Catalog

UNIT III CLOUD ARCHITECTURE, SERVICES AND STORAGE

Layered Cloud Architecture Design – NIST Cloud Computing Reference Architecture – Public, Private and Hybrid Clouds - laaS – PaaS – SaaS – Architectural Design Challenges – Cloud Storage – Storage-as-a-Service – Advantages of Cloud Storage – Cloud Storage Providers – S3.

3.1 LAYERED ARCHITECTURE:

Generic Cloud Architecture Design:

An Internet cloud is envisioned as a public cluster of servers provisioned on demand to perform collective web services or distributed applications using data-center resources.

- ❖ Cloud Platform Design Goals
- ❖ Enabling Technologies for Clouds
- ❖ A Generic Cloud Architecture

Cloud Platform Design Goals

- □ Scalability
- □ Virtualization
- □ Efficiency
- □ Reliability
- □ Security

Cloud management receives the user request and finds the correct resources. Cloud calls the provisioning services which invoke the resources in the cloud. Cloud management software needs to support both physical and virtual machines

Enabling Technologies for Clouds

- □ Cloud users are able to demand more capacity at peak demand, reduce costs, experiment with new services, and remove unneeded capacity.
- □ Service providers can increase system utilization via multiplexing, virtualization and dynamic resource provisioning.
- □ Clouds are enabled by the progress in hardware, software and networking technologies
- □ Cloud users are able to demand more capacity at peak demand, reduce costs, experiment with new services, and remove unneeded capacity.
- □ Service providers can increase system utilization via multiplexing, virtualization and dynamic resource provisioning.

□ Clouds are enabled by the progress in hardware, software and networking technologies

Generic Cloud Architecture

□ The Internet cloud is envisioned as a massive cluster of servers.

□ Servers are provisioned on demand to perform collective web services using data-center resources.

□ The cloud platform is formed dynamically by provisioning or deprovisioning servers, software, and database resources.

□ Servers in the cloud can be physical machines or VMs.

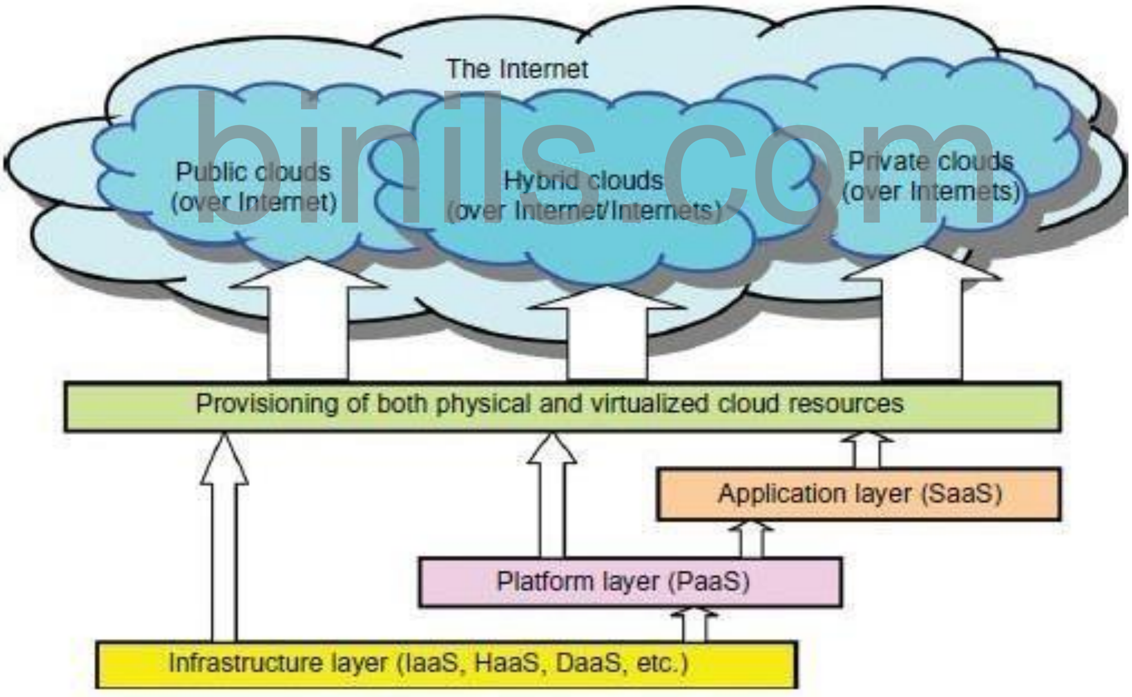
□ User interfaces are applied to request services.

- □ The cloud computing resources are built into the data centers.
- □ Data centers are typically owned and operated by a third-party provider.

Consumers do not need to know the underlying technologies

- □ In a cloud, software becomes a service.
- □ Cloud demands a high degree of trust of massive amounts of data retrieved from large data centers.
- □ The software infrastructure of a cloud platform must handle all resource management and maintenance automatically.
- □ Software must detect the status of each node server joining and leaving.
- □ Cloud computing providers such as Google and Microsoft, have built a large number of data centers.
- □ Each data center may have thousands of servers.
- □ The location of the data center is chosen to reduce power and cooling costs.

Layered Cloud Architectural Development


The Internet
Public clouds (over Internet)
Hybrid clouds (over Internet/Internets)
Private clouds (over Internets)
Provisioning of both physical and virtualized cloud resources
Application layer (SaaS)
Platform layer (PaaS)
Infrastructure layer (IaaS, HaaS, DaaS, etc.)

- □ The architecture of a cloud is developed at three layers
  - □ Infrastructure
  - □ Platform
  - □ Application

□ Implemented with virtualization and standardization of hardware and software resources provisioned in the cloud.

The services to public, private and hybrid clouds are conveyed to users through networking support

Infrastructure Layer

□ Foundation for building the platform layer.

□ Built with virtualized compute, storage, and network resources.

□ Provide the flexibility demanded by users.

□ Virtualization realizes automated provisioning of resources and optimizes the infrastructure management process.

Platform Layer

□ Foundation for implementing the application layer for SaaS applications.

□ Used for general-purpose and repeated usage of the collection of software resources.

□ Provides users with an environment to develop their applications, to test operation flows, and to monitor execution results and performance.

The platform should be able to assure users that they have scalability, dependability, and security protection

Application Layer

□ Collection of all needed software modules for SaaS applications.

□ Service applications in this layer include daily office management work, such as information retrieval, document processing, and authentication services.

□ The application layer is also heavily used by enterprises in business marketing and sales, consumer relationship management (CRM) and financial transactions.

□ Not all cloud services are restricted to a single layer.

□ Many applications may apply resources at mixed layers.

□ Three layers are built from the bottom up with a dependence relationship.

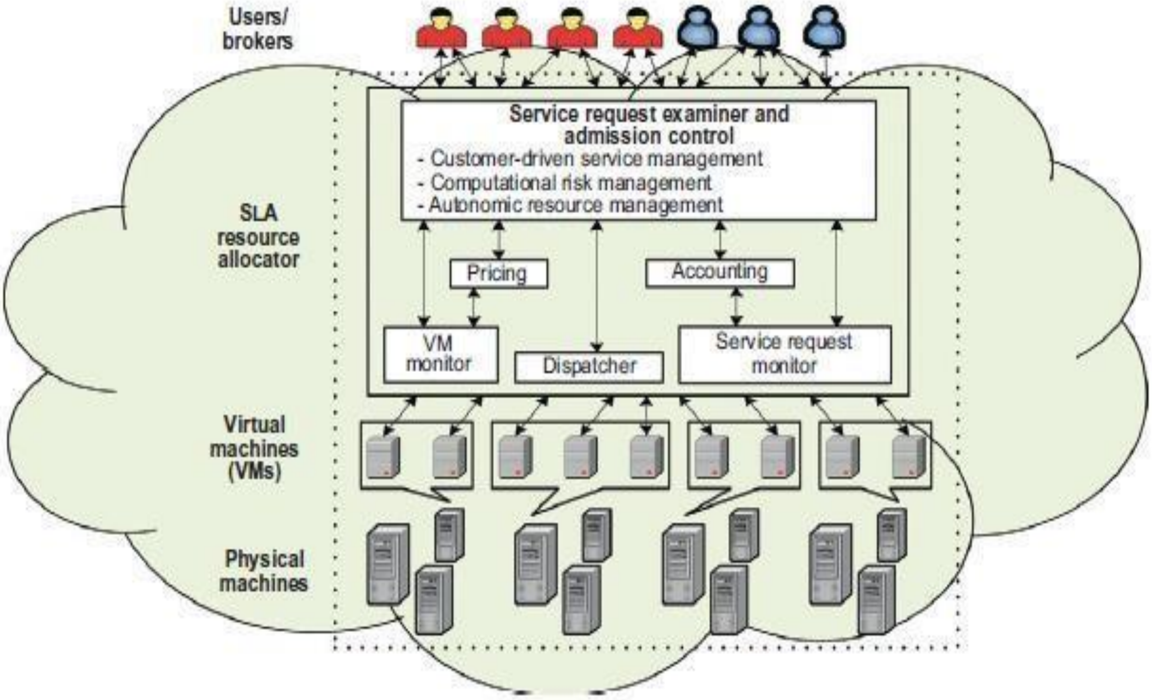
Market-Oriented Cloud Architecture

□ High-level architecture for supporting market-oriented resource allocation in a cloud computing environment.

□ Users or brokers acting on user’s behalf submit service requests to the data center.

□ When a service request is first submitted, the service request examiner interprets the submitted request for QoS requirements.

Accept or Reject the request.



□ **VM Monitor**: Latest status information regarding resource availability.

□ **Service Request Monitor**: Latest status information workload processing

□ **Pricing mechanism:**Decides how service requests are charged.

□ **Accounting mechanism:**Maintains the actual usage of resources by requests to compute the final cost.

□ VM Monitor mechanism keeps track of the availability of VMs and their resource entitlements.

□ Dispatcher starts the execution of accepted service requests on allocated VMs.

Service Request Monitor mechanism keeps track of the execution progress of service requests.

Multiple VMs can be started and stopped on demand

<u>Quality of Service Factors</u>

QoS parameters

□ Time

□ Cost

□ Reliability

□ Trust/security

QoS requirements cannot be static and may change over time.

3.1.1 CLOUD REFERENCE ARCHITECTURE

Definitions

- □ A model of computation and data storage based on “pay as you go” access to “unlimited” remote data center capabilities.
- □ A cloud infrastructure provides a framework to manage scalable, reliable, on-demand access to applications.
- □ Cloud services provide the “invisible” backend to many of our mobile applications.

High level of elasticity in consumption.

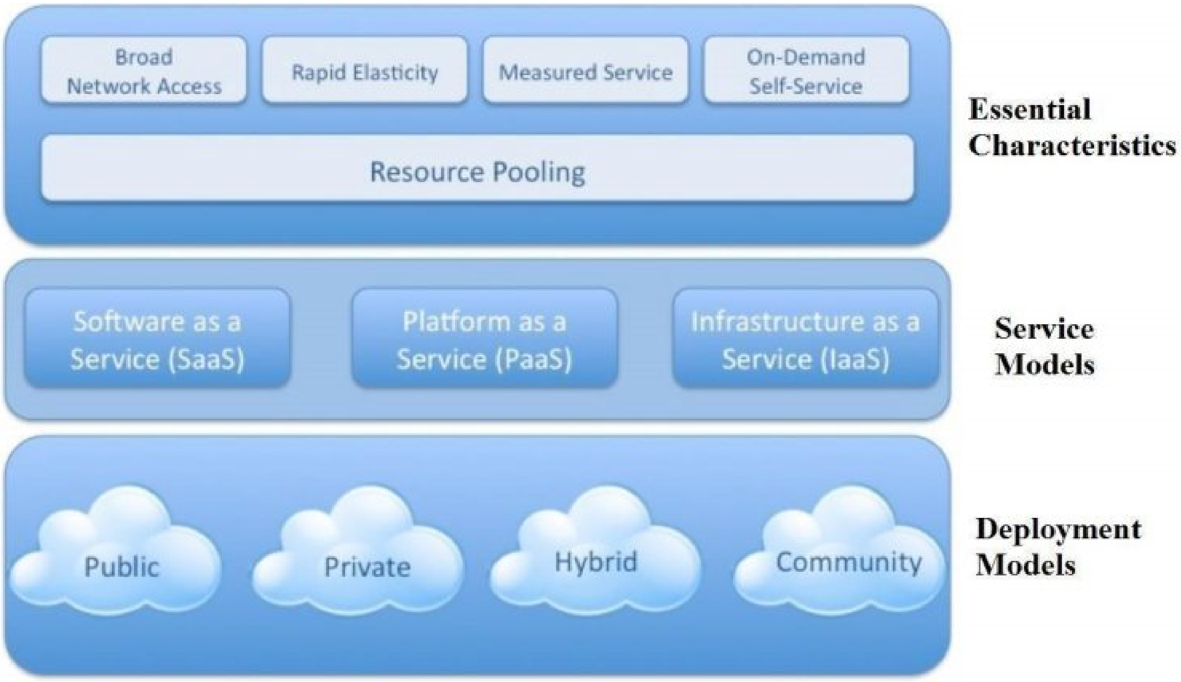
NIST Cloud Definition:

The National Institute of Standards and Technology (NIST) defines cloud computing as a

> **"pay-per-use model for enabling available, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."**

Architecture

- □ Architecture consists of 3 tiers
  - ◦ Cloud Deployment Model
  - ◦ Cloud Service Model
  - ◦ Essential Characteristics of Cloud Computing .



Essential Characteristics 1

□ On-demand self-service.

- A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

Essential Characteristics 2

□ Broad network access.

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloudbased software services.

Essential Characteristics 3

□ Resource pooling.

- The provider's computing resources are pooled to serve multiple consumers using a **multi-tenant model**, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Essential Characteristics 4

□ **Rapid elasticity.**

- Capabilities can be rapidly and elastically provisioned - in some cases automatically - to quickly scale out; and rapidly released to quickly scale in.
- To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Essential Characteristics 5

□ **Measured service.**

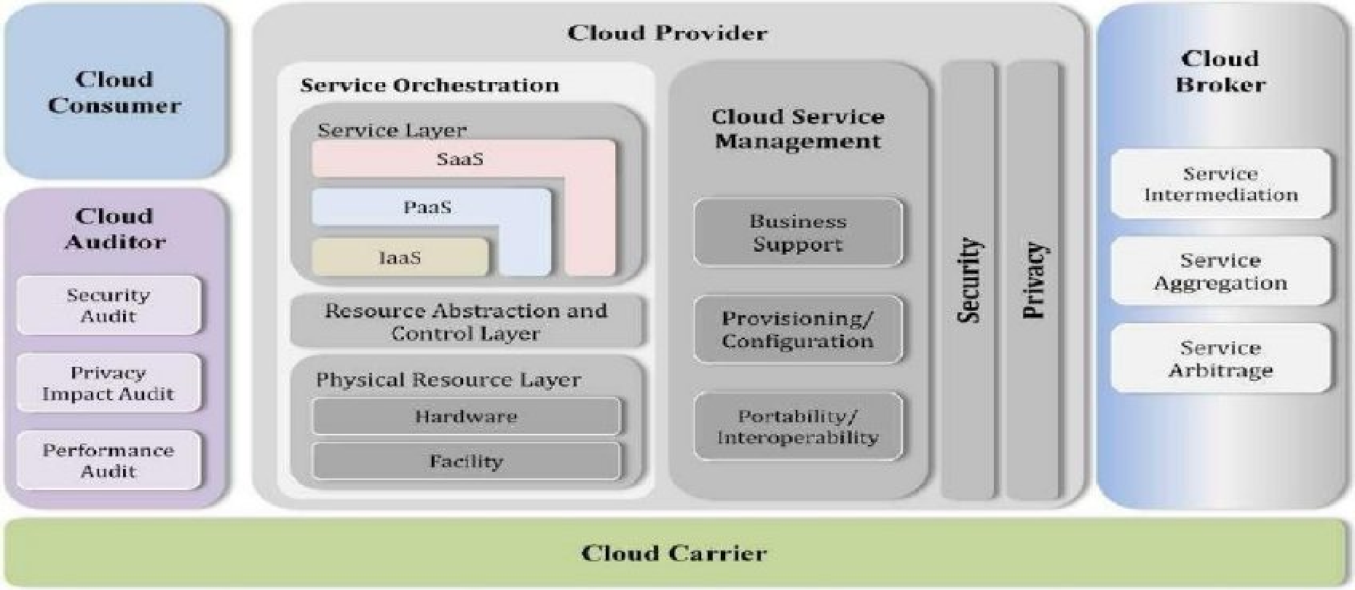
- Cloud systems automatically control and optimize resource usage byleveraging a metering capability at some level of abstraction appropriate to thetype of service.

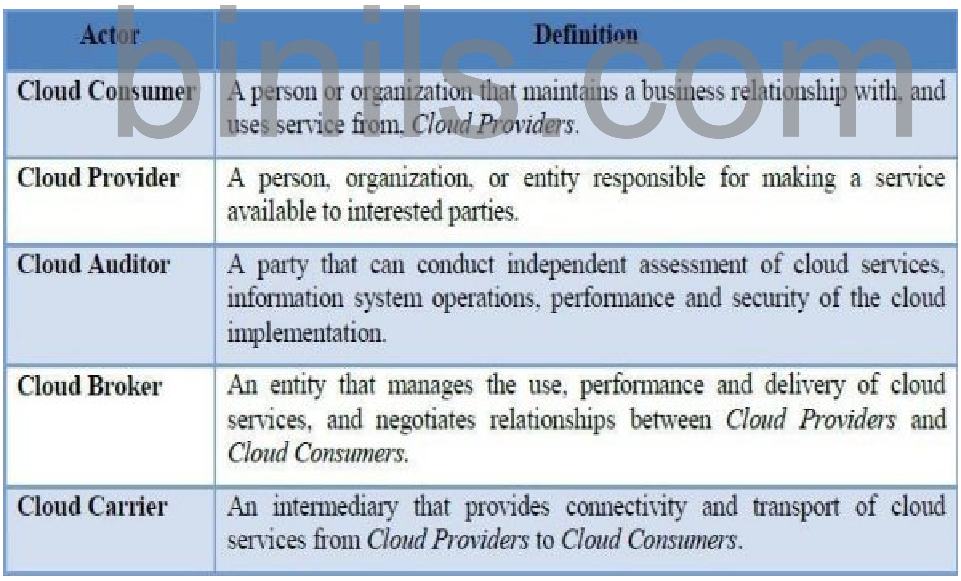
Resource usage can be monitored, controlled, and reported - providing transparency for both the provider and consumer of the service.

NIST (National Institute of Standards and Technology Background)

The goal is to accelerate the federal government's adoption of secure and effective cloud computing to reduce costs and improve services.

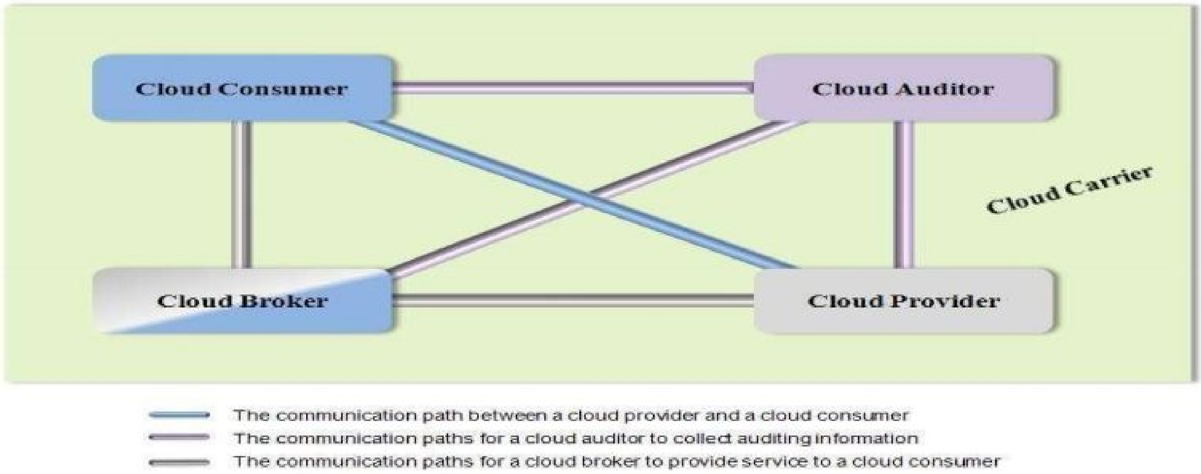
Cloud Computing Reference Architecture:





Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Interactions between the Actors in Cloud Computing


Cloud Consumer
Cloud Auditor
Cloud Carrier
Cloud Broker
Cloud Provider
The communication path between a cloud provider and a cloud consumer
The communication paths for a cloud auditor to collect auditing information
The communication paths for a cloud broker to provide service to a cloud consumer

Example Usage Scenario 1:

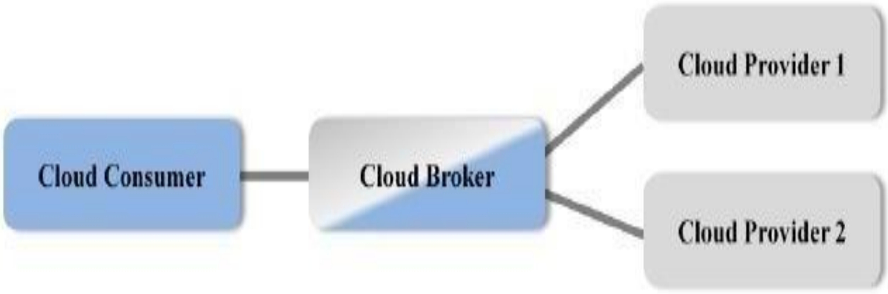
□ A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly.

□ The cloud broker may create a new service by combining multiple services or by enhancing an existing service.

Usage Scenario- Cloud Brokers

□ In this example, the actual cloud providers are invisible to the cloud consumer.

□ The cloud consumer interacts directly with the cloud broker.



Example Usage Scenario 2

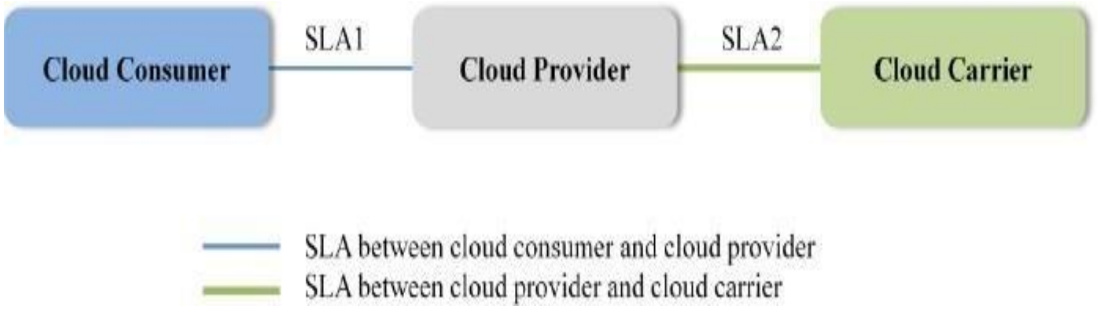
□ Cloud carriers provide the connectivity and transport of cloud services from cloud providers to cloud consumers.

□ A cloud provider participates in and arranges for two unique service level agreements (SLAs), one with a cloud carrier (e.g. SLA2) and one with a cloud consumer (e.g. SLA1).

Usage Scenario for Cloud Carriers

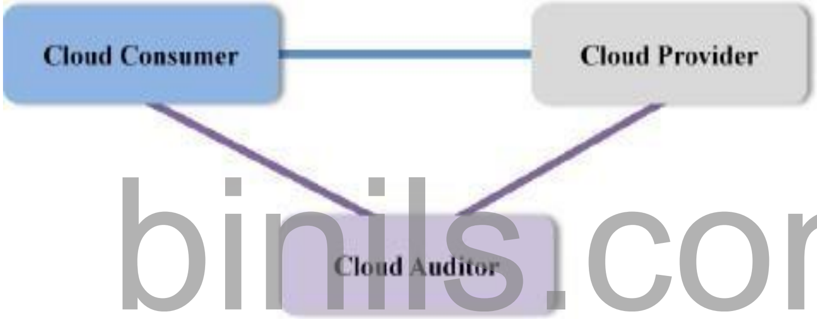
➢ A cloud provider arranges service level agreements (SLAs) with a cloud carrier.

➢ Request dedicated and encrypted connections to ensure the cloud services.


Cloud Consumer
SLA1
Cloud Provider
SLA2
Cloud Carrier
SLA between cloud consumer and cloud provider
SLA between cloud provider and cloud carrier

Example Usage Scenario 3

- For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation.
- The audit may involve interactions with both the Cloud Consumer and the Cloud Provider.



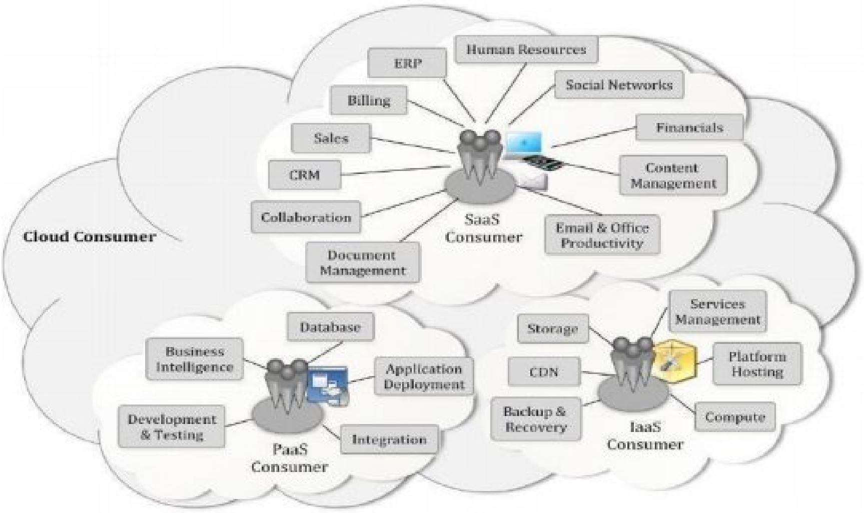
Cloud Consumer

- □ The cloud consumer is the principal stakeholder for the cloud computing service.
- □ A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider.

The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.

Example Services Available to a Cloud Consumer

□ The consumers of SaaS can be organizations that provide their members with access to software applications, end users or software application administrators.



□ SaaS consumers can be billed based on the number of end users, the time of use, the network bandwidth consumed, the amount of data stored or duration of stored data.Cloud consumers of PaaScan employ the tools and execution resources provided by cloud providers to develop, test, deploy and manage the applications.

□ PaaS consumers can be application developers or application testers who run and test applications in cloud-based environments,.

□ PaaS consumers can be billed according to, processing, database storage and network resources consumed.

□ Consumers of IaaS have access to virtual computers, network-accessible storage & network infrastructure components.

□ The consumers of IaaS can be system developers, system administrators and IT managers.

□ IaaS consumers are billed according to the amount or duration of the resources consumed, such as CPU hours used by virtual computers, volume and duration of data stored.

Cloud Provider

□ A cloud provider is a person, an organization;

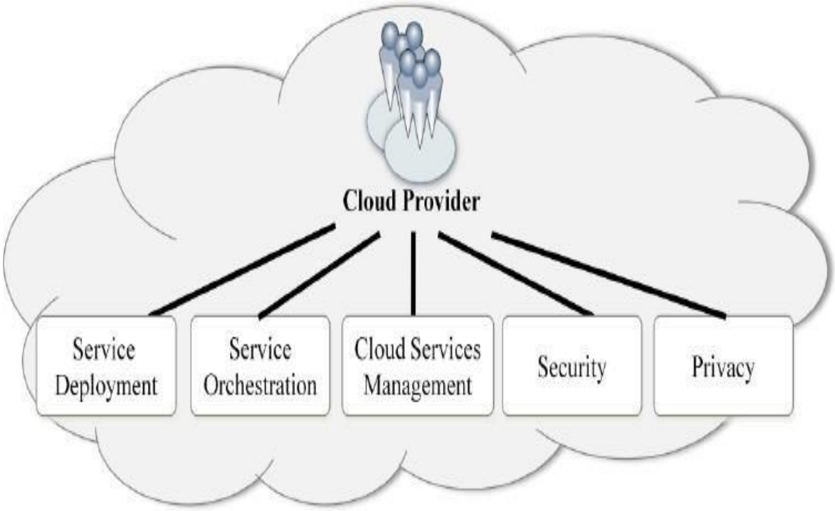
□ It is the entity responsible for making a service available to interested parties.

□ A Cloud Provider acquires and manages the computing infrastructure required for providing the services.

□ Runs the cloud software that provides the services.

Makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

Cloud Provider - Major Activities



Cloud Auditor

- □ A cloud auditor is a party that can perform an independent examination of cloud service controls.
- □ Audits are performed to verify conformance to standards through review of objective evidence.
- □ A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

Cloud Broker

- □ Integration of cloud services can be too complex for cloud consumers to manage.
- □ A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly.
- □ A cloud broker is an entity that manages the use, performance and delivery of cloud services. Negotiates relationships between cloud providers and cloud consumers.

Services of cloud broker

Service Intermediation:

- □ A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers.

Service Aggregation:

- □ A cloud broker combines and integrates multiple services into one or more new services.
- □ The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.

Services of cloud broker

Service Arbitrage:

- □ Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed.
- □ Service arbitrage means a broker has the flexibility to choose services from multiple agencies.

Eg: The cloud broker can use a credit-scoring service to measure and select an agency with the best score.

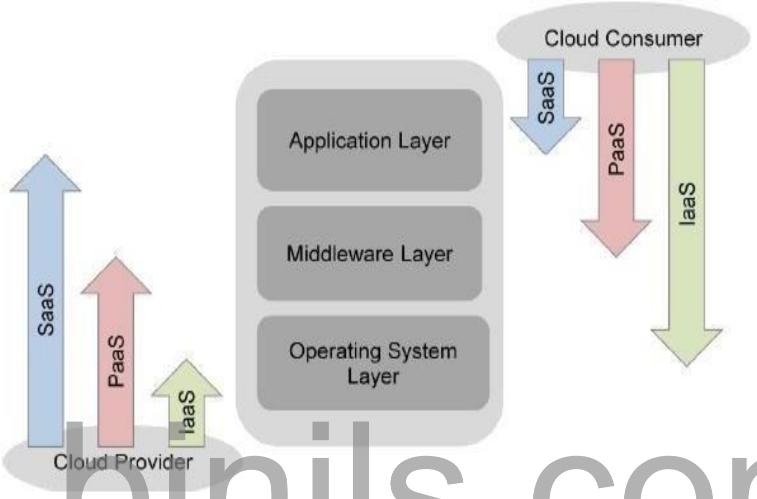
Cloud Carrier

- □ A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

- ☐ Cloud carriers provide access to consumers through network.
- ☐ The distribution of cloud services is normally provided by network and telecommunication carriers or a *transport agent*
- ☐ A transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives and other access devices.

Scope of Control between Provider and Consumer

The Cloud Provider and Cloud Consumer share the control of resources in a cloud system



- ☐ The application layer includes software applications targeted at end users or programs.

The applications are used by SaaS consumers, or installed/managed/maintained by PaaS consumers, IaaS consumers and SaaS providers.

- ☐ The middleware layer provides software building blocks (e.g., libraries, database, and Java virtual machine) for developing application software in the cloud.
- ☐ Used by PaaS consumers, installed/ managed/ maintained by IaaS consumers or PaaS providers, and hidden from SaaS consumers.
- ☐ The OS layer includes operating system and drivers, and is hidden from SaaS consumers and PaaS consumers.
- ☐ An IaaS cloud allows one or multiple guest OS to run virtualized on a single physical host.

The IaaS consumers should assume full responsibility for the guest OS, while the IaaS provider controls the host OS.

Cloud Deployment Model

- □ Public Cloud
- □ Private Cloud
- □ Hybrid Cloud
- □ Community Cloud

3.3.1 Public cloud

- □ A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network.
- □ A public cloud is meant to serve a multitude(huge number) of users, not a single customer.
- □ A fundamental characteristic of public clouds is multitenancy.
- □ Multitenancy allows multiple users to work in a software environment at the same time, each with their own resources.
- □ Built over the Internet (i.e., service provider offers resources, applications storage to the customers over the internet) and can be accessed by any user.
- □ Owned by service providers and are accessible through a subscription.
- □ Best Option for small enterprises, which are able to start their businesses without large up-front(initial) investment.
- □ By renting the services, customers were able to dynamically upsize or downsize their IT according to the demands of their business.
- □ Services are offered on a price-per-use basis.
- □ Promotes standardization, preserve capital investment
- □ Public clouds have geographically dispersed datacenters to share the load of users and better serve them according to their locations
- □ Provider is in control of the infrastructure

Examples:

o Amazon EC2 is a public cloud that provides Infrastructure as a Service

o Google AppEngine is a public cloud that provides Platform as a Service

o SalesForce.com is a public cloud that provides software as a service.

Advantage

- □ **Offers unlimited scalability** – on demand resources are available to meet your business needs.
- □ **Lower costs**—no need to purchase hardware or software and you pay only for the service you use.

- □ **No maintenance -** Service provider provides the maintenance.
- □ **Offers reliability:** Vast number of resources are available so failure of a system will not interrupt service.
- □ Services like SaaS, PaaS, IaaS are easily available on Public Cloud platform as it can be accessed from anywhere through any Internet enabled devices.
- □ **Location independent** – the services can be accessed from any location

Disadvantage

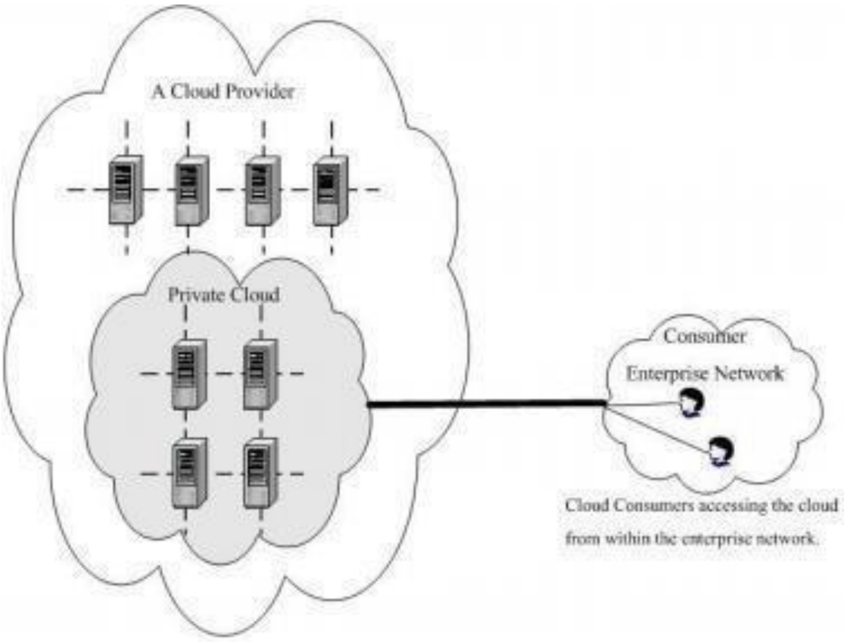
- □ No control over privacy or security
- □ Cannot be used for use of sensitive applications(Government and Military agencies will not consider Public cloud)
- □ Lacks complete flexibility(since dependent on provider)
- □ No stringent (strict) protocols regarding data management

3.3.2 Private Cloud

- □ Cloud services are used by a single organization, which are not exposed to the public
- □ Services are always maintained on a private network and the hardware and software are dedicated only to single organization
- □ Private cloud is physically located at
  - Organization’s premises [On-site private clouds] **(or)**
  - Outsourced(Given) to a third party[Outsource private Clouds]
- □ It may be managed either by
- □ Cloud Consumer organization (or)
  - By a third party
- □ Private clouds are used by
  - government agencies
  - financial institutions
  - Mid size to large-size organisations.
- □ On-site private clouds

Out-sourced Private Cloud

- □ Supposed to deliver more efficient and convenient cloud


A Cloud Provider
Private Cloud
Consumer
Enterprise Network
Cloud Consumers accessing the cloud
from within the enterprise network.

- □ Offers higher efficiency, resiliency(to recover quickly), security, and privacy
- □ **Customer information protection**: In-house security is easier to maintain and rely on.
    - Follows its own(private organization) standard procedures and operations(where as in public cloud standard procedures and operations of service providers are followed)

Advantage

- □ Offers greater Security and Privacy
- □ Organization has control over resources
- □ Highly reliable
- □ Saves money by virtualizing the resources

Disadvantage

- □ Expensive when compared to public cloud
- □ Requires IT Expertise to maintain resources.

3.3.3 Hybrid Cloud

- □ Built with both public and private clouds

- □ It is a heterogeneous cloud resulting from a private and public clouds.
- □ Private cloud are used for
  - sensitive applications are kept inside the organization's network
  - business-critical operations like financial reporting
- □ Public Cloud are used when
  - Other services are kept outside the organization's network
  - high-volume of data
  - Lower-security needs such as web-based email(gmail,yahoomail etc)
- □ The resources or services are temporarily leased for the time required and then released. This practice is also known as **cloud bursting.**

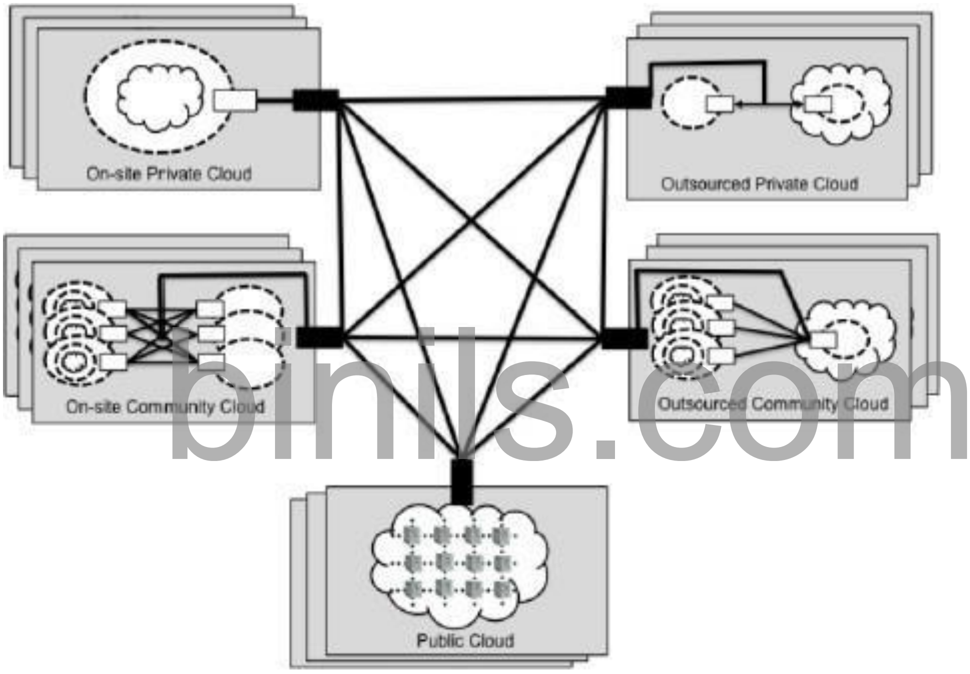


Fig:Hybrid Cloud

Advantage

- □ It is scalable
- □ Offers better security
- □ Flexible-Additional resources are availed in public cloud when needed
- □ Cost-effectiveness—we have to pay for extra resources only when needed.
- □ Control - Organisation can maintain a private infrastructure for sensitive application

Disadvantage

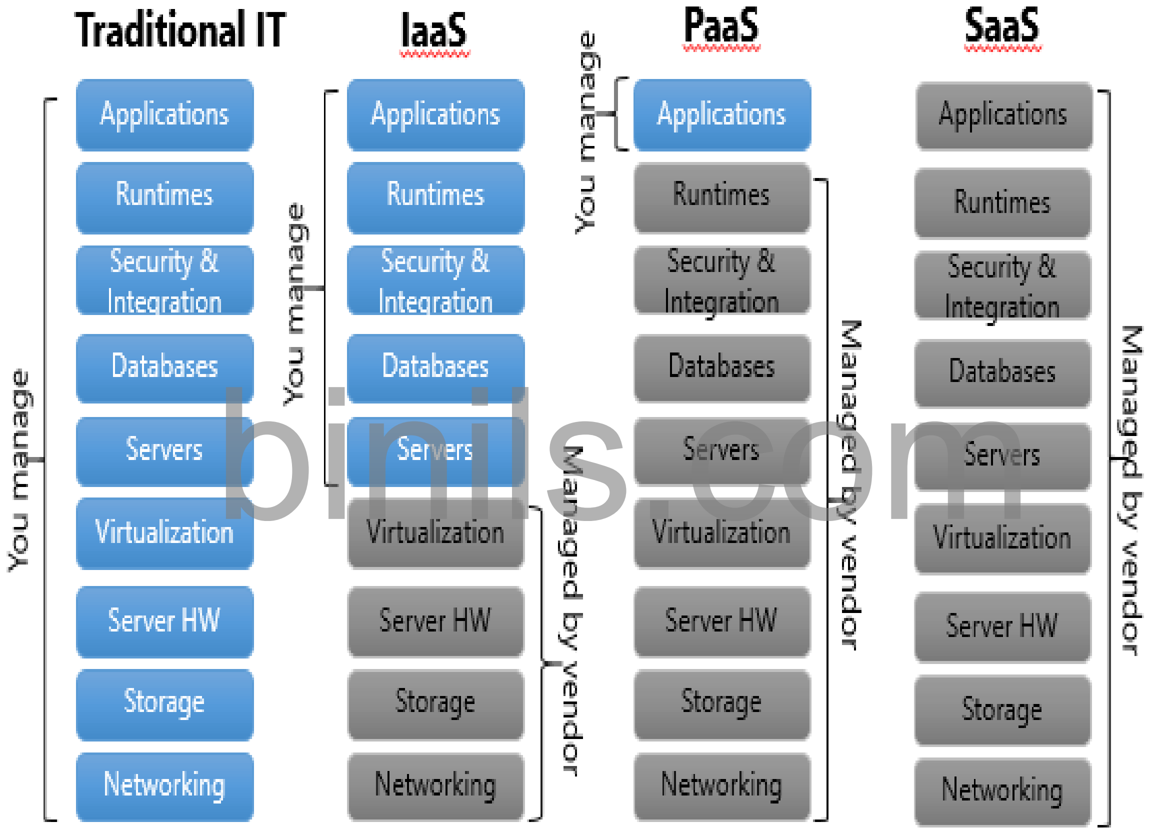
- □ Infrastructure Dependency

- Possibility of security breach(violate) through public cloud

Difference	Public	Private	Hybrid
Tenancy	**Multi-tenancy:** the data of multiple organizations in stored in a shared environment.	**Single tenancy:** Single organizations data is stored in the cloud.	Data stored in the public cloud is multi-tenant. Data stored in private cloud is Single Tenancy.
Exposed to the Public	Yes: anyone can use the public cloud services.	No: Only the organization itself can use the private cloud services.	Services on private cloud can be accessed only by the organization's users Services on public cloud can be Accessed by anyone.
Data Center Location	Anywhere on the Internet	Inside the organization's network.	Private Cloud-Present in organization's network. Public Cloud - anywhere on the Internet.
Cloud Service Management	Cloud service provider manages the services.	Organization has their own administrators managing services	Organization manages the private cloud. Cloud Service Provider(CSP) manages the public cloud.
Hardware Components	CSP provides all the hardware.	Organization provides hardware.	Private Cloud – organization provides resources. Public Cloud – Cloud service Provider provides.
Expenses	Less Cost	Expensive when compared to public cloud	Cost required for setting up private cloud.

Cloud Service Models

- **S**oftware as a Service (**S**aaS)
- **P**latform as a Service (**P**aaS)
- □ **I**nfrastructure as a Service (**I**aaS)
- □ SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a Web-based service. Usually billed based on usage
  - ◦ Usually multi tenant environment



- ◦ Highly scalable architecture
- ▸ Customers do not invest on software application programs.
- ▸ The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- □ The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).
- □ The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, data or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
- □ On the customer side, there is no upfront investment in servers or software licensing.
- □ It is a "one-to-many" software delivery model, whereby an application is shared across multiple users
- □ Characteristic of Application Service Provider(ASP)

o Product sold to customer is application access.

o Application is centrally managed by Service Provider.

o Service delivered is one-to-many customers

o Services are delivered on the contract

E.g. Gmail and docs, Microsoft SharePoint, and the CRM software(Customer Relationship management)

- □ **SaaS providers**
- □ Google's Gmail, Docs, Talk etc
- □ Microsoft's Hotmail, Sharepoint
- □ SalesForce,
- □ Yahoo
- □ Facebook

<u>3.4.2 Infrastructure as a Service (IaaS) (Hardware offerings on the cloud)</u>

IaaS is the delivery of technology infrastructure (mostly hardware) as an on demand, scalable service .

- ◦ Usually billed based on usage
- ◦ Usually multi tenant virtualized environment
- ◦ Can be coupled with Managed Services for OS and application support
- ◦ User can choose his OS, storage, deployed app, networking components

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources.
- Consumer is able to deploy and run arbitrary software, which may include operating systems and applications.
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications.

☐ IaaS/HaaS solutions bring all the benefits of hardware virtualization: workload partitioning, application isolation, sandboxing, and hardware tuning

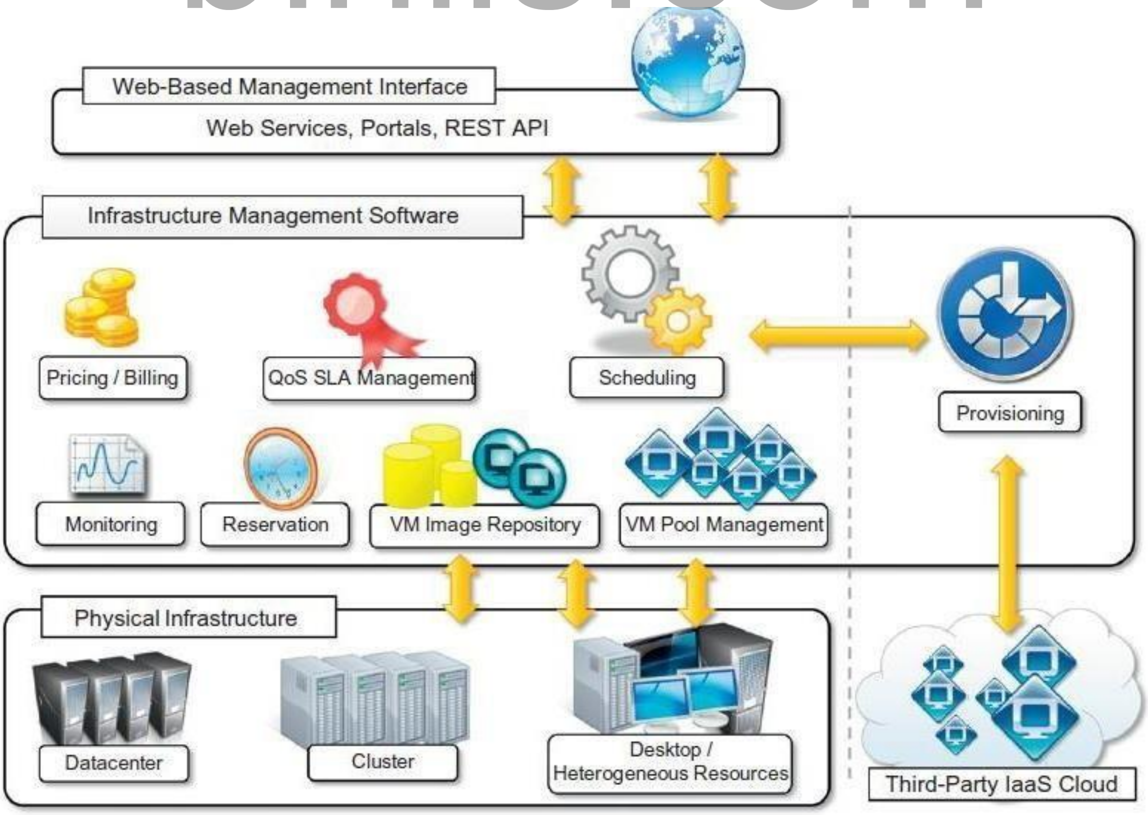
☐ **Sandboxing:** A program is set aside from other programs in a separate environment so that if errors or security issues occur, those issues will not spread to other areas on the computer.

☐ **Hardware tuning:** To improve the performance of system

☐ The user works on multiple VMs running guest OSes

☐ the service is performed by rented cloud infrastructure

☐ The user does not manage or control the cloud infrastructure, but can specify when to request and release the needed resources.



IaaS providers

- □ Amazon Elastic Compute Cloud (EC2)
  - ◦ Each instance provides 1-20 processors, upto 16 GB RAM, 1.69TB storage
- □ RackSpace Hosting
  - ◦ Each instance provides 4 core CPU, upto 8 GB RAM, 480 GB storage
- □ Joyent Cloud
  - ◦ Each instance provides 8 CPUs, upto 32 GB RAM, 48 GB storage
- □ Go Grid
  - ◦ Each instance provides 1-6 processors, upto 15 GB RAM, 1.69TB storage

3.4.3 Platform as a Service (PaaS) (Development platform)

- □ PaaS provides all of the facilities required to support the complete life cycle of building, delivering and deploying web applications and services entirely from the Internet.
- □ Typically applications must be developed with a particular platform in mind
  - Multi tenant environments
  - Highly scalable multi tier architecture
- □ The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider.
- □ The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Have control over the deployed applications and possibly application hosting environment configurations.

Customers are provided with execution platform for developing applications.

Execution platform includes operating system, programming language execution environment, database, web server, hardware etc.

This acts as **middleware** on top of which applications are built

The user is freed from managing the cloud infrastructure

- Developers design their applications in the execution environment.
- Developers need not concern about hardware (physical or virtual), operating systems, and other resources.
- PaaS core middleware manages the resources and scaling of applications on demand.
- PaaS offers

o Execution environment and hardware resources (infrastructure) **(or)**

o software is installed on the user premises

- **PaaS:** Service Provider provides Execution environment and hardware resources (infrastructure)

Characteristics of PaaS

- **Runtime framework:** Executes end-user code according to the policies set by the user and the provider.
- **Abstraction:** PaaS helps to deploy(install) and manage applications on the cloud.

- **Automation:** Automates the process of deploying applications to the infrastructure, additional resources are provided when needed.
- **Cloud services:** helps the developers to simplify the creation and delivery cloud applications.

Category	Description	Product Type	Vendors and Products
PaaS-I	Execution platform is provided along with hardware resources (infrastructure)	Middleware + Infrastructure	Force.com, Longjump
PaaS -II	Execution platform is provided with additional components	Middleware + Infrastructure, Middleware	Google App Engine
PaaS- III	Runtime environment for developing any kind of application development	Middleware + Infrastructure, Middleware	Microsoft Azure

Architectural Design Challenges

Challenge 1 : Service Availability and Data Lock-in Problem

Service Availability

- Service Availability in Cloud might be affected because of
- Single Point Failure
- Distributed Denial of Service
- Single Point Failure
  - o Depending on single service provider might result in failure.
  - o In case of single service providers, even if company has multiple data centres located in different geographic regions, it may have **common software infrastructure and accounting systems**.

Solution:

o Multiple cloud providers may provide more protection from failures and they provide High Availability (HA)

o Multiple cloud Providers will rescue the loss of all data.

Distributed Denial of service (DDoS) attacks.

o Cyber criminals, attack target websites and online services and makes services unavailable to users.

o DDoS tries to overwhelm (disturb) the services unavailable to user by having more traffic than the server or network can accommodate.

Solution:

o Some SaaS providers provide the opportunity to defend against DDoS attacks by using quick scale-ups.

Customers cannot easily extract their data and programs from one site to run on another.

Solution:

o Have standardization among service providers so that customers can deploy (install) services and data across multiple cloud providers.

Data Lock-in

- It is a situation in which a customer using service of a provider cannot be moved to another service provider because technologies used by a provider will be incompatible with other providers?
- This makes a customer dependent on a vendor for services and makes customer unable to

use service of another vendor.

Solution:

o Have standardization (in technologies) among service providers so that customers can easily move from a service provider to another.

Challenge 2: Data Privacy and Security Concerns

Cloud services are prone to attacks because they are accessed through internet.

Security is given by

o Storing the encrypted data in to cloud.

o Firewalls, filters.

Cloud environment attacks include

o Guest hopping

o Hijacking

o VM rootkits.

Guest Hopping: Virtual machine hyper jumping (VM jumping) is an attack method that exploits (make use of) hypervisor's weakness that allows a virtual machine (VM) to be accessed from another.

Hijacking: Hijacking is a type of network security attack in which the attacker takes control of a communication **VM Rootkit:** is a collection of malicious (harmful) computer software, designed to enableaccess to a computer that is not otherwise allowed.

A **man-in-the-middle (MITM)** attack is a form of eavesdroppping(Spy) where communication between two users is monitored and modified by an unauthorized party.

o Man-in-the-middle attack may take place **during VM migrations** [virtual machine (VM) migration - VM is moved from one physical host to another host].

Passive attacks steal sensitive data or passwords.

Active attacks may manipulate (control) kernel data structures which will cause major damage to cloud servers.

Challenge 3: Unpredictable Performance and Bottlenecks

Multiple VMs can share CPUs and main memory in cloud computing, but I/O sharing is problematic.

Internet applications continue to become more data-intensive (handles huge amount of data).

Handling huge amount of data (data intensive) is a bottleneck in cloud environment.

Weak Servers that does not provide data transfers properly must be removed from cloud environment

Challenge 4: Distributed Storage and Widespread Software Bugs

- The database is always growing in cloud applications.
- There is a need to create a storage system that meets this growth.
- This demands the design of efficient distributed SANs (Storage Area Network of Storage devices).
- Data centres must meet

o Scalability

o Data durability

o HA(High Availability)

o Data consistence

- Bug refers to errors in software. Debugging
- must be done in data centres.

Challenge 5: Cloud Scalability, Interoperability and Standardization

Cloud Scalability

- Cloud resources are scalable. Cost increases when storage and network bandwidth scaled(increased)

Interoperability

- Open Virtualization Format (OVF) describes an open, secure, portable, efficient, and extensible format for the packaging and distribution of VMs.
- OVF defines a transport mechanism for VM, that can be applied to different virtualization platforms

Standardization

- Cloud standardization, should have ability for virtual machine to run on any virtual platform.

Challenge 6: Software Licensing and Reputation Sharing

- Cloud providers can use both pay-for-use and bulk-use licensing schemes to widen the business coverage.
- Cloud providers must create reputation-guarding services similar to the “trusted e-mail” services
- Cloud providers want legal liability to remain with the customer, and vice versa.

3.6. Cloud Storage

- Storing your data on the storage of a cloud service provider rather than on a local system.
- Data stored on the cloud are accessed through Internet.
- Cloud Service Provider provides Storage as a Service

3.6.1 Storage as a Service

☐ Third-party provider rents space on their storage to cloud users.

☐ Customers move to cloud storage when they lack in budget for having their own storage.

☐ Storage service providers takes the responsibility of taking current backup, replication, and disaster recovery needs.

☐ Small and medium-sized businesses can make use of Cloud Storage

☐ Storage is rented from the provider using a

o cost-per-gigabyte-stored **(or)**

o cost-per-data-transferred

☐ The end user doesn't have to pay for infrastructure (resources), they have to pay only for how much they transfer and save on the provider's storage.

5.2 Providers

☐ Google Docs allows users to upload documents, spreadsheets, and presentations to Google's data servers.

☐ Those files can then be edited using a Google application.

☐ Web email providers like Gmail, Hotmail, and Yahoo! Mail, store email messages on their own servers.

☐ Users can access their email from computers and other devices connected to the Internet.

☐ Flicker and Picasa host millions of digital photographs, Users can create their own online photo albums.

☐ YouTube hosts millions of user-uploaded video files.

☐ Hostmonster and GoDaddy store files and data for many client web sites.

☐ Facebook and MySpace are social networking sites and allow members to post pictures and other content. That content is stored on the company's servers.

☐ MediaMax and Strongspace offer storage space for any kind of digital data.

3.6.2 Data Security

☐ To secure data, most systems use a combination of techniques:

o Encryption

o Authentication

o Authorization

Encryption

o Algorithms are used to encode information. To decode the information keys are required.

Authentication processes

o This requires a user to create a name and password.

Authorization practices

o The client lists the people who are authorized to access information stored on the cloud system.

If information stored on the cloud, the head of the IT department might have complete and free access to everything.

Reliability

☐ Service Providers gives reliability for data through redundancy (maintaining multiple copies of data).

Reputation is important to cloud storage providers. If there is a perception that the provider is unreliable, they won't have many clients.

Advantages

- □ Cloud storage providers balance server loads.
- □ Move data among various datacenters, ensuring that information is stored close and thereby available quickly to where it is used.
- □ It allows to protect the data in case there's a disaster.
- □ Some products are agent-based and the application automatically transfers information to the cloud via FTP

Cautions

- □ Don't commit everything to the cloud, but use it for a few, noncritical purposes.
- □ Large enterprises might have difficulty with vendors like Google or Amazon.
- □ Forced to rewrite solutions for their applications.
- □ Lack of portability.

Theft (Disadvantage)

- □ User data could be stolen or viewed by those who are not authorized to see it.
- □ Whenever user data is let out of their own datacenter, risk trouble occurs from a security point of view.
- □ If user store data on the cloud, make sure user encrypts data and secures data transit with technologies like SSL.

Cloud Storage Providers

Amazon Simple Storage Service (S3)

- □ The best-known cloud storage service is Amazon’s Simple Storage Service (S3), launched in 2006.
- □ Amazon S3 is designed to make computing easier for developers.
- □ Amazon S3 provides an interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the Web.
- □ Amazon S3 is intentionally built with a minimal feature set that includes the following functionality:

  • Write, read, and delete objects containing from 1 byte to 5 gigabytes of data each.

  The number of objects that can be stored is unlimited.

  • Each object is stored and retrieved via a unique developer-assigned key.

  • Objects can be made private or public, and rights can be assigned to specific users.

  • Uses standards-based REST and SOAP interfaces designed to work with any Internet-development toolkit.

Design Requirements

Amazon built S3 to fulfill the following design requirements:

• **Scalable** Amazon S3 can scale in terms of storage, request rate, and users to support an unlimited number of web-scale applications.

- **Reliable** Store data durably, with 99.99 percent availability. Amazon says it does not allow any downtime.

• **Fast** Amazon S3 was designed to be fast enough to support high-performance applications. Server-side latency must be insignificant relative to Internet latency. Any performance bottlenecks can be fixed by simply adding nodes to the system.

• **Inexpensive** Amazon S3 is built from inexpensive commodity hardware components. As a result, frequent node failure is the norm and must not affect the overall system. It must be hardware-agnostic, so that savings can be captured as Amazon continues to drive down infrastructure costs.

• **Simple** Building highly scalable, reliable, fast, and inexpensive storage is difficult. Doing so in a way that makes it easy to use for any application anywhere is more difficult. Amazon S3 must do both.

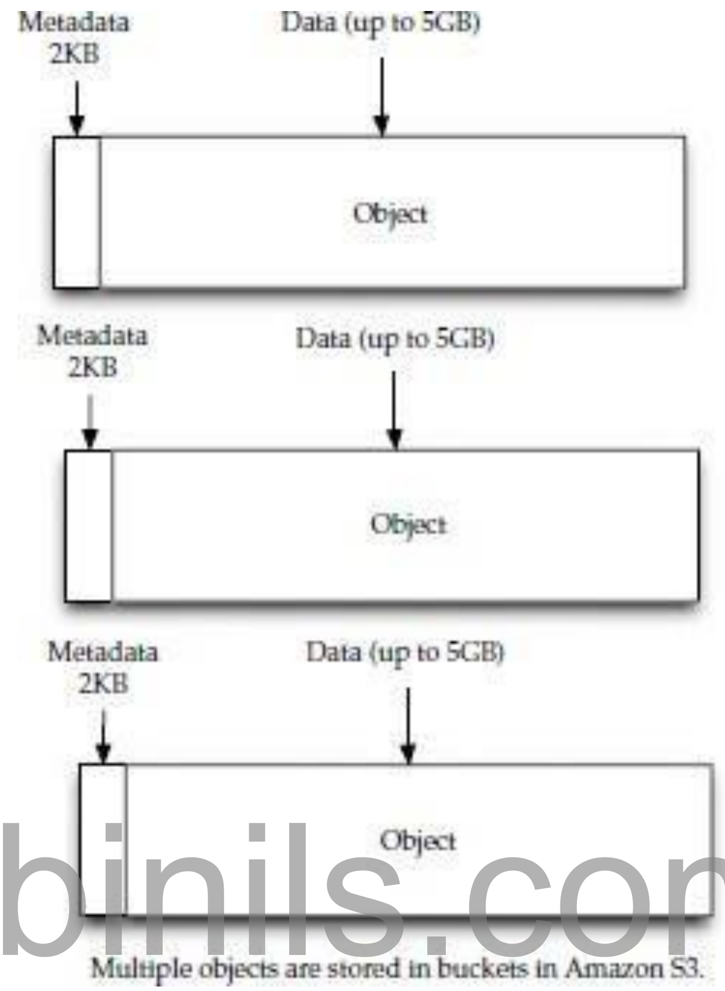
Design Principles

Amazon used the following principles of distributed system design to meet Amazon S3 requirements:

- **Decentralization** It uses fully decentralized techniques to remove scaling bottlenecks and single points of failure.
- **Autonomy** The system is designed such that individual components can make decisions based on local information.
- **Local responsibility** Each individual component is responsible for achieving its consistency; this is never the burden of its peers.
- **Controlled concurrency** Operations are designed such that no or limited concurrency control is required.
- **Failure toleration** The system considers the failure of components to be a normal mode of operation and continues operation with no or minimal interruption.
- **Controlled parallelism** Abstractions used in the system are of such granularity that parallelism can be used to improve performance and robustness of recovery or the introduction of new nodes.
- **Small, well-understood building blocks** Do not try to provide a single service that does everything for everyone, but instead build small components that can be used as building blocks for other services.
- **Symmetry** Nodes in the system are identical in terms of functionality, and require no or minimal node-specific configuration to function.
- **Simplicity** The system should be made as simple as possible, but no simpler.

How S3 Works

Amazon keeps its lips pretty tight about how S3 works, but according to Amazon, S3's design aims to provide scalability, high availability, and low latency at commodity costs. S3 stores arbitrary objects at up to 5GB in size, and each is accompanied by up to 2KB of metadata. Objects are organized by *buckets*. Each bucket is owned by an AWS account and the buckets are identified by a unique, user-assigned key.



Multiple objects are stored in buckets in Amazon S3.

Buckets and objects are created, listed, and retrieved using either a REST-style or SOAP interface.

Objects can also be retrieved using the HTTP GET interface or via BitTorrent. An access control list restricts who can access the data in each bucket. Bucket names and keys are formulated so that they can be accessed using HTTP. Requests are authorized using an access control list associated with each bucket and object, for instance:

http://s3.amazonaws.com/examplebucket/examplekey

http://examplebucket.s3.amazonaws.com/examplekey

The Amazon AWS Authentication tools allow the bucket owner to create an authenticated URL with a set amount of time that the URL will be valid.