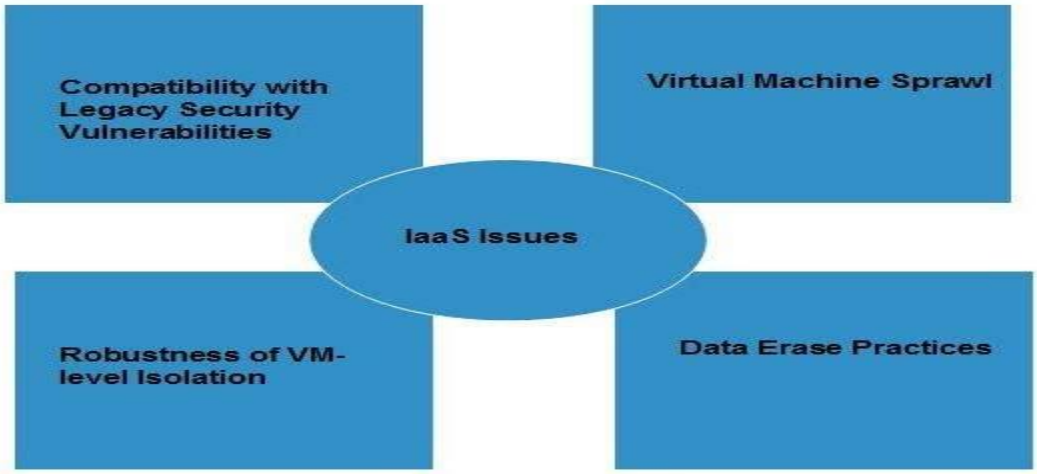
IaaS resources such as virtual machines, storage devices, bandwidth, IP addresses, monitoring services, firewalls, etc. are made available to the customers on rent. The payment is based upon the amount of time the customer retains a resource. Also with administrative access to virtual machines, the customer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



a. 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.

b. 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.

c. 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.

d. 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.

On-demand Computing:

On-demand computing is a delivery model in which computing resources are made available to the user as needed. The resources may be maintained within the user's enterprise, or made available by a cloud service provider. When the services are provided by a third-party, the term cloud computing is often used as a synonym for on-demand computing.

Amazon's Elastic Cloud:

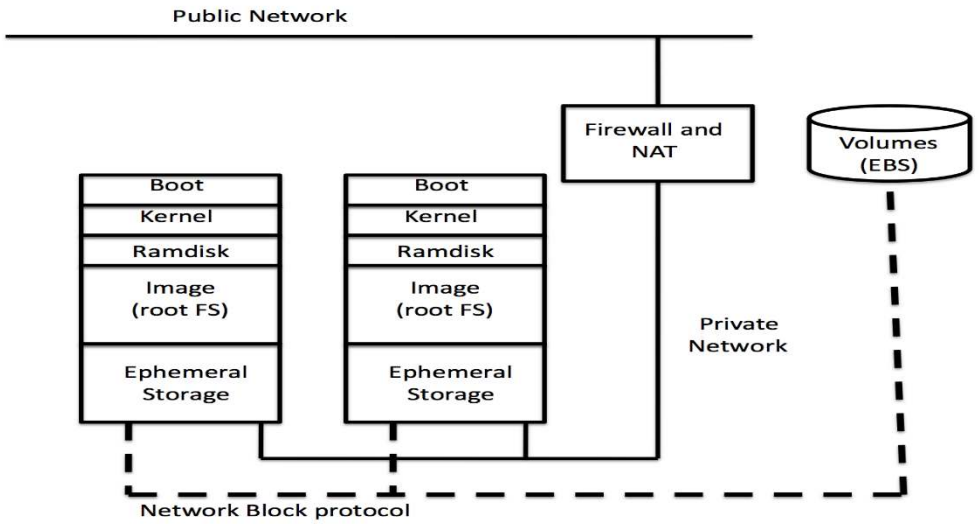
Amazon Elastic Compute Cloud (Amazon EC2) is an Amazon Web Service (AWS) you can use to access servers, software, and storage resources across the Internet in a self-service manner. It provides scalable, pay as-you-go compute capacity. It is said to be an elastic since it is scalable in both direction along the client as well as service provider. Amazon EC2 provides the following features:

- Virtual computing environments, known as *instances*
- Preconfigured templates for your instances, known as *Amazon Machine Images (AMIs)*, that package the bits you need for your server (including the operating system and additional software)
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as *instance types*
- Secure login information for your instances using *key pairs* (AWS stores the public key, and you store the private key in a secure place)
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as *instance store volumes*
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as *Amazon EBS volumes*
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as *regions* and *Availability Zones*
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using *security groups*
- Static IPv4 addresses for dynamic cloud computing, known as *Elastic IP addresses*
- Metadata, known as *tags*, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds*(VPCs)

Amazon's EC2 provides essentially three functionalities:

- virtual machine provisioning
- network provisioning (including firewalls)
- block storage provisioning (persistent volumes)

It use the following service model:



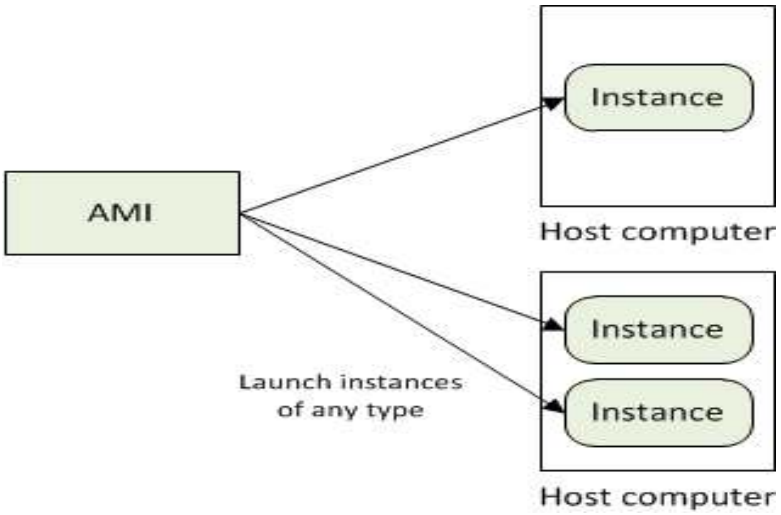
EC2 includes following components:

- AMI & Instance
- Region & Zones
- Storage
- Networking and Security
- Monitoring
- Auto Scaling
- Load Balancer

AMI and Instance

Amazon Machine Image (AMI) is a template for software configuration (Operating System, Application Server, and Applications). Amazon publishes many AMI for public use and Custom AMIs provided by community members. In this platform, user can create their own AMI.

Instance is an AMI running on virtual servers in the cloud and instance type specifies the different operating environment. Each *instance type* offers different compute and memory facilities to each user.



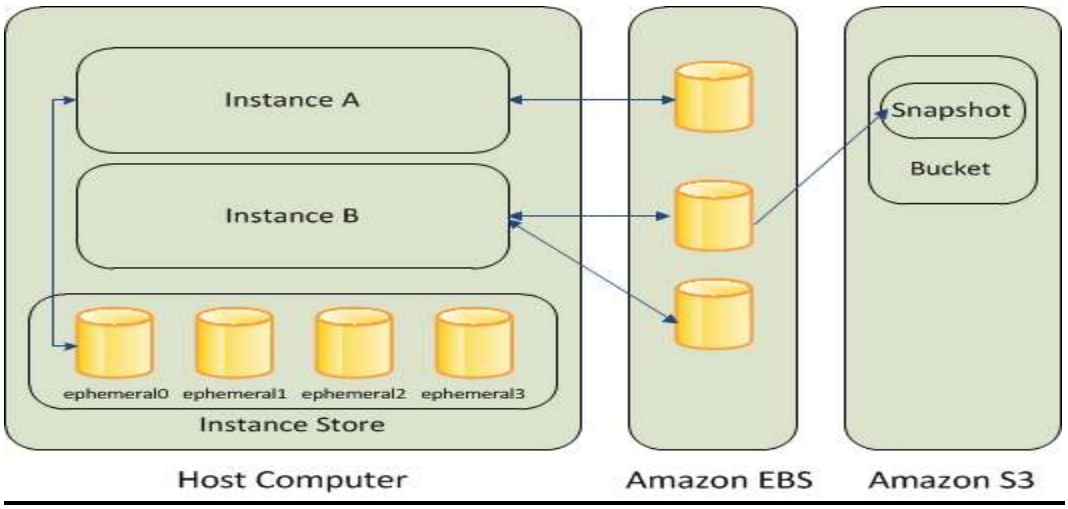
Region and Zones:

Amazon have data centers in different region across the globe for example North America, Europe, and Asia. Prices for Amazon EC2 usage vary by region. An instance can be launched in different regions depending on the need. It depends on

- Closer to specific customer
- To meet legal or other requirements

Each region has set of zones and Zones are isolated from failure in other zones. When each region contains multiple distinct locations then it is called as *Availability Zones*. Inexpensive, low latency connectivity between zones in same region must be maintained to provide the better service.

Storage:



Amazon EC2 provides three type of storage option

- Amazon EBS
- Amazon S3

- Instance Storage

Amazon EBS (Elastic Block Store) provides with persistent, block-level storage. Basically additional Hard Disk that you can attach to instance. It is suitable for apps which require database, file system, and block level storage. User can Create, Attach, Detach, Delete the storage as per requirement.

When the EBS be partitions into no of small dedicated volume then it is called S3 storage. By taking snapshots that is stored in S3, a new EBS can be re-created using the snapshot. S3 simple storage service storage for the Internet or web service interface that enables you to store and retrieve any amount of data from anywhere on the web.

Storage physically attached to the computer is called as Instance Storage. Instance store comes with each instance except the micro-one, temporary block level storage.

Networking and Security:

Instances can be launched on one of the two platforms

- ✓ EC2-Classic
- ✓ EC2-VPC

VPC launch Amazon Web Services (AWS) resources into a virtual network that you've defined. During the Configuration of VPC we select its IP address range, create subnets, and configure route tables, network gateways, and security settings. Instance IP address is dynamic since a new IP address is assigned every time instance is launched.

The Security Group be created that enables you to specify the protocols, ports, and source IP ranges that are allowed to reach your instances. In this model, we can create multiple security groups, assign instance to a particular group, and determine the traffic.

Monitoring, Auto Scaling, and Load Balancing:

In this model. We can monitor statistics of instances and EBS through the Cloud Watch. It is a tools that is used to monitor, manage, and publish various metrics of cloud service.

Amazon EC2 capacity be scaled up and down automatically so that it's called as elastic and based on following rules

- Add and remove compute resource based on demand
- Suitable for businesses experiencing variability in usage

The no of the load balancers are used to balance incoming traffic. It distributes incoming traffic across multiple instances and corresponding procedure is called Elastic Load Balancing.

Benefits of EC2

1. **Elastic Web-Scale Computing**

Amazon EC2 enables you to increase or decrease capacity within minutes, not hours or days. You can commission one, hundreds or even thousands of server instances simultaneously. Of course, because this is all controlled with web service APIs, your application can automatically scale itself up and down depending on its needs.

2. **Completely Controlled**

You have complete control of your instances. You have root access to each one, and you can interact with them as you would any machine. You can stop your instance while retaining the data on your boot partition and then subsequently restart the same instance using web service APIs. Instances can be rebooted remotely using web service APIs. You also have access to console output of your instances.

3. **Flexible Cloud Hosting Services**

You have the choice of multiple instance types, operating systems, and software packages. Amazon EC2 allows you to select a configuration of memory, CPU, instance storage, and the boot partition size that is optimal for your choice of operating system and application. For example, your choice of operating systems includes numerous Linux distributions, and Microsoft Windows Server.

4. **Designed for use with other Amazon Web Services**

Amazon EC2 works in conjunction with Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) and Amazon Simple Queue Service (Amazon SQS) to provide a complete solution for computing, query processing and storage across a wide range of applications.

5. **Reliable**

Amazon EC2 offers a highly reliable environment where replacement instances can be rapidly and predictably commissioned. The service runs within Amazon's proven network infrastructure and datacenters.

6. **Secure**

Amazon EC2 works in conjunction with Amazon VPC to provide security and robust networking functionality for your computer resources. Your compute instances are located in a Virtual Private Cloud (VPC) with an IP range that you specify. You decide which instances are exposed to the Internet and which remain private.

- Security Groups and networks ACLs allow you to control inbound and outbound network access to and from your instances.
- You can provision your EC2 resources as Dedicated Instances. Dedicated Instances are Amazon EC2 Instances that run on hardware dedicated to a single customer for additional isolation.
- If you do not have a default VPC you must create a VPC and launch instances into that VPC to leverage advanced networking features such as private subnets, outbound security group filtering, network ACLs and Dedicated Instances.

7. **Inexpensive**

Amazon EC2 passes on to you the financial benefits of Amazon's scale. You pay a very low rate for the compute capacity you actually consume.

- On-Demand Instances – On-Demand Instances let you pay for compute capacity by the hour with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs. On-Demand Instances also remove the need to buy "safety net" capacity to handle periodic traffic spikes.
- Reserved Instances – Reserved Instances provide you with a significant discount compared to On-Demand Instance pricing. There are three Reserved Instance payment options (No Upfront, Partial Upfront, All Upfront) that enable you to balance the amount you pay upfront with your effective hourly price.
- Spot Instances - Spot instances allow you to bid on spare Amazon EC2 computing capacity. Since Spot instances are often available at a discount compared to On-Demand pricing, you can significantly reduce the cost of running your applications, grow your application's compute capacity and throughput for the same budget, and enable new types of cloud computing applications.

8. Easy to Start

Quickly get started with Amazon EC2 by visiting the AWS Management Console to choose preconfigured software on Amazon Machine Images (AMIs). You can quickly deploy this software to EC2 via the EC2 console.

Monitoring-as-a-Service (MaaS):

Monitoring as a service (MaaS) is one of many cloud delivery models under anything as a service (XaaS). It is a framework that facilitates the deployment of monitoring functionalities for various other services and applications within the cloud. The most common application for MaaS is online state monitoring, which continuously tracks certain states of applications, networks, systems, instances or any element that may be deployable within the cloud.

MaaS offerings consist of multiple tools and applications meant to monitor a certain aspect of an application, server, system or any other IT component. There is a need for proper data collection, especially of the performance and real-time statistics of IT components, in order to make proper and informed management possible.

The tools being offered by MaaS providers may vary in some ways, but there are very basic monitoring schemes that have become ad hoc standards simply because of their benefits. State monitoring is one of them, and has become the most widely used feature. It is the overall monitoring of a component in relation to a set metric or standard. In state monitoring, a certain aspect of a component is constantly evaluated, and results are usually displayed in real time or periodically updated as a report. For example, the overall timeout requests measured in a period of time might be evaluated to see if this deviates from what's considered an acceptable value. Administrators can later take action to rectify faults or even respond in real time. State monitoring is very powerful because notifications now come in almost every form, from emails and text messages to various social media alerts like a tweet or a status update on Facebook.

Protection against Internal and External Threats in cloud computing:

Cloud services are becoming the main part of the infrastructure for many companies. Enterprises should pay maximum attention to security issues, moving away from typical approaches used in physical infrastructures, which are often insufficient in an atmosphere of constantly changing business requirements. Although cloud providers do all they can to guarantee infrastructure reliability, some of them limit their services to standard security measures, which can and should be significantly expanded. According to the Cloud Security Alliance the list of the main cloud security threats includes the following:

1. Data Leaks

Data in the cloud is exposed to the same threats as traditional infrastructures. Due to the large amount of data, platforms of cloud providers become an attractive target for attackers. Data leaks can lead to a chain of unfortunate events for IT companies and infrastructure as a service (IaaS) providers.

2. Compromising Accounts and Authentication Bypass

Data leaks often result from insufficient attention to authentication verification. More often than not, weak passwords in conjunction with poor management of encryption keys and certificates are to blame. In addition, IT organizations are faced with problems of managing rights and permissions when users are assigned with much greater powers than they actually need. The problem can also occur when a user takes another position or leaves the company: no one is in a rush to update permissions under the new user roles. As a result, the account has rights to more features than necessary.

Moreover, cloud environments are often prone to use of all kinds of phishing, scams, exploits and various attempts to manipulate data.

The threat may also come from current or former employees, system administrators, contractors or business partners. Insiders may have different motives, ranging from data theft to simple revenge. In the case of IaaS, the consequences of such actions can even take the form of full or partial infrastructure destruction, data access or even data destruction.

3. Interface and API Hacking

Today, it is impossible to imagine cloud services and applications without friendly user interfaces (UIs) and application program interfaces (APIs). The security and availability of cloud services depends on reliable mechanisms of data access control and encryption. Weak interfaces become bottlenecks in matters of availability, confidentiality, integrity and security of systems and data.

4. Cyber attacks

Targeted cyber attacks are common in our times. An experienced attacker, who has secured his presence in a target infrastructure, is not so easy to detect. Remote network attacks may have significant impact on the availability of infrastructure in general.

Despite the fact that denial-of-service (DoS) attacks have a long history, the development of cloud computing has made them more common. DoS attacks can cause business critical services to slow down or even stop. DoS attacks consume a large amount of computing power that comes with a hefty bill. Despite the fact that the principles of DoS attacks are simple at first glance, you need to understand their characteristics at the application level: the focus on the vulnerability of web servers, databases and applications.

5. Permanent Data Loss

Data loss due to malicious acts or accidents at the provider's end is no less critical than a leak. Daily backups and their storage on external protected alternative platforms are particularly important for cloud environments.

In addition, if you are using encryption before moving data to the cloud, it is necessary to take care of secure storage for encryption keys. As soon as keys fall into the wrong hands, data itself becomes available to attackers, the loss of which can wreak havoc on any organization.

6. Vulnerabilities

A common mistake when using cloud-based solutions in the IaaS model is paying too little attention to the security of applications, which are placed in the secure infrastructure of the cloud provider. And the vulnerability of applications becomes a bottleneck in enterprise infrastructure security.

7. Lack of Awareness

Organizations moving to the cloud without understanding the capabilities the cloud has to offer are faced with many problems. If a team of specialists is not very familiar with the features of cloud technologies and principles of deploying cloud-based applications, operational and architectural issues arise that can lead not only to downtime but also to much more serious problems.

8. Abuse of Cloud Services

The cloud can be used by legal and illegal businesses. The purpose of the latter is to use cloud resources for criminal activity: launching DoS attacks, sending spam, distributing malicious content, etc. It is extremely important for suppliers and service users to be able to detect such activities. To do this, detailed traffic inspections and cloud monitoring tools are recommended.

Protection Methodology:

In order to reduce risks associated with information security, it is necessary to determine and identify the levels of infrastructure that require attention and protection. For example, the computing level (hypervisors), the data storage level, the network level, the UI and API level, and so on.

Next you need to define protection methods at each level, distinguish the perimeter and cloud infrastructure security zones, and select monitoring and audit tools.

Enterprises should develop an information security strategy that includes the following, at the very least:

- Regular software update scheduling
- Patching procedures
- Monitoring and audit requirements
- Regular testing and vulnerability analysis

IaaS Information Security Measures:

Some IaaS providers already boast advanced security features. It is necessary to carefully examine the services and systems service providers offer at their own level, as well as conditions and guarantees of these offerings. Alternatively, consider implementing and utilizing them on your own.

1. **Data Encryption**

Encryption is the main and also the most popular method of data protection. Meticulously managing security and encryption key storage control is an essential condition of using any data encryption method.

It is worth noting that the IaaS provider must never be able to gain access to virtual machines and customer data.

2. **Network Encryption**

It is mandatory also to encrypt network connections, which is already a gold standard for cloud infrastructure.

3. **Access Control**

Attention must also be paid to access control, for example, by using the concept of federated cloud. With the help of federated services, it's easy to organize a flexible and convenient authentication system of internal and external users. The use of multi-factor authentication, including OTP, tokens, smart cards, etc., will significantly reduce the risks of unauthorized access to the infrastructure.

Be sure not to forget hardware and virtual firewalls as a means of providing network access control.

4. **Cloud Access Security Broker (CASB)**

A CASB is a unified security tool that allows administrators to identify potential data loss risks and ensure a high level of protection. The solution works in conjunction with the IaaS provider's cloud infrastructure by enabling users to monitor shared files and prevent data leakage. This way, administrators know where important content is stored and who has access to the data.

5. **Vulnerability Control**

Implementing and using vulnerability control, together with regular software updates, can significantly reduce the risks associated with information security, and it is an absolute must for both the IaaS provider and its clients.

6. Monitor, Audit and Identify Anomalies

Monitoring and auditing systems allow you to track standard indicators of infrastructure performance and identify abnormalities related to system and service security. Using deep packet inspection (DPI) or intrusion detection and prevention solutions (IDS/IPS) helps detect network anomalies and attacks.

7. Staff Training

Conducting specialized training and adopting a general attitude of focused attention to the technical competence of staff that have access to the virtual infrastructure will enhance the overall level of information security.

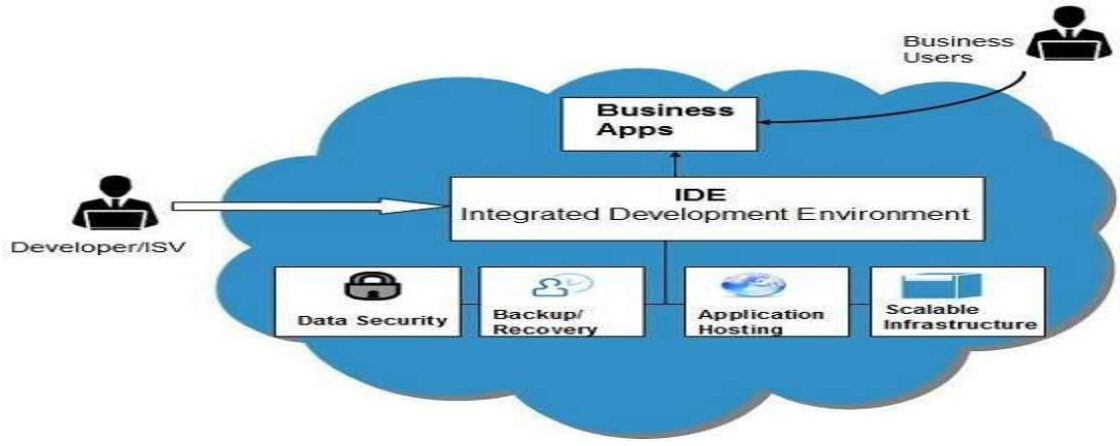
Platform-as-a-Service :

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.

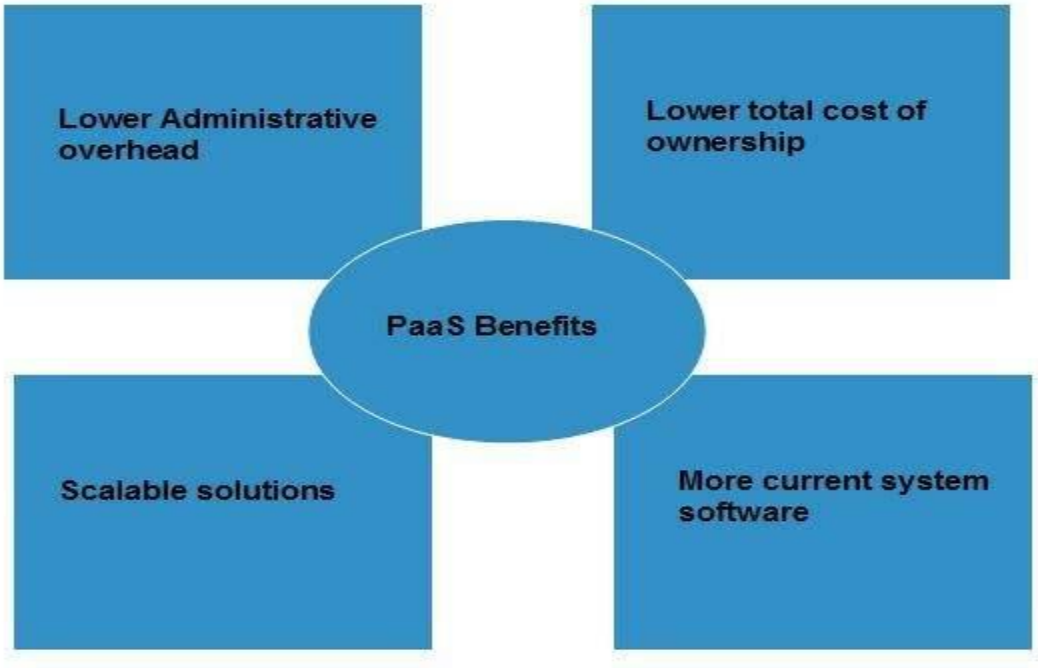
But the disadvantage of using PaaS is that, the developer locks-in with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

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:



1. Lower administrative overhead

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

2. Lower total cost of ownership

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

3. Scalable solutions

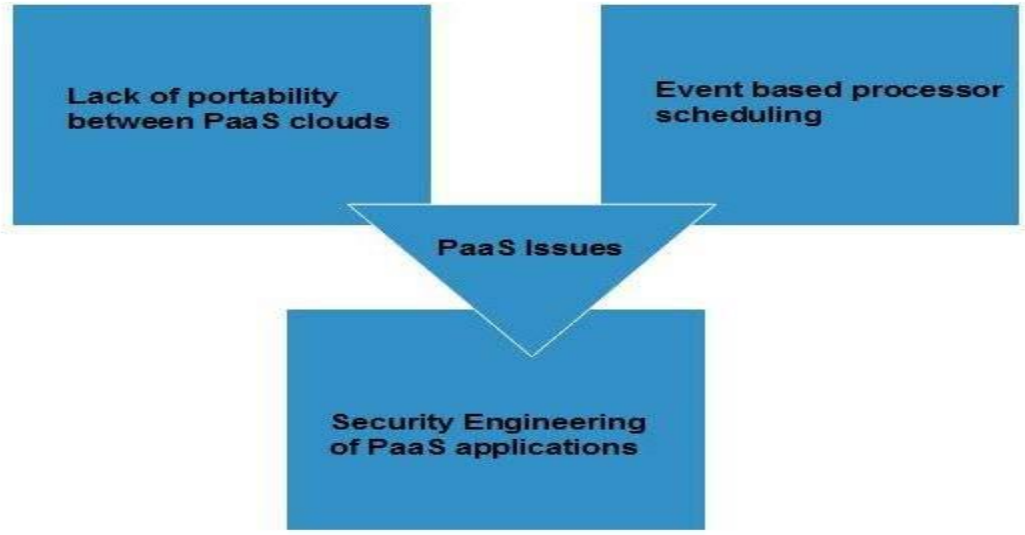
It is very easy to scale the resources up or down automatically, based on their demand.

4. 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:



1. 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.

2. 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.

3. Security engineering of PaaS applications

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

Characteristics

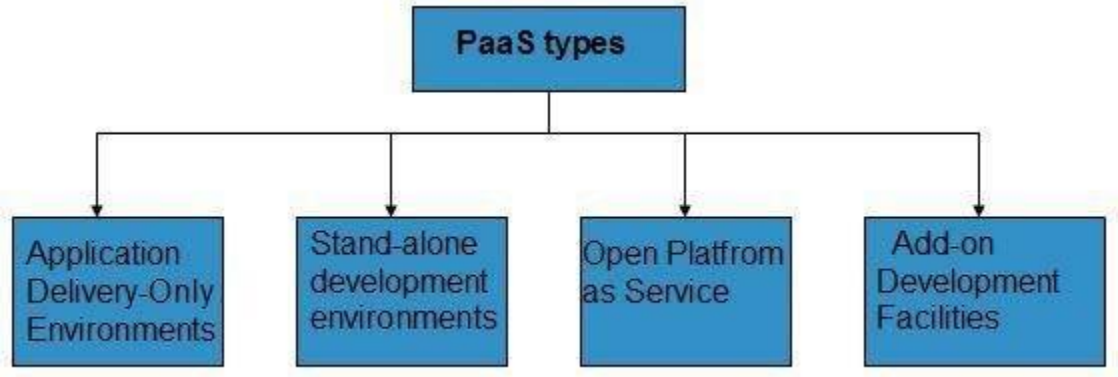
Here are the characteristics of PaaS service model:

- 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:



1. 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.

2. Application delivery-only environments

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

3. Open platform as a service

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

4. Add-on development facilities

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

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

1. **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

2. 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.

3. 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.

4. **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.

5. 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

1. 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.

2. 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.

3. **Lack of portability between SaaS clouds**

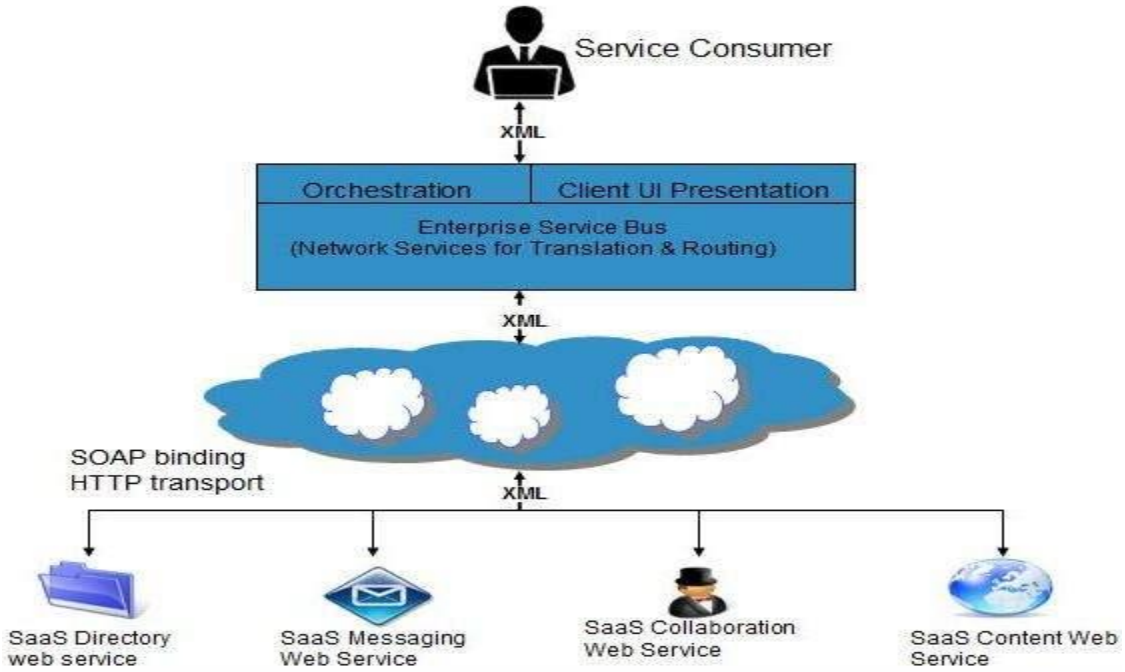
Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.

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:



SOA presents services for solution logic in an architectural model. By having these services as the foremost method of sending solutions, SOA's goal is to be more efficient, productive, and agile than other technology solutions. It provides support for realizing the advantages of computing and principles that are service-oriented. SOA implementations are made of various products, technologies, programming interfaces (for applications), and other different extensions. Application of the service-orientation principles to the software solutions will produce services. These services are the basic logic unit in SOA. Although the services have the ability to exist automatically, they're by no means isolated. There are certain standard and common features that are maintained by the services, but they have the ability to be extended and evolved independently. It's possible to combine services, enabling other services to be created. There are autonomous messages that are used for services to communicate and these messages are intelligent enough so that they can self-govern the parts of their own logic. The most important principles of SOA are service contract, autonomy, reusability, composability, loose coupling, discoverability, and statelessness.

Jericho Cloud Cube Model

Cloud computing offers a huge possibility for scalability, at almost instantaneous availability and low cost. Business managers requires IT operations to assess the risks and benefit this representation of computing model. The Jericho forum is an independent group of international information security leaders, have added their input as to how to collude securely in the clouds. The Jericho Cloud Cube Model portrays the multidimensional elements of cloud computing, that frames not only cloud use cases but also how they are set up and used.

Objectives of Jericho Forum:

The Jericho Forum's objectives associated to cloud computing are unique – "enabling secure combination in the appropriate cloud formations suited best to the business needs".

The Jericho forum:

- points out that in clouds not everything is best implemented; it may be best to conduct some business functions using a conventional non-cloud approach
- Explains the Jericho forum identified different cloud formations.
- describes benefits, key characteristics, and risks of each cloud formation
- Provide a framework for seeking in more detail the nature of different cloud formations and the issues that demands to answer to make secure places to work in and make them safe.

The Jericho Forum is actively supporting solution providers and merchants to develop the missing capabilities and services to assure customers are protected from the rough association of clouds.

Protecting our Data

First, it is necessary to categorize our data so as to know what rules must be applied to protecting it:

- Its sensitivity - must it exclusively exist at specific trust levels? If so, which?
- What supervisory /compliance restrictions apply – e.g. Must it remain within your national borders?

We only can meet this requirement if we have comprehensively adopted standards for:

- a data classification model that is easy enough for all originators of data to use – for eg the G8 Traffic Light Protocol
- an associated basis for managing trust levels
- Regulated metadata that signals to "cloud security" what security must be applied to each item of data.

With consideration of what security we must apply to our data, we're in a position to take decision:

- what data and processes to migrated to the Clouds
- At what level we want to perform in the Clouds? Cloud models isolate layers of business service from one another, for example, Infrastructure, Process, Platform, Software, and Process.
- Which Cloud composition are best suited to our needs.

Cloud Formations- the cloud cube model

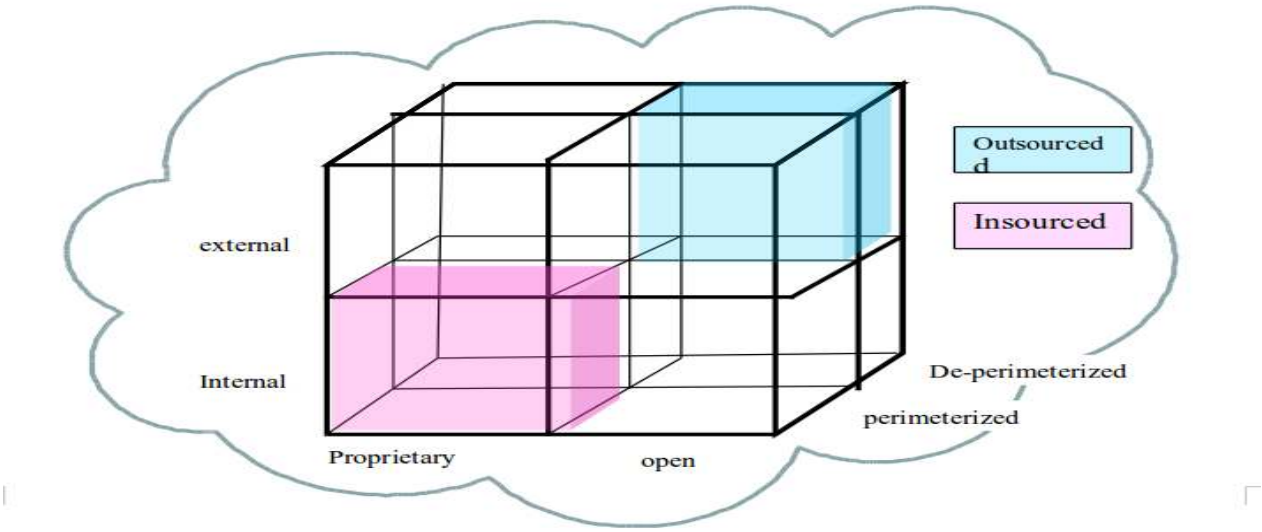


Fig: Cloud Cube Model

The Jericho forum has identified 4 gauge for judgment to differentiate cloud formations from each other and manner of their provisions. The cloud cube model summarizes these four dimensions.

Cloud Cube Model Dimensions

1. **Dimension: Internal (I) / External (E)**
2. **Dimension: Proprietary (P) / Open (O)**
3. **Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures**
4. **Dimension: Insourced / Outsourced**

1. Dimension: Internal (I) / External (E):

This dimension defines the physical location of the data such as where does the cloud form we want to use lie, inside or outside your organization's boundaries.

- It is Internal If it is within your own physical boundary.
- It is External If it is not within your own physical boundary.

For example, while Amazon SC33 would be external at some location "off-site, virtualized hard disks in an organization's data center will be internal.

2. Dimension: Proprietary (P) / Open (O)

This is the dimension that represents the state of ownership of the cloud technology, interfaces, services, etc. It indicates the degree of interoperability, allowing "data/application transportability" between other cloud forms and your own systems, and the ability to pull out your data from a cloud form or to migrate it to another without force.

- Proprietary means that the organization that provides the service is keeping the means of arrangement under their ownership. As a result, when functioning in clouds that are proprietary, you may not be allowed to move to another cloud provider without specific effort or investment. Mostly the more innovative technology progress occur in the proprietary realm. As such the proprietor may choose to accomplish restrictions through patents and by keeping the involved technology a trade secret.
- Open clouds use technology that is not proprietary, meaning that there are likely to be more suppliers, and user are not as strained in being able to share your data and using the same open technology collide with selected parties. Open services tend to be those that are consumerized and widespread, and apparently most likely a published open standard, for example, email (SMTP).

3. Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures

Architectural mindset is represented in the third dimension. De-parameterisation has always akin to the gradual failure, collapse, shrinking, and removal of the traditional IT perimeter based in silo.

- Perimeterised indicates continuing to operate within the classical IT perimeter, often indicated by "network firewalls". This approach discourages collaboration. When operating in the parameterised areas, you may simply prolong your own organization's perimeter using a VPN and operating the virtual server in your own IP domain into the external cloud computing domain, using your own directory services for access control. Then, when the computing task is finished you can pull out your perimeter back to its original classical position.
- De-perimeterised, considers that the system perimeter is architected succeeding the principles put forward in the Jericho Forum's Commandments and collusion Oriented Architectures Framework. In a de-perimeterised frame the data would be wrapped with meta-data and mechanisms that from inappropriate usage would protect the data .In a de-perimeterised environment an organization can associate securely with selected parties globally over COA capable network.

4. Dimension: Insourced / Outsourced

We define a 4th dimension having 2 states in every one of the 8 cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO), that answers to the question "Who do you want running our Clouds?":

- Outsourced: In outsourced dimension, the service is provided by a 3rd party
- Insourced: In insourced dimension the service is provided by your own staff under your control

These 2 states express who is managing the delivery of the cloud service(s) that you are using. This is generally a policy issue (i.e. not a technical or architectural decision but a business decision) which must be represented in a contract with the cloud service provider.

Chapter – 3

Building Cloud Networks

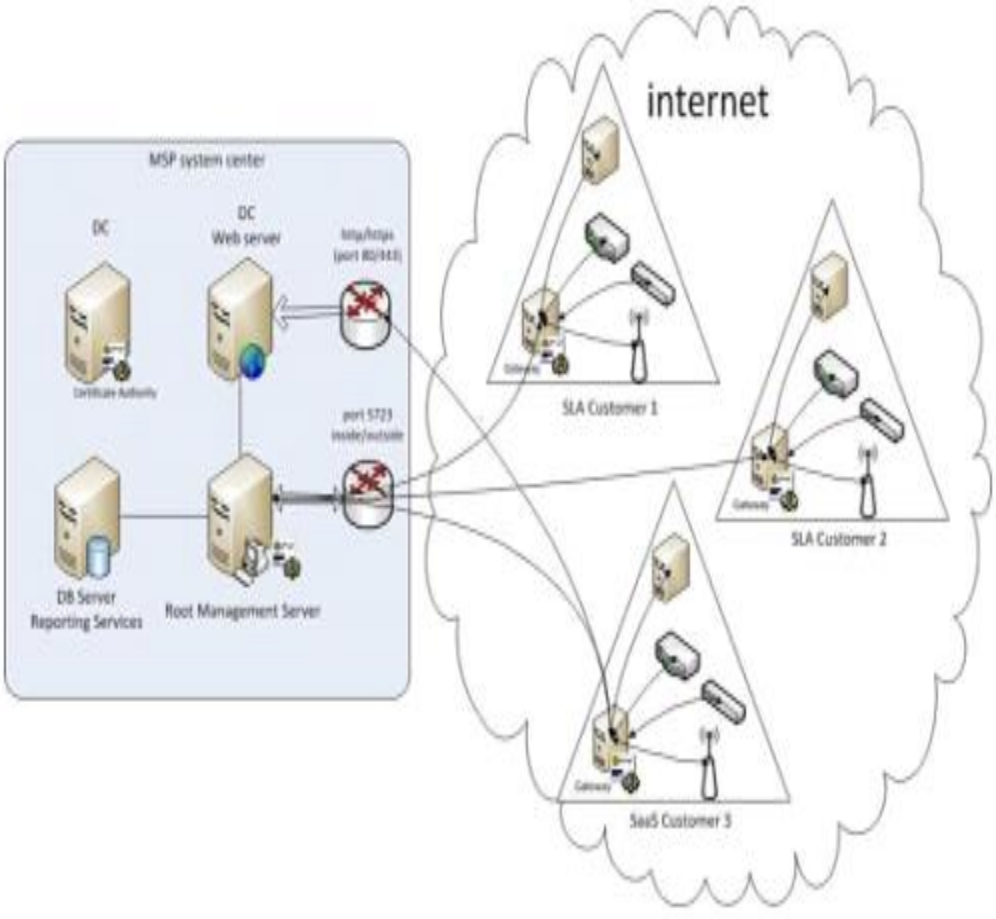
Managed service providers can be hosting companies or access providers that offer IT services such as fully outsourced network management arrangements, including IP telephony, messaging and call center management, virtual private networks (VPNs), managed firewalls and monitoring/reporting of network servers. Most of these services can be performed from outside a company's internal network with a special emphasis placed on integration and certification ofInternet security for applications and content.

MSPs serve as outsourcing agents for companies, especially other service providers like ISPs, that don't have the resources to constantly upgrade or maintain faster and faster computer networks.MSP can manage and integrate a range of activities associated with enterprise networks, including cloud storage. Managed service providers sometimes are referred to as management service providers. In the past, management service providers was used to describe infrastructure services delivered on a subscription basis, but with the advent of cloud computing, managed IT services and management services have become synonyms.

Evolution from Managed service providers (MSP) to Cloud Computing:

The first iteration of cloud computing can probably be traced back to the days of frame relay networks. Organizations with frame relay were essentially singular clouds that were interconnected to other frame relay-connected organizations using a carrier/provider to transport data communications between the two entities. Everyone within the frame network sharing a common Private Virtual Connection (PVC) could share their data with everyone else on the same PVC. To go outside their cloud and connect to another cloud, users had to rely on the infrastructure's routers and switches along the way to connect the dots between the clouds. The endpoint for this route between the clouds and the pathway was a demarcation point between the cloud and the provider's customer. Where the dots ended between the clouds (i.e., the endpoints) was where access was controlled by devices such as gateways, proxies, and firewalls on the customer's premises.

In the past, the concept of providing a service involved much more than inventing and designing the service, itself. The appropriate amount and quality of hardware was required for every company to not only build their service, but have and adequate amount of space to hold and maintain the hardware for the life of each service, as well. Fortunately, that on-premise era is slowly but surely passing, leaving those rather dated companies still attempting to manage their own server rooms, hung out to dry.



The Colocation

A few years later, colocation service providers solved the storage and maintenance issues by providing actual warehouses to store provided hardware. This transformation in the world of MSPs enabled companies to focus more on developing and enhancing their services, and less, if at all, on the headaches caused by hardware. Moving right along, the following level of managed service providers took a giant leap forward by even offering their own colocation hardware. This left companies solely responsible for their applications' deployment.

One Stop CAPX Shop

The time consuming hassle that once was hardware maintenance disappeared in the blink of an eye, however the revolution didn't stop there. On top of MSPs owning and maintaining all of the necessary hardware, an even further step forward included the actual deployment and management of the provided services or applications. These MSPs took full responsibility of ensuring a service or application's existence, abiding by the applicable SLA from top to bottom. What more could you wish for? With the weight of hardware and deployment management on the shoulders of the MSP, all of the bases seem to be covered…but at what cost? The aforementioned levels of service providers display wonderful achievements for the world of IT, unfortunately, each one also included a hefty capital expense and long term relationship. Today's on-demand mentality does not allot the time or funds that are coupled with the risks involved in those more traditional user-MSP relationships.

The Modern Cloud MSP

Opportunely, the next generation of MSPs not only fully understands this way of thinking, they utilize it themselves. Companies, like Emind, use the giant public cloud resources, such as AWS and Google, to provide a completely managed service that is deployed and monitored on hardware that they, themselves, purchase on-demand from the cloud. There are no hardware constraints or capital expense risks involved. Emind's strategy is to merely pass its risk free flexibility on to customers, consequently improving optimization due to the ability to select different types of instances. The modern cloud MSP has an obligation to ensure that customers' applications are run in an efficient manner.

SLA, Performance and Efficiency

By utilizing the cloud's infrastructure, we are able to offer customers the most advanced and available resources across the globe, at an extremely attractive price. Our comprehensive knowledge of the cloud has granted us the honor of being completely transparent with our customers while providing the optimal cloud environment. Akin to other next generation MSPs, we provide our customers with a set of tools which are essential to managing a cloud dynamic environment. With a faster time to market, you will find yourself ahead of the game with doors opening left and right to greater innovation, DevOps culture and the speed and agility you've always dreamed of. Emind is not your typical MSP…we are the future of what MSPs should be.

Single Purpose architectures to multi-purpose architectures:

In the early days of MSPs, the providers would actually go onto customer sites and perform their services on customer-owned premises. Over time, these MSPs specialized in implementation of infrastructure and quickly figured out ways to build out data centers and sell those capabilities off in small chunks commonly known as monthly recurring services, in addition to the basic fees charged for ping, power, and pipe (PPP). Ping refers to the ability to have a live Internet connection, power is obvious enough, and pipe refers to the amount of data throughput that a customer is willing to pay for. Generally, the PPP part of the charge was built into the provider's monthly service fee in addition to their service offerings.

Data center virtualization:

A data center (or datacenter) is a facility composed of networked computers and storage that businesses or other organizations use to organize, process, store and disseminate large amounts of data. A business typically relies heavily upon the applications, services and data contained within a data center, making it a focal point and critical asset for everyday operations. Virtualization is the ability to create multiple logical devices from one physical device i.e. Virtualization means that the services provided by a hardware device are abstracted from the physical hardware. VLANs and VRFs on the network, Volumes and LUNs on storage, and even our servers were virtualized.

Data center virtualization, which includes storage, desktop, and server virtualization, reduces overall IT equipment electrical load through consolidation of systems. The Concept of a virtualized data center means that every aspect of every piece of hardware is abstracted from every other piece of hardware.

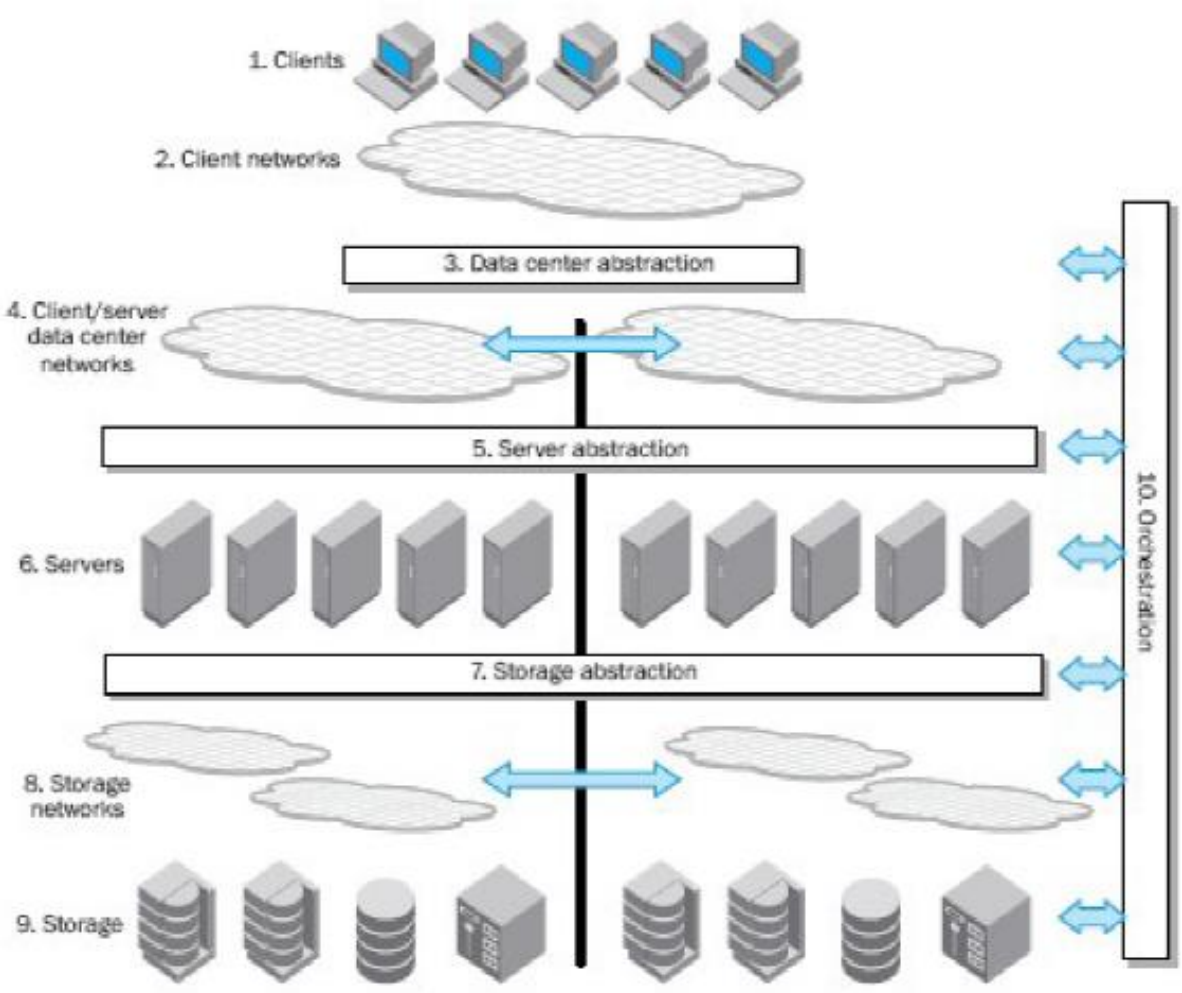


Fig: Building blocks of data centers

Benefits of Data Centre Virtualization:

Data center virtualization can reduce costs on facilities, power, cooling, and hardware and simplifies administration and maintenance. Following are the major benefit of data center virtualization.

- Pay for and consume the IT infrastructure as and when you need it
- Change capital expenditures to operating expenses
- Lower total cost of ownership of your IT infrastructure
- Increase the scalability of your infrastructure
- Decrease your time to market
- Reallocate staff to focus on value added activities rather than routine operations
- Increase IT capabilities and agility as business needs change

Cloud Computing Virtualization (Cloud data center)

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

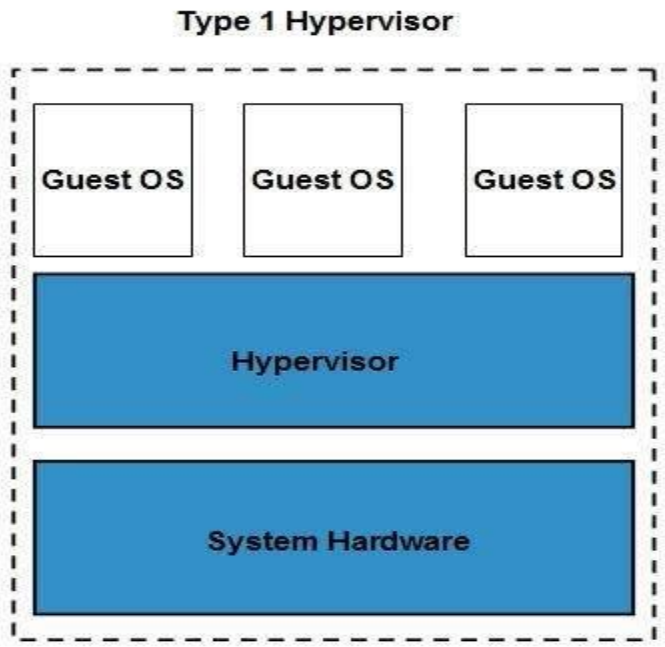
Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware.

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

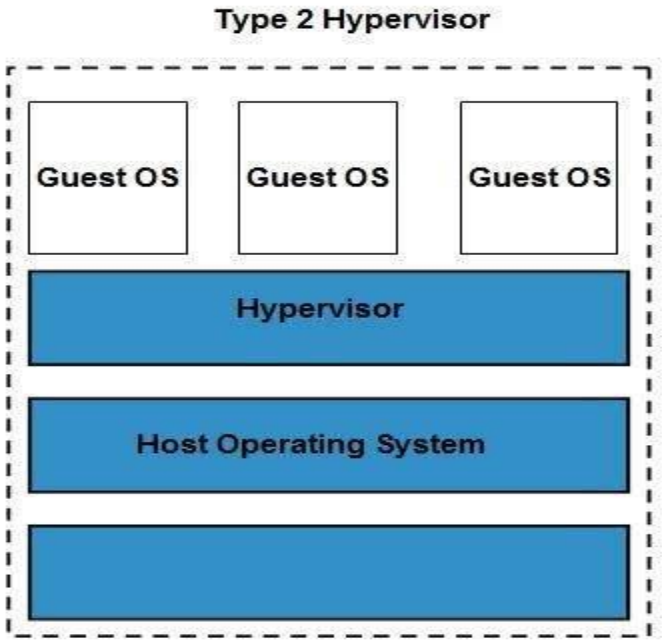
The hypervisor is a firmware or low-level program that acts as a Virtual Machine Manager. There are two types of hypervisor:

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.



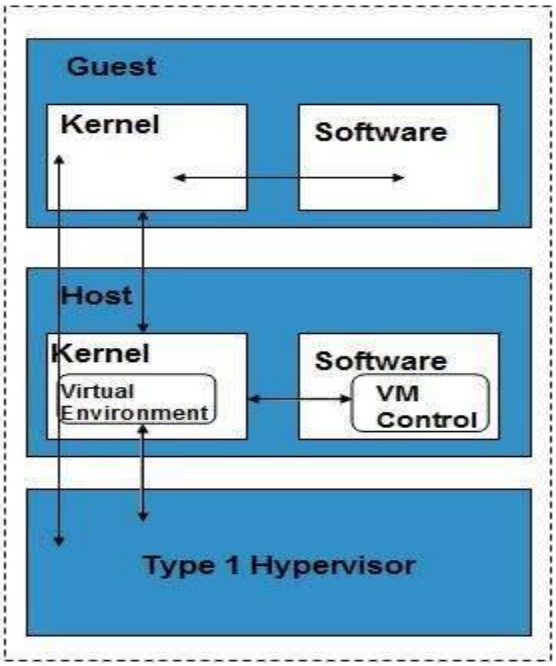
Types of Hardware Virtualization

Here are the three types of hardware virtualization:

- Full Virtualization
- Emulation Virtualization
- Paravirtualization

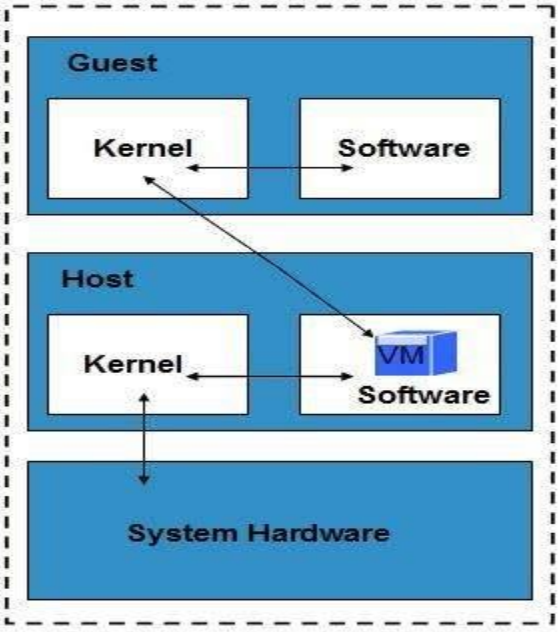
Full Virtualization

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



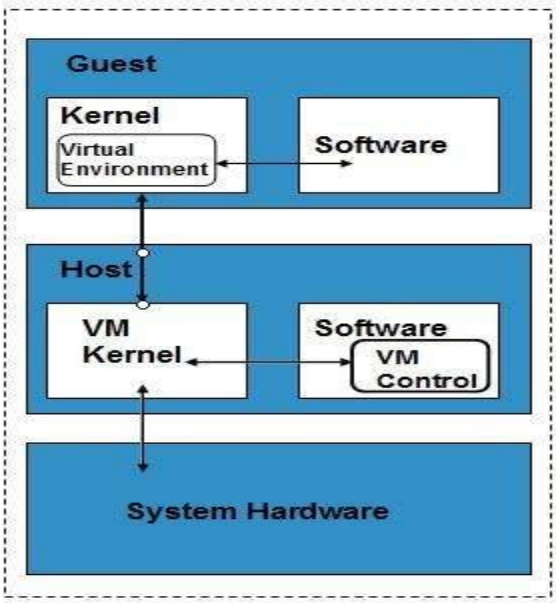
Emulation Virtualization

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.

Service Oriented Architectures (SOA):

A cloud has some key characteristics: elasticity, self-service provisioning, standards based interfaces, and pay as you go. This type of functionality has to be engineered into the software. To accomplish this type of engineering requires that the foundation for the cloud be well designed and well architected. What about cloud architecture makes this approach possible? The fact is that the services and structure behind the cloud should be based on a modular architectural approach. A modular, component-based architecture enables flexibility and reuse. A Service Oriented Architecture (SOA) is what lies beneath this flexibility.

SOA is much more than a technological approach and methodology for creating IT systems. It's also a business approach and methodology. Companies have used the principles of SOA to deepen the understanding between the business and IT and to help business adapt to change.

One of the key benefits of a service oriented approach is that software is designed to reflect best practices and business processes instead of making the business operate according to the rigid structure of a technical environment. A service-oriented architecture is essentially a collection of services. A service is, in essence, a function that is well defined, self-contained, and does not depend on the context or state of other services. Services most often reflect logical business activities. Some means of connecting services to each other is needed, so services communicate with each other, have an interface, and are message-oriented. The communication between

services may involve simple data passing or may require two or more services coordinating an activity. The services generally communicate using standard protocols, which allows for broad interoperability. SOA encompasses legacy systems and processes, so the effectiveness of existing investments is preserved. New services can be added or created without affecting existing services. Service-oriented architectures are not new. The first service-oriented architectures are usually considered to be the Distributed Component Object Model (DCOM) or Object Request Brokers (ORBs), which were based on the Common Object Requesting Broker Architecture (CORBA) specification. The introduction of SOA provides a platform for technology and business units to meet business requirements of the modern enterprise. With SOA, your organization can use existing application systems to a greater extent and may respond faster to change requests. These benefits are attributed to several critical elements of SOA:

1. Free-standing, independent components
2. Combined by loose coupling
3. Message (XML)-based instead of API-based
4. Physical location, etc., not important

Combining Cloud and SOA:

Cloud services benefit the business by taking the best practices and business process focus of SOA to the next level. These benefits apply to both cloud service providers and cloud service users. Cloud service providers need to architect solutions by using a service-oriented approach to deliver services with the expected levels of elasticity and scalability. Companies that architect and govern business processes with reusable service-oriented components can more easily identify which components can be successfully moved to public and private clouds. A service oriented architecture (SOA) is a software architecture for building business applications that implement business processes or services through a set of loosely coupled, black-box components orchestrated to deliver a well defined level of service. This approach lets companies leverage existing assets and create new business services that are consistent, controlled, more easily changed, and more easily managed. SOA is a business approach to designing efficient IT systems that support reuse and give the businesses the flexibility to react quickly to opportunities and threats.

Characterizing SOA :

The principal characteristics of SOA are described in more detail here:

- SOA is black-box component architecture. The black box lets you reuse existing business applications; it simply adds a fairly simple adapter to them. You don't need to know every detail of what's inside each component; SOA hides the complexity whenever possible.
- SOA components are loosely coupled. Software components are loosely coupled if they're designed to interact in a standardized way that minimizes dependencies. One loosely coupled component passes data to another component and makes a request; the second component carries out the request and, if necessary, passes data back to the first. Each component offers a small range of simple services to other components. A set of loosely coupled components does the same work that software components in tightly structured applications used to do, but with loose coupling you can combine and recombine the components in a bunch of ways. This makes a world of difference in the ability to make changes easily, accurately, and quickly.

SOA components are orchestrated to link through business processes to deliver a well-defined level of service. SOA creates a simple arrangement of components that, together, deliver a very complex business service. Simultaneously, SOA must provide acceptable service levels. To that end, the components ensure a dependable service level. Service level is tied directly to the best practices of conducting business, commonly referred to as business process management (BPM) — BPM focuses on effective design of business process and SOA allows IT to align with business processes.

Open Source Software in data centers:

Linux, Apache and other open-source applications have long been used to power Web and file servers. But when it comes to managing the data center, many companies have held back. Now, though, some users have turned into big believers that open source works here, too. In general, enterprises are using open source in the following three primary areas.

1. Web presence and portals - most common is Apache, used for content management, dynamic applications and a variety of e-commerce and catalog functions.
2. The small to medium-size database tier - most common are PostgreSQL and Oracles open-source Berkeley database.
3. The application tier - Java-based packages running on JBox, Apache Geronimo and Zend hosting Ajax applications.

Nowadays even the biggest companies like Google, Facebook and the like, run their data centers on almost 100% free software. Most of them even contribute back to the community too. Some of the open source software's used in data center are:

GlusterFS

Using FUSE (Filesystem in Userspace) to hook itself with the VFS (Virtual File System), GlusterFS creates a clutered network filesystem written in userspace, or, outside the kernel and its privileged extensions. GlusterFS uses existing filesystems like ext3, ext4, xfs, etc. to store data. The popularity of GlusterFS comes from the accessibility of a framework that can scale, providing petabytes of data under a single mount point. GlusterFS distributes files across a collection of subvolumes and makes one large storage unit from a host of smaller ones. This can be done across volumes on a single (or several) server. Volume can be increased by adding new servers, essentially on the fly. With replicate functionality, GlusterFS provides redundancy of storage and availability.

Ceph

Ceph's technical foundation is the Reliable Autonomic Distributed Object Store (RADOS), which provides applications with object, block, and file system storage in a single unified storage cluster. With libraries giving client applications direct access to the RADOS object-based storage system, users can leverage RADOS Block Device (RBD), RADOS Gateway, as well as the Ceph filesystem. The RADOS Gateway provides Amazon S3 and OpenStack compatible interfaces to the RADOS object store. Additionally, POSIX is a key feature in Ceph. POSIX semantics drive the interface with Ceph's traditional filesystem, so applications that use POSIX-compliant filesystems can easily use Ceph's object storage system. Additional libraries allow apps written in C, C++, Java, Python and PHP to also access the Ceph object storage FS. Advanced features include partial or complete read/writes, snapshots, object level key-value mappings, and atomic transactions with features like append, truncate and clone range. Ceph is also compatible with several VM clients.

OpenStack

Among the many architectural features of OpenStack, storage is one of the foundational cloud architecture necessities. Providing scalable, redundant object storage, OpenStack uses clusters of servers and can store petabytes of data. Through this distributed storage system, OpenStack adds to its feature list another area of scalability, redundancy and durability. Written to multiple disks across the data center, data replication is managed and replication ensured. For those that are mindful of budgets, the OpenStakc storage solution can write across older, smaller drives as well as newer, faster ones. Not satisfied with OpenStack storage? OpenStack is compatible with other storage solutions like Ceph, NetApp, Nexenta, SolidFire and Zadara. Additional features include snapshots (can be restored or used to create a new storage block), scaling (add new servers to scale and replicate data across), support for block storage, self-healing, a variety of powerful management tools for usage, performance, and general reporting, including auditing.

Sheepdog

Another distributed object storage solution, Sheepdog stands by its small codebase, simplicity and ease of use. Primarily for volume and container services, Sheepdog intelligently manages disks

and nodes to which it can scale out to by the thousands. Sheepdog can attach to QEMU VMs and Linux SCSI targets, also supporting snapshot, cloning and thin provisioning. It can also attach to other VMs and OS that run on baremetal hardware (iSCSI must be supported, however). Sheepdog has support for libvirt and OpenStack, can interface with HTTP Simple Storage, and has backend storage features like discard support, journaling, multi-disk on single node support, and erasure code support. With OpenStack Swift and Amazon S3 compatibility via web interface, Sheepdog can store and retrieve vast amounts of data.

Advantages of Open Source Cloud Computing Software

Open source cloud computing software can offer distinct advantages to organizations, often leveraging strong user and developer communities and aggressive release cycles. While there are a good number of commercial offerings on the market for building cloud infrastructure, before you start spending hard cash you may want to take a look at the open source options that are available. While often referred to as "alternatives" to commercial counterparts, open source cloud software is anything but. And in many cases, the open applications were the first cloud technology of their kind on the scene.

There are many reasons to turn to open source software for your cloud computing needs. Depending on the size of your business, you could see considerable savings when turning to one or more of these open applications

But there are other reasons that might compel you to try out these offerings. Many cloud computing open source projects have larger user bases. Because of the low barrier to implement the software, there is a wider number and variety of people using it, and often a vibrant community behind the software that acts as a support system. Typically, open source projects are innovative, with aggressive release cycles that push the technology forward. In fact, users often determine the next feature release cycle based on real-world business needs.

And, open source means open access to application programming interfaces (APIs) and the open standards they are written against. More transparency in the application code base often helps move the innovation forward and increase knowledgeable community support.

Across the many cloud computing service models, such as user cloud (a.k.a. software as a service), development cloud (a.k.a. platform as a service) and systems cloud (a.k.a infrastructure as a service), there are a large and diverse number of applications to choose from and both commercial and free open source offerings. As you'll notice, many of the open projects excel in their purpose because of the large, open communities of developers committed to creating innovative software and hoping to further cloud technology. Fortunately, there are open standards and many of the open source applications interface with one another, allowing you to pick and choose your apps and build a solid, interfaced cloud computing solution for your enterprise.

Examples of these applications and solutions include Salesforce.com, Google Docs, Red Hat Network, VMware Cloud Foundry, Google AppEngine, Windows Azure, Rackspace Sites, Red

Hat OpenShift, Active State Stackato, AppFog, EC2, Rackspace Cloud Files, OpenStack, CloudStack, Eucalyptus, OpenNebula and many more.

Chapter -4

Security in Cloud Computing

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:

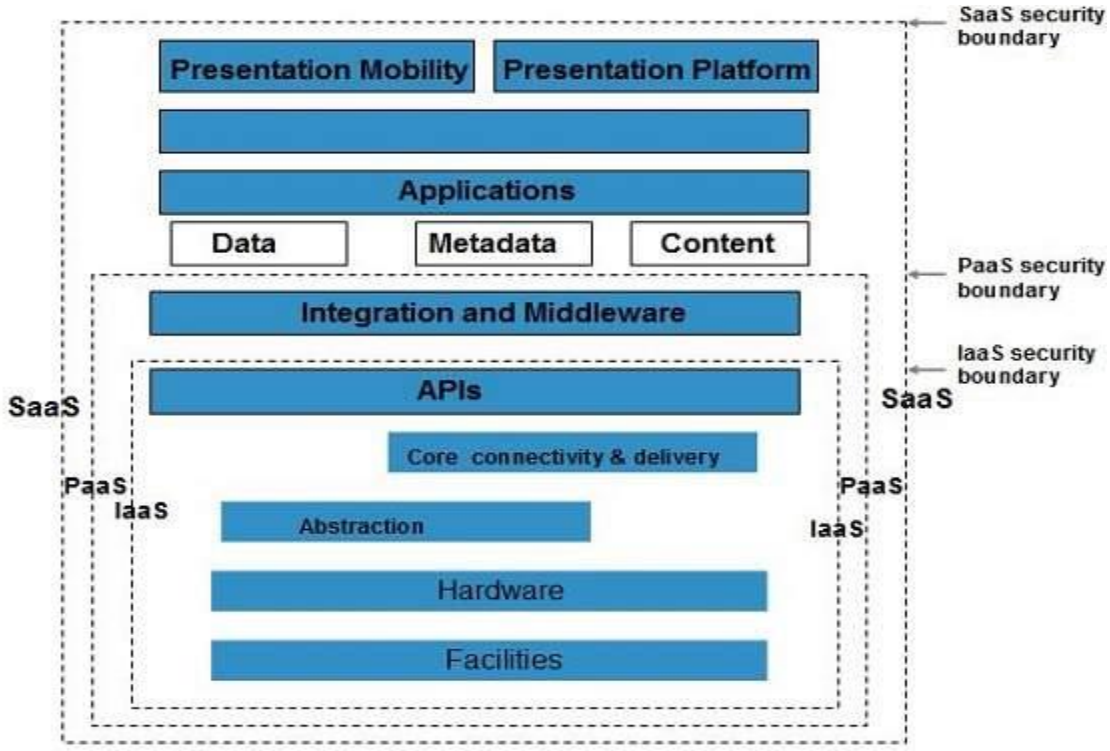
- ✓ Select resource that needs to move to the cloud and analyze its sensitivity to risk.
- ✓ Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.
- ✓ Consider the cloud type to be used such as public,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

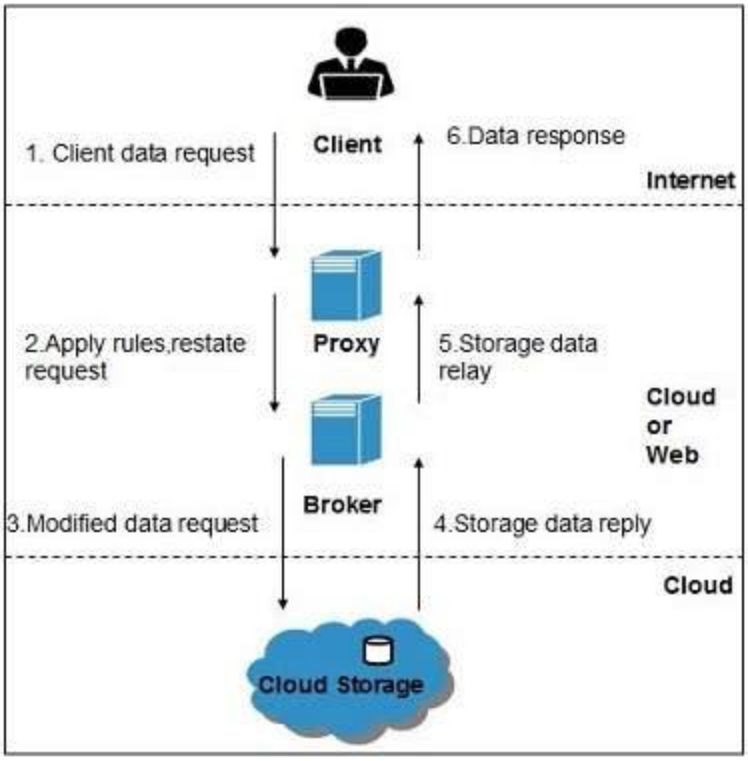
- ✓ A broker with full access to storage but no access to client.
- ✓ A proxy with no access to storage but access to both client and broker.

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 Security Challenges

In our technology driven world, security in the cloud is an issue that should be discussed from the board level. These challenges are:

1. **DDoS attacks:** A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.
2. **Data breaches:** Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in private, public and hybrid scenarios), some of those controls are relinquished to a trusted partner. Choosing the right vendor, with a strong record of security, is vital to overcoming this challenge.

3. **Data loss:** When business critical information is moved into the cloud, it's understandable to be concerned with its security. Losing data from the cloud, either though accidental deletion, malicious tampering (i.e. DDoS) or an act of nature brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.
4. **Insecure access points:** A behavioral web application firewall examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications from security breaches.
5. **Notifications and alerts:** Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough security plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

Cloud security challenges are not insurmountable. With the right partners, technology and forethought, enterprises can leverage the benefits of cloud technology.

Software as a Service Security:

The seven security issues which one should discuss with a cloud-computing vendor:

1. **Privileged user access** —inquire about who has specialized access to data, and about the hiring and management of such administrators.
2. **Regulatory compliance**—make sure that the vendor is willing to undergo external audits and/or security certifications.
3. **Data location**—does the provider allow for any control over the location of data?
4. **Data segregation** —make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
5. **Recovery** —Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
6. **Investigative support** —Does the vendor have the ability to investigate any inappropriate or illegal activity?
7. **Long-term viability** —What will happen to data if the company goes out of business? How will data be returned, and in what format?

To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves. The baseline security practices for the SaaS environment as currently formulated are discussed in the following sections.

Security Management (People):

One of the most important actions for a security team is to develop a formal charter for the security organization and program. This will foster a shared vision among the team of what security leadership is driving toward and expects, and will also foster "ownership" in the success of the collective team. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals. Morale among the team and pride in the team is lowered, and security suffers as a result.

Security Governance:

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. A charter for the security team is typically one of the first deliverables from the steering committee. This charter must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions. Lack of a formalized strategy can lead to an unsustainable operating model and security level as it evolves. In addition, lack of attention to security governance can result in key needs of the business not being met, including but not limited to, risk management, security monitoring, application security, and sales support. Lack of proper governance and management of duties can also result in potential security risks being left unaddressed and opportunities to improve the business being missed because the security team is not focused on the key security functions and activities that are critical to the business.

Risk Management:

Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy

controls. A formal risk assessment process should be created that allocates security resources linked to business continuity.

Risk Assessment:

Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals, and can lead to inefficient and ineffective selection of security controls that may not adequately mitigate information security risks to an acceptable level. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure. Doing so can help the product management and engineering groups to be more proactive in designing and testing the security of applications and systems and to collaborate more closely with the internal security team. Threat modeling requires both IT and business process knowledge, as well as technical knowledge of how the applications or systems under review work.

Security Monitoring and Incident Response:

Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring). Management of periodic, independent third-party security testing should also be included. Many of the security threats and issues in SaaS center around application and data layers, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and data-level activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threats and attacks to its customer data and service stability.

Third-Party Risk Management:

As SaaS moves into cloud computing for the storage and processing of customer data, there is a higher expectation that the SaaS will effectively manage the security risks with third parties. Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

Benefits of SaaS

Security-as-a-Service offers a number of benefits, including:

- Constant virus definition updates that are not reliant on user compliance.
- Greater security expertise than is typically available within an organization.
- Faster user provisioning.
- Outsourcing of administrative tasks, such as log management, to save time and money and allow an organization to devote more time to its core competencies.
- A Web interface that allows in-house administration of some tasks as well as a view of the security environment and on-going activities

Security Architecture Design:

A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, non-repudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting. A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance. A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans. Technology and design methods should be included, as well as the security processes necessary to provide the following services across all technology layers:

1. Authentication
2. Authorization

3. Availability

4. Confidentiality

5. Integrity

6. Accountability

7. Privacy

The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

Vulnerability Assessment:

Vulnerability assessment classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading. It measures the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and faster mitigation. Vulnerability management should be integrated with discovery, patch management, and upgrade management processes to close vulnerabilities before they can be exploited.

Data Privacy:

A risk assessment and gap analysis of controls and procedures must be conducted. Based on this data, formal privacy processes and initiatives must be defined, managed, and sustained. As with security, privacy controls and protection must an element of the secure architecture design. Depending on the size of the organization and the scale of operations, either an individual or a team should be assigned and given responsibility for maintaining privacy. A member of the security team who is responsible for privacy or a corporate security compliance team should collaborate with the company legal team to address data privacy issues and concerns. As with security, a privacy steering committee should also be created to help make decisions related to data privacy. Typically, the security compliance team, if one even exists, will not have formalized training on data privacy, which will limit the ability of the organization to address adequately the data privacy issues they currently face and will be continually challenged on in the future. The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

For example, customer contractual requirements/agreements for data privacy must be adhered to, accurate inventories of customer data, where it is stored, who can access it, and how it is used must be known, and, though often overlooked, Request for Interest/Request for Proposal questions regarding privacy must answered accurately. This requires special skills, training, and experience that do not typically exist within a security team. As companies move away from a service model under which they do not store customer data to one under which they do store customer data, the data privacy concerns of customers increase exponentially. This new service model pushes companies into the cloud computing space, where many companies do not have sufficient experience in dealing with customer privacy concerns, permanence of customer data throughout its globally distributed systems, cross-border data sharing, and compliance with regulatory or lawful intercept requirements.

Data Security:

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider. Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the United States. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS). True unified end-to-end security in the cloud will likely requires an ecosystem of partners.

Application Security:

Application security is one of the critical success factors for a world-class SaaS company. This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement. This should be a collaborative effort between the security and product development team. External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly. Fragmented and undefined collaboration on application security can result in lower-quality design, coding efforts, and testing results.

Virtual Machine Security:

In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments. By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely. To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.

This approach to virtual machine security, which connects the machine back to the mother ship, has some advantages in that the security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings for both the service provider and the enterprise.

Disaster recovery plan (DRP)

A disaster recovery plan (DRP) is a documented, structured approach with instructions for responding to unplanned incidents. This step-by-step plan consists of the precautions to minimize the effects of a disaster so the organization can continue to operate or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs. Before generating a detailed plan, an organization often performs a business impact analysis (BIA) and risk analysis (RA), and it establishes the recovery time objective (RTO) and recovery point objective (RPO).

Recovery strategies

A disaster recovery strategy should start at the business level and determine which applications are most important to running the organization. The RTO describes the target amount of time a business application can be down, typically measured in hours, minutes or seconds. The RPO describes the previous point in time when an application must be recovered. Recovery strategies define an organization's plans for responding to an incident, while disaster recovery plans describe how the organization should respond. In determining a recovery strategy, organizations should consider such issues as:

- ✓ Budget
- ✓ Resources -- people and physical facilities
- ✓ Management's position on risks
- ✓ Technology
- ✓ Data
- ✓ Suppliers

Management approval of recovery strategies is important. All strategies should align with the organization's goals. Once disaster recovery strategies have been developed and approved, they can be translated into disaster recovery plans.

Disaster recovery planning steps

The disaster recovery plan process involves more than simply writing the document. In advance of the writing, a risk analysis and business impact analysis help determine where to focus resources in the disaster recovery planning process. The BIA identifies the impacts of disruptive events and is the starting point for identifying risk within the context of disaster recovery. It also generates the RTO and RPO. The RA identifies threats and vulnerabilities that could disrupt the operation of systems and processes highlighted in the BIA. The RA assesses the likelihood of a disruptive event and outlines its potential severity. A DR plan checklist includes the following steps, according to independent consultant and IT auditor.

- ✓ Establishing the scope of the activity;
- ✓ Gathering relevant network infrastructure documents;

- ✓ Identifying the most serious threats and vulnerabilities, and the most critical assets;
- ✓ Reviewing the history of unplanned incidents and outages, and how they were handled;
- ✓ Identifying the current DR strategies;
- ✓ Identifying the emergency response team;
- ✓ Having management review and approve the disaster recovery plan;
- ✓ Testing the plan;
- ✓ Updating the plan; and
- ✓ Implementing a DR plan audit.

Disaster recovery plans are living documents. Involving employees -- from management to entry-level -- helps to increase the value of the plan.

Creating a disaster recovery plan

An organization can begin its DR plan with a summary of vital action steps and a list of important contacts, so the most essential information is quickly and easily accessible. The plan should define the roles and responsibilities of disaster recovery team members and outline the criteria to launch the plan into action. The plan then specifies, in detail, the incident response and recovery activities. Other important elements of a disaster recovery plan template include:

- ✓ Statement of intent and DR policy statement;
- ✓ Plan goals;
- ✓ Authentication tools, such as passwords;
- ✓ Geographical risks and factors;
- ✓ Tips for dealing with media;
- ✓ Financial and legal information and action steps; and
- ✓ Plan history.

Scope and objectives of DR planning

A disaster recovery plan can range in scope from basic to comprehensive. Some DRPs can be upward of 100 pages long.

Disaster recovery budgets can vary greatly and fluctuate over time. Organizations can take advantage of free resources, such as online DR plan templates from SearchDisasterRecovery or the Federal Emergency Management Agency. Several organizations, such as the Business Continuity Institute and Disaster Recovery Institute International, also provide free information and online how-to articles.

A disaster recovery plan checklist of goals includes identifying critical IT systems and networks, prioritizing the RTO, and outlining the steps needed to restart, reconfigure and recover systems and networks. The plan should at least minimize any negative effect on business operations. Employees should know basic emergency steps in the event of an unforeseen incident.

Distance is an important, but often overlooked, element of the DR planning process. A disaster recovery site that is close to the primary data center may seem ideal -- in terms of cost, convenience, bandwidth and testing -- but outages differ greatly in scope. A severe regional event can destroy the primary data center and its DR site if the two are located too close together.

Specific types of disaster recovery plans

DR plans can be specifically tailored for a given environment.

- **Virtualized disaster recovery plan.** Virtualization provides opportunities to implement disaster recovery in a more efficient and simpler way. A virtualized environment can spin up new virtual machine (VM) instances within minutes and provide application recovery through high availability. Testing can also be easier to achieve, but the plan must include the ability to validate that applications can be run in disaster recovery mode and returned to normal operations within the RPO and RTO.
- **Network disaster recovery plan.** Developing a plan for recovering a network gets more complicated as the complexity of the network increases. It is important to detail the step-by-step recovery procedure, test it properly and keep it updated. Data in this plan will be specific to the network, such as in its performance and networking staff.
- **Cloud disaster recovery plan.** Cloud-based disaster recovery can range from a file backup in the cloud to a complete replication. Cloud DR can be space-, time- and cost-efficient, but maintaining the disaster recovery plan requires proper management. The manager must know

the location of physical and virtual servers. The plan must address security, which is a common issue in the cloud that can be alleviated through testing.

- **Data center disaster recovery plan.** This type of plan focuses exclusively on the data center facility and infrastructure. An operational risk assessment is a key element in data center DR planning, and it analyzes key components such as building location, power systems and protection, security and office space. The plan must address a broad range of possible scenarios.

Types of disasters

A disaster recovery plan protects an organization from both human-made and natural disasters. There is not one specific way to recover from all kinds of disasters, so a plan should tackle a range of possibilities. A natural disaster may seem unlikely, but if it can happen in the organization's location, the DR plan should address it. According to independent consultant Edward Haletky, potential disasters to plan for include:

- ✓ Application failure
- ✓ VM failure
- ✓ Host failure
- ✓ Rack failure
- ✓ Communication failure
- ✓ Data center disaster
- ✓ Building disaster
- ✓ Campus disaster
- ✓ Citywide disaster
- ✓ Regional disaster
- ✓ National disaster
- ✓ Multinational disaster

Testing your disaster recovery plan

DR plans are substantiated through testing, which identifies deficiencies and provides opportunities to fix problems before a disaster occurs. Testing can offer proof that the plan is effective and hits

RPOs and RTOs. Since IT systems and technologies are constantly changing, DR testing also helps ensure a disaster recovery plan is up to date.

Reasons given for not testing DR plans include budget restrictions, resource constraints or a lack of management approval. Disaster recovery testing takes time, resources and planning. It can also be a risk if the test involves using live data.

DR testing can be simple to complex. In a plan review, a detailed discussion of the disaster recovery plan looks for missing elements and inconsistencies. In a tabletop test, participants walk through plan activities step by step to demonstrate whether disaster recovery team members know their duties in an emergency. A simulation test uses resources such as recovery sites and backup systems in what is essentially a full-scale test without an actual failover.

Cloud disaster recovery (cloud DR)

Cloud disaster recovery (cloud DR) is a backup and restore strategy that involves storing and maintaining copies of electronic records in a cloud computing environment as a security measure. The goal of cloud DR is to provide an organization with a way to recover data and/or implement failover in the event of a man-made or natural catastrophe.

There are a number of benefits that make cloud disaster recovery appealing, including the variety of ways it can be implemented: in-house, partially in-house or purchased as a service. This flexibility allows smaller enterprises to implement robust disaster recovery plans that would otherwise have been impossible. Typically, cloud providers charge for storage on a pay-per-use model, based on capacity, bandwidth or seat. Because the provider is in charge of purchasing and maintaining its storage infrastructure, the customer doesn't have to spend money on additional hardware, network resources, data center space and the personnel required to support them.

In addition to cost, there are other important issues to consider before adopting cloud-based disaster recovery:

- ✓ Does the organization have the necessary bandwidth and network resources to move data fast enough between the primary site and the cloud?
- ✓ Can the organization encrypt data in flight as it leaves the data center?

Failover, failback keys to cloud recovery

Effective cloud disaster recovery provides continuity for services and the ability to fail over to a second site if there is a hardware or software failure of IT systems. Workloads are then failed back to their original locations when the crisis is resolved. Failover and failback can be automated. Organizations should run tests at regular intervals on isolated network segments that do not impact production data.

Organizations can choose to fail over data, entire applications or virtual machine (VM) images. When data is failed over, it is available from file services in the cloud. However, cloud recovery can take a long time if there is a great deal of data. Application-based data can be replicated to another application running in the cloud. Or an entire VM image, including data, can be replicated to the cloud and powered up and accessed if there is an on-premises failover.

Cloud service-level agreements

Service-level agreements (SLAs) hold cloud providers accountable and establish recourses and penalties if providers don't live up to their promises about cloud services.

LAs can call for the provider to reimburse customers with credits if there is a service outage or data cannot be recovered during a disaster. Customers can usually apply credits toward their cloud bill or a subscription to another service, but these credits seldom make up for the loss of business if cloud recovery is delayed. Customers should also study SLAs to help formulate an exit strategy for the service.

SLAs for cloud disaster recovery can include guarantees for uptime, recovery time objectives (RTOs) and recovery point objectives. For instance, an RTO can be from one hour up to 24 hours or even longer, depending on how important an application is to restore the business. The faster the guaranteed restore time, the more expensive the service costs.

Cloud disaster recovery providers, vendors

Because the cloud removes the need to maintain a second site, DR is considered a prime use case for the cloud. Disaster recovery requires failing applications over to the cloud and failing back, so hundreds of vendors have sprung up to offer cloud DR services. The leading cloud DR as a

service vendors include Axcient, Bluelock, IBM Resiliency Services, iland, Microsoft Azure Site Recovery and SunGard Availability Services.

Traditional backup vendors, such as Acronis, Carbonite (EVault), Datto and Unitrends, have expanded into DR services. Amazon Web Services and VMware vCloud AirDisaster Recovery have also expanded into cloud DR. Other vendors providing cloud DR products and services include Databarracks, Windstream, Zerto and Zetta.