2

CHAPTER

CLOUD COMPUTING ARCHITECTURE

CHAPTER OUTLINE

After studying this chapter, students will be able to understand the:

- Cloud Computing Reference Model, Community Cloud
- Cloud Service Models, Identity-As–A-Service (IDAAS)
- Federated Identity Management (FIDM), Network-As-A-Service (NaaS)
- Communication-As-A-Service (CaaS), Monitoring-As-A-Service (MaaS)
- Cloud Interoperability and Standards, Cloud Solutions
- Cloud Service Management, Cloud Offerings
- Testing Under Control, Cloud testing strategy components include
- Virtual Desktop Infrastructure, Cloud Governance
- Market-Based Management of Clouds

CLOUD COMPUTING REFERENCE MODEL

The cloud computing reference model is a general high-level architecture and is meant to aid understanding of the cloud computing needs, uses, features, and standards. An overview of the NIST cloud computing reference architecture is provided, which outlines the primary performer/actor and their cloud computing activities and roles. The NIST cloud computing reference architecture identifies five primary players, as indicated in the figure below. Each performer is an entity that might be a person or an organization that takes part in a transaction or process and completes duties in cloud computing.

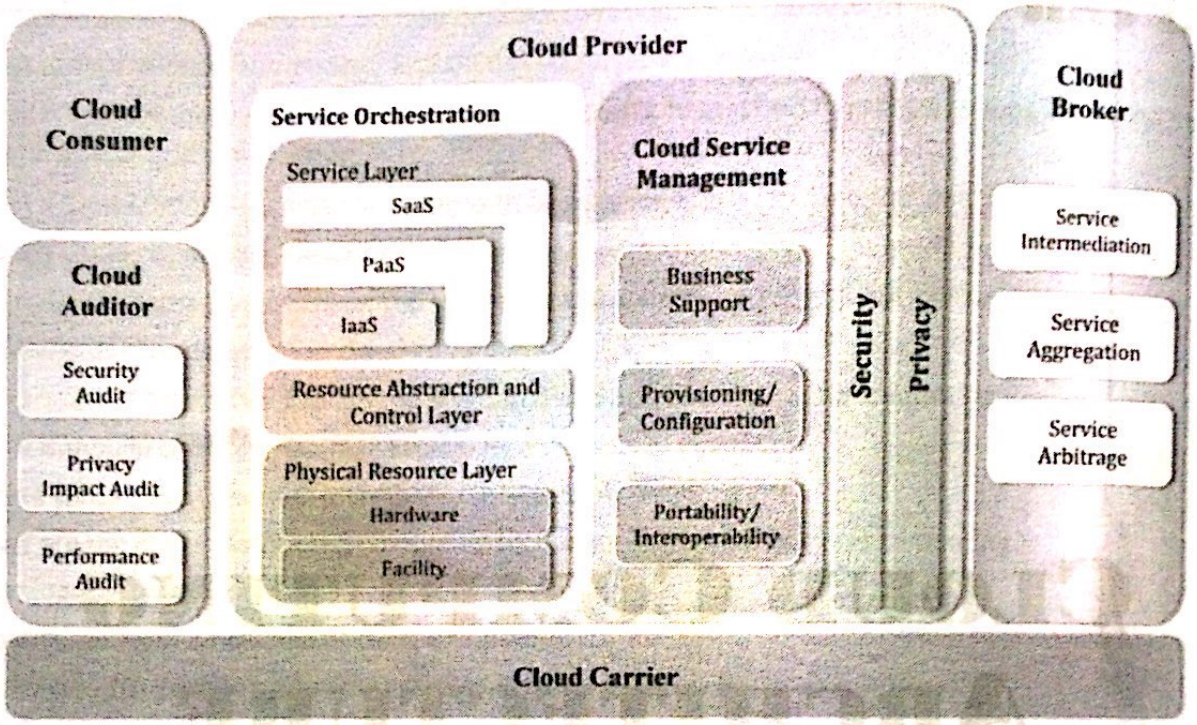


Figure 2.1 Cloud Computing Reference Model

1. **Cloud consumer:** The cloud consumer is the cloud computing service's most significant stakeholder. A cloud consumer is a person or organization who has a commercial connection with a cloud provider and consumes its services. A cloud consumer browses a cloud provider's service catalog, requests the right service, establishes service contracts with the cloud provider, and consumes the service. The cloud consumer may be invoiced for the service provided and must make payment arrangements appropriately.

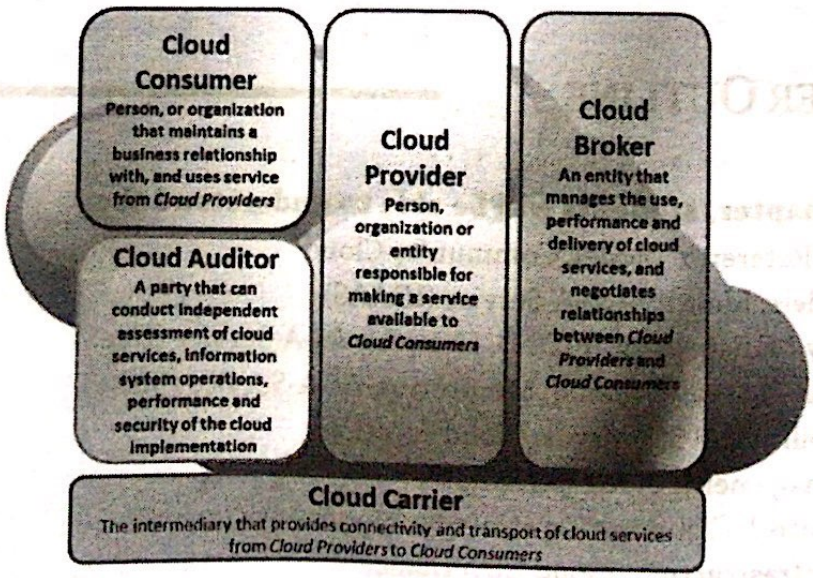


Figure 2.2 Actors of cloud environment

2. **Cloud Provider:** A cloud provider is a person or an organization that is responsible for making a service available to interested parties. A cloud provider purchases and administers the computer equipment necessary to supply the services, operates the cloud software that offers the services, and arranges for the cloud services to be delivered to cloud consumers via network access. In the case of Software as a Service, the cloud provider deploys, configures, maintains, and upgrades the functioning of software applications on cloud infrastructure so that the services are provided to cloud consumers at the required service levels.

3. **Cloud Auditor**: A cloud auditor is a party who can do an impartial analysis of cloud service controls to provide an opinion on them. Audits are carried out to ensure that standards are met by reviewing objective evidence. A cloud auditor can assess a cloud provider's services in terms of security measures, privacy implications, performance, and so on.

4. **Cloud broker:** As cloud computing advances, cloud service integration may become too difficult for cloud users to maintain. Instead of contacting a cloud provider directly, a cloud user might request cloud services using a cloud broker. A cloud broker is a company that handles the usage, performance, and delivery of cloud services and negotiates contracts between cloud providers and cloud users.

Actor	Definition
Cloud Consumer	A person or organization that maintain a business relationship with, and uses service from, cloud providers.
Cloud Provider	A person, organization, or entity responsible for making an available service to interest parties.
Cloud Auditor	A. party that can conduct independent assessment of cloud service, information system operations, performance, and security of the loud implementation.
Cloud Borker	An entity that manages the use, performance, and delivery of cloud services, and negotiates relationship between cloud providers and cloud consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud service from cloud providers to cloud consumers.

5. **Cloud carrier:** A cloud carrier operates as a middleman between cloud users and cloud providers, providing connectivity and transfer of cloud services. Cloud carriers give users access via a network, telecommunication, and other access devices. Cloud users, for example, can access cloud services via network access devices such as PCs, laptops, mobile phones, mobile Internet devices, and so on.

The interaction between the performers is depicted in the figure below. A cloud consumer can request cloud services directly from a cloud provider or through a cloud broker. A cloud auditor does independent audits and may contact others to get information.

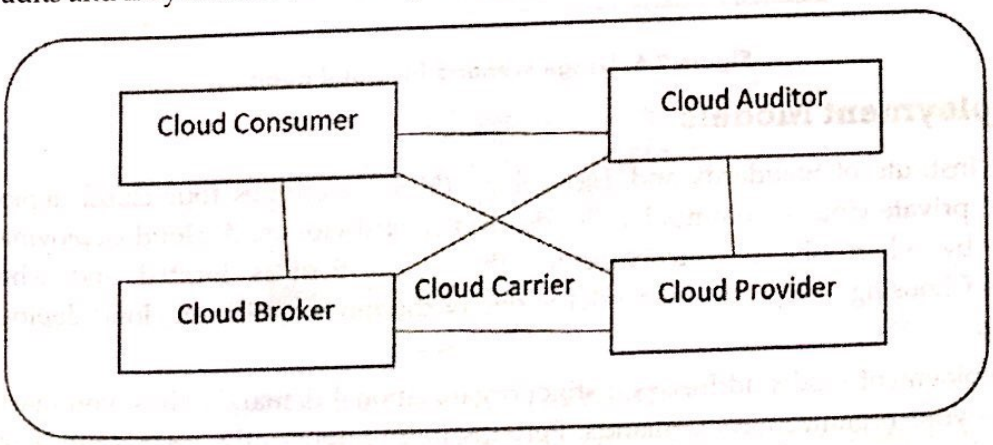


Figure 2.3: Interaction between the Actors in Cloud Computing

Followings are some of the examples of NIST Cloud Computing standard architecture utilization scenario of different performers/actors:

(i) **Usage scenario of cloud brokers:** Instead of contacting a cloud provider directly, a cloud customer might request service using a cloud broker. As demonstrated in Figure, the cloud broker can establish a new service by integrating various services or by upgrading an existing service. The real cloud providers are invisible to the cloud consumer in this scenario, and the cloud consumer communicates directly with the cloud broker.

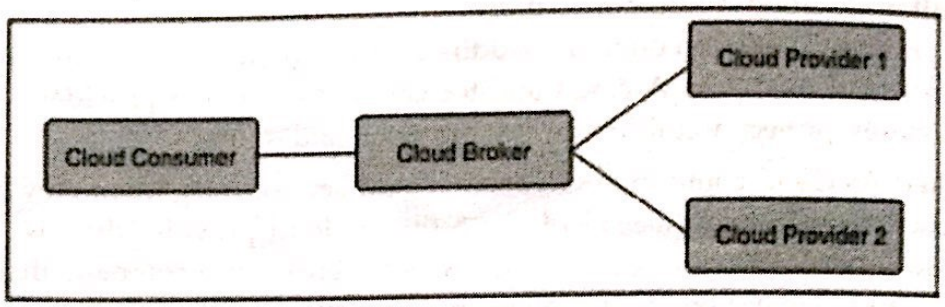


Figure 2.4: Usage scenario of cloud brokers

(ii) **Usage scenario for cloud carriers:** Cloud carriers connect cloud providers and transmit cloud services from providers to customers. A cloud provider engages in and negotiates two distinct service level agreements (SLAs), one with a cloud carrier (e.g., SLA2) and one with a cloud consumer (e.g., SLA1). A cloud provider negotiates service level agreements (SLAs) with a cloud carrier and may seek dedicated and encrypted connections to guarantee that cloud services are utilized consistently following contractual commitments with cloud users. In this situation, the provider may express its capacity, adaptability, and functionality needs in SLA2 to meet the basic needs in SLA1.

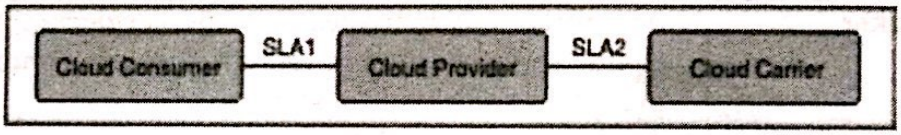


Figure 2.5: Usage scenario for cloud carriers

(iii) **Usage scenario for cloud auditors:** A cloud auditor performs impartial audits of the operation and security of a cloud service deployment. Interactions with both the cloud consumer and the cloud provider may be required during the audit.

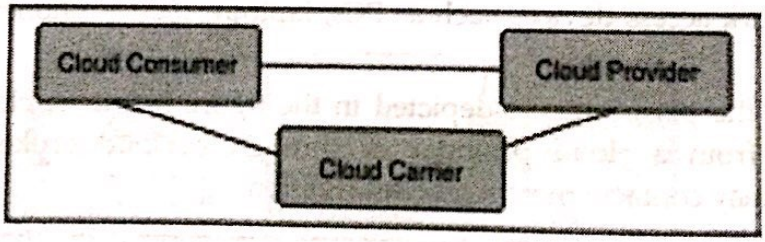


Figure 2.6: Usage scenario for cloud auditors

Cloud Deployment Models

The National Institute of Standards and Technology (NIST) identifies four cloud deployment models: public clouds, private clouds, community clouds, and hybrid clouds. A cloud deployment paradigm is characterized by where the infrastructure for the deployment is located and who controls that infrastructure. Choosing a deployment model is one of the most significant cloud deployment decisions you will make.

Each cloud deployment model addresses distinct organizational demands; thus, you must select a model that addresses your organization's demands. Perhaps more importantly, each cloud deployment option has a particular value proposition and expenses associated with it. As a result, in many circumstances,

your choice of a cloud deployment architecture may simply be a matter of cost. In any event, to make an informed selection, you must be familiar with the peculiarities of each setting.

Cloud deployment models describe how consumers can access cloud services. Following are the four cloud computing deployment models:

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

1. **Public Cloud:** As the name implies, this sort of cloud deployment architecture caters to all customers who wish to subscribe to a computational resource, such as hardware (OS, CPU, memory, storage) or software (application server, database).

   Public clouds are most commonly used for application development and testing, non-mission-critical functions such as file sharing, and e-mail service.Businesses that operate in industries with low privacy concerns choose to use the public cloud deployment strategy. The vast majority of public clouds contain large quantities of accessible space, allowing for simple expansion. For software development and collaborative projects, a public cloud is frequently recommended. Companies can create portable apps so that a project tested in the public cloud may be moved to the private cloud for production.

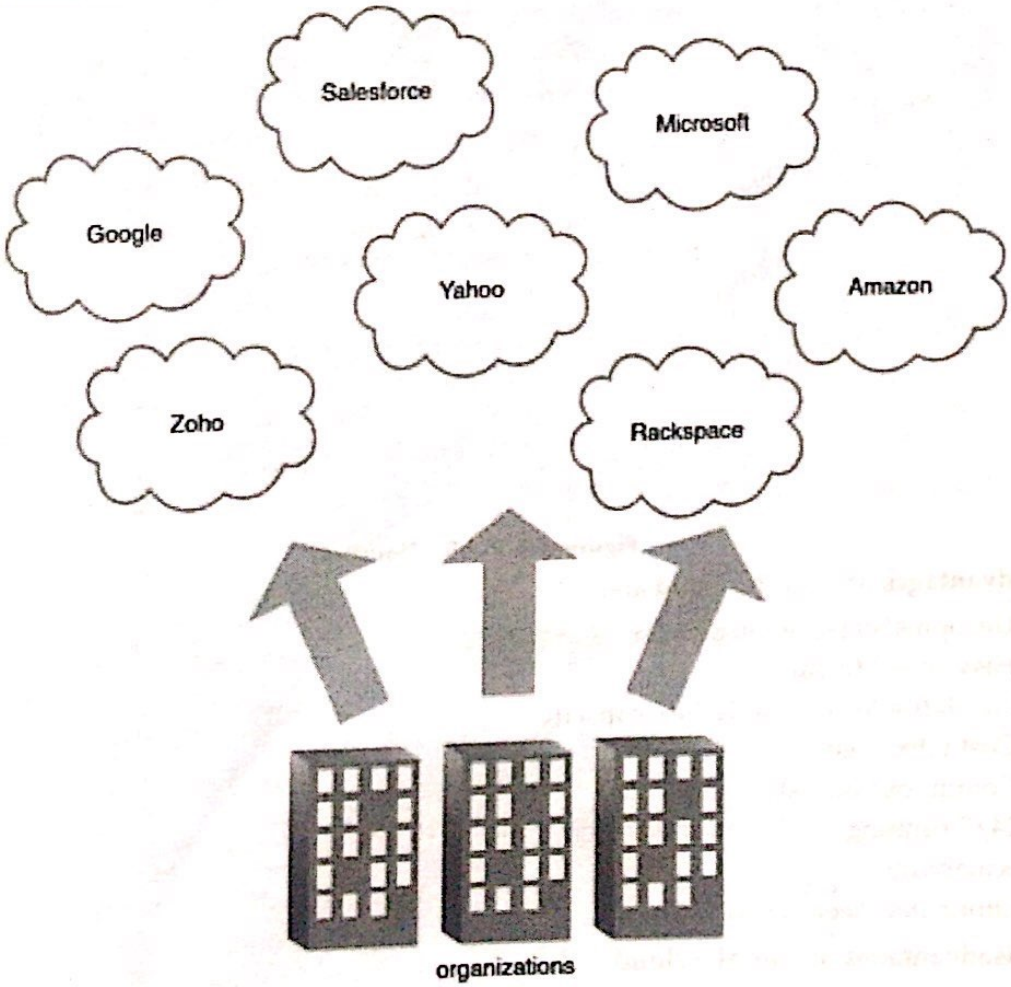


Figure 2.7 Popular Cloud Providers

Popular cloud deployment strategies include Amazon Elastic Compute, Google AppEngine, IBM Blue, Microsoft Azure, Salesforce Heroku, and others.

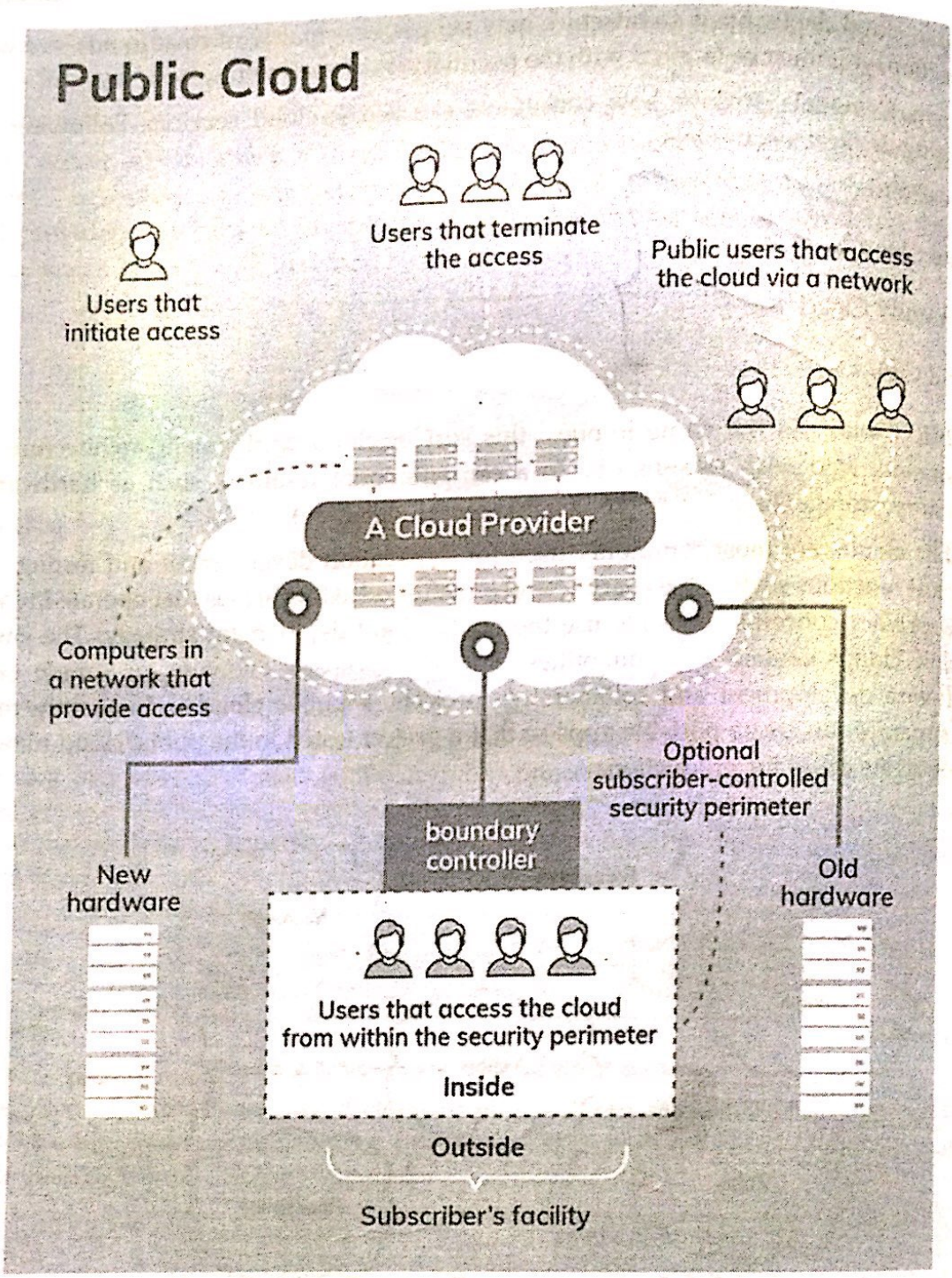


Figure 2.8: Public Cloud

The advantages of a public cloud are:

- Unsophisticated setup and use
- Easy access to data
- Flexibility to add and reduce capacity
- Cost-effectiveness
- Continuous operation time
- 24/7 running
- Scalability
- Eliminated need for software

The disadvantages of a public cloud:

- Data security and privacy
- Compromised reliability
- The lack of an individual approach

2. **Private Cloud:** A private cloud, as the name implies, is primarily infrastructure utilized by a single enterprise.

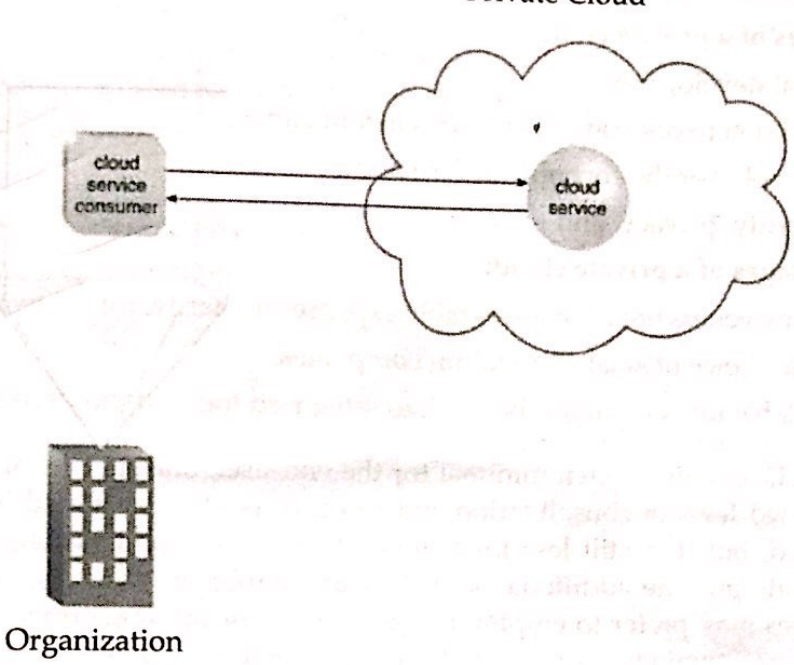


Figure 2.9 Private Cloud

Such infrastructure may be maintained by the organization itself to accommodate diverse user groups, or it may be maintained by a service provider on-site or off-site. Because of the financial investment required to acquire and operate private clouds, they are more expensive than public clouds. Private clouds, on the other hand, are more suited to handle enterprises' security and concerns today.

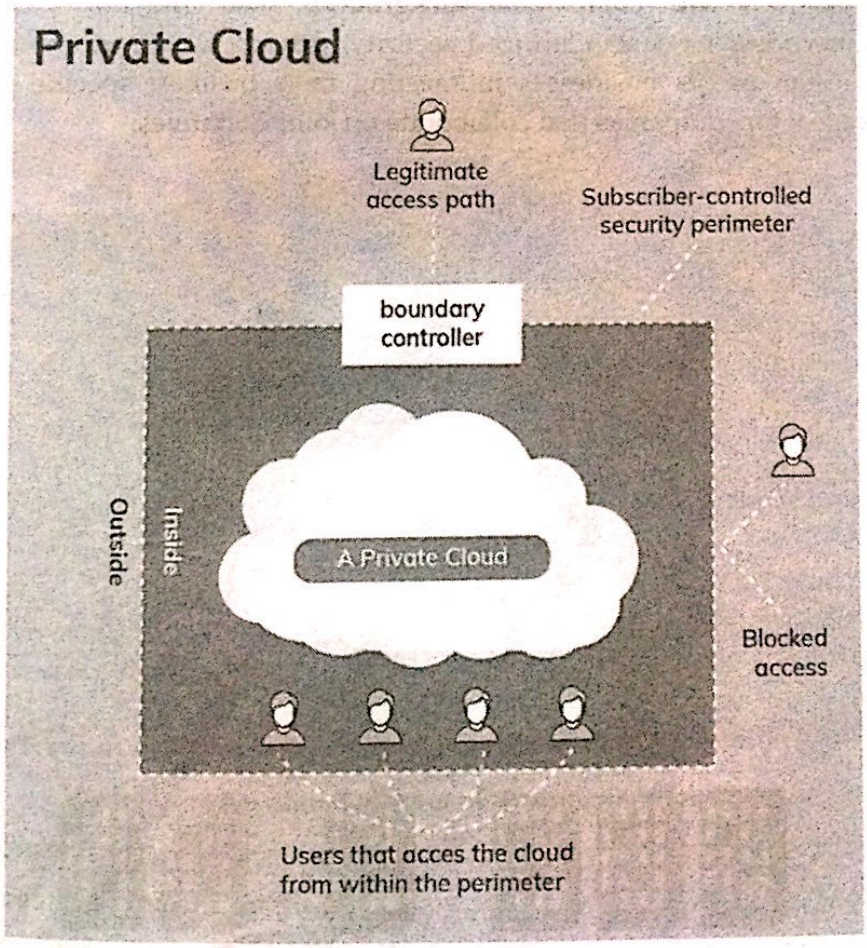


Figure 2.10 Detailed view of private cloud

Private solutions are also built by several service providers, including Amazon, IBM, Cisco, Dell and Red Hat. CloudBOX is a proprietary cloud solution developed by SaM Solutions.

The advantages of a private cloud:

- Individual development
- Storage and network components are customizable
- High control over the corporate information
- High security, privacy, and reliability

The disadvantages of a private cloud:

- Cost intensiveness entails considerable expenses on hardware, software, and staff training.
- Not in the choice of small to medium companies.
- Only suitable for companies that seek to safeguard their mission-critical operations

The cost of using public clouds is often minimal for the end-user, and no capital expenditure is required. Because of the increased level of consolidation and resource pooling provided by private clouds, capital investment is required, but it is still less than the cost of owning and managing the infrastructure. In addition, private clouds provide additional security and compliance assistance than public clouds. As a result, some businesses may prefer to employ private clouds for mission-critical, secure applications and public clouds for basic functions like application development and testing environments and e-mail services.

COMMUNITY CLOUD

The sole difference between a community cloud deployment architecture and a private one is the collection of users. While a private type means that just one firm owns the server, a community type means that numerous firms with comparable backgrounds share the infrastructure and associated resources. Because enterprises have standardized security, privacy, and performance needs, this multi-tenant data center design assists businesses in meeting their business-specific goals. As a result, a community model is ideal for companies that collaborate on joint initiatives.

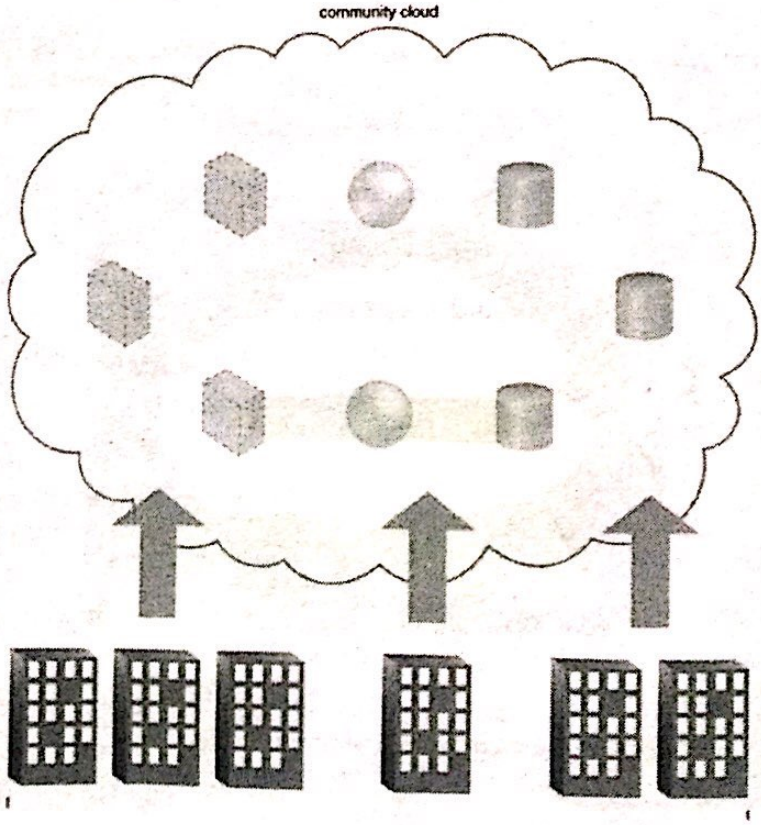


Figure 2.13 Community Cloud

A community cloud helps project creation, administration, and implementation in this situation. Furthermore, the expenditures are shared by all users. This deployment strategy allows several organizations to share computer resources that are part of a community: for example, colleges working in certain areas of study or police forces within a country or state sharing computing resources. Access to a community cloud environment is often restricted to community members.

The advantages of a community cloud:

- Cost reduction
- Improved security, privacy, and reliability
- Ease of data sharing and collaboration
-

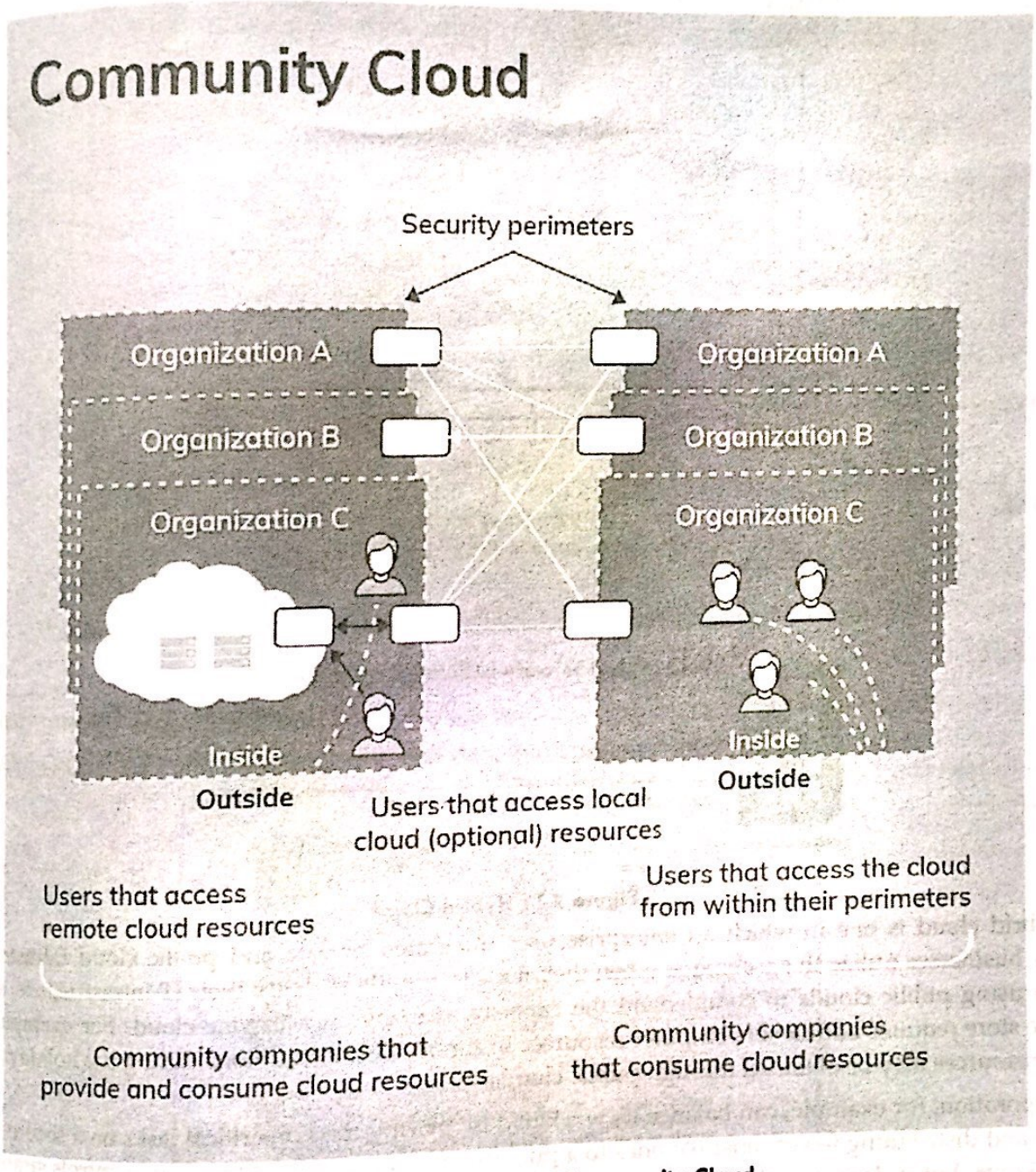


Figure 2.14: Detailed view of Community Cloud

The disadvantages of community cloud:

- Higher cost than that of a public one
- Sharing of fixed storage and bandwidth capacity
- It is not widespread so far

Hybrid Cloud

A hybrid cloud, as is typical of any hybrid phenomena, combines the finest aspects of the three cloud computing deployment paradigms stated above - public, private, and community. It enables businesses to mix and match the aspects of all three categories that best fit their needs.

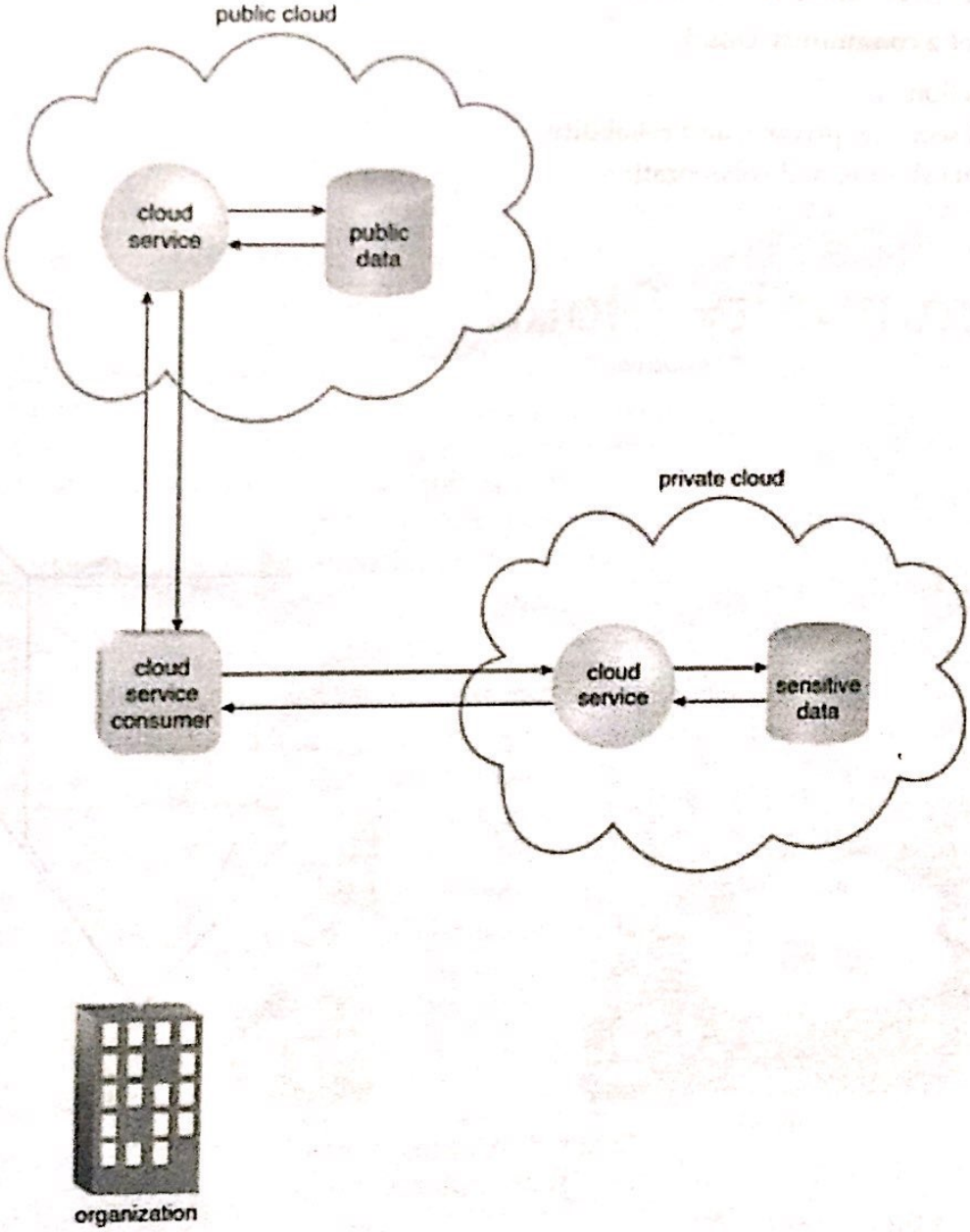


Figure 2.11 Hybrid Cloud

A hybrid cloud is one in which an enterprise uses integrated private and public cloud infrastructure. Many businesses utilize this technique when they need to rapidly scale up their IT infrastructure, such as when using public clouds to complement the capacity available in a private cloud. For example, if an online store requires additional computer resources to run its web applications during the holiday season, such resources may be obtained through public clouds.

A corporation, for example, can balance its workload by placing mission-critical tasks on a secure private cloud and distributing fewer sensitive ones to a public cloud. It not only protects and controls strategically vital assets, but it does it in the most cost- and resource-effective manner feasible for each scenario. This method also makes data and application mobility easier.

The advantages of a hybrid cloud:

- Improved security and privacy
- Enhanced scalability and flexibility

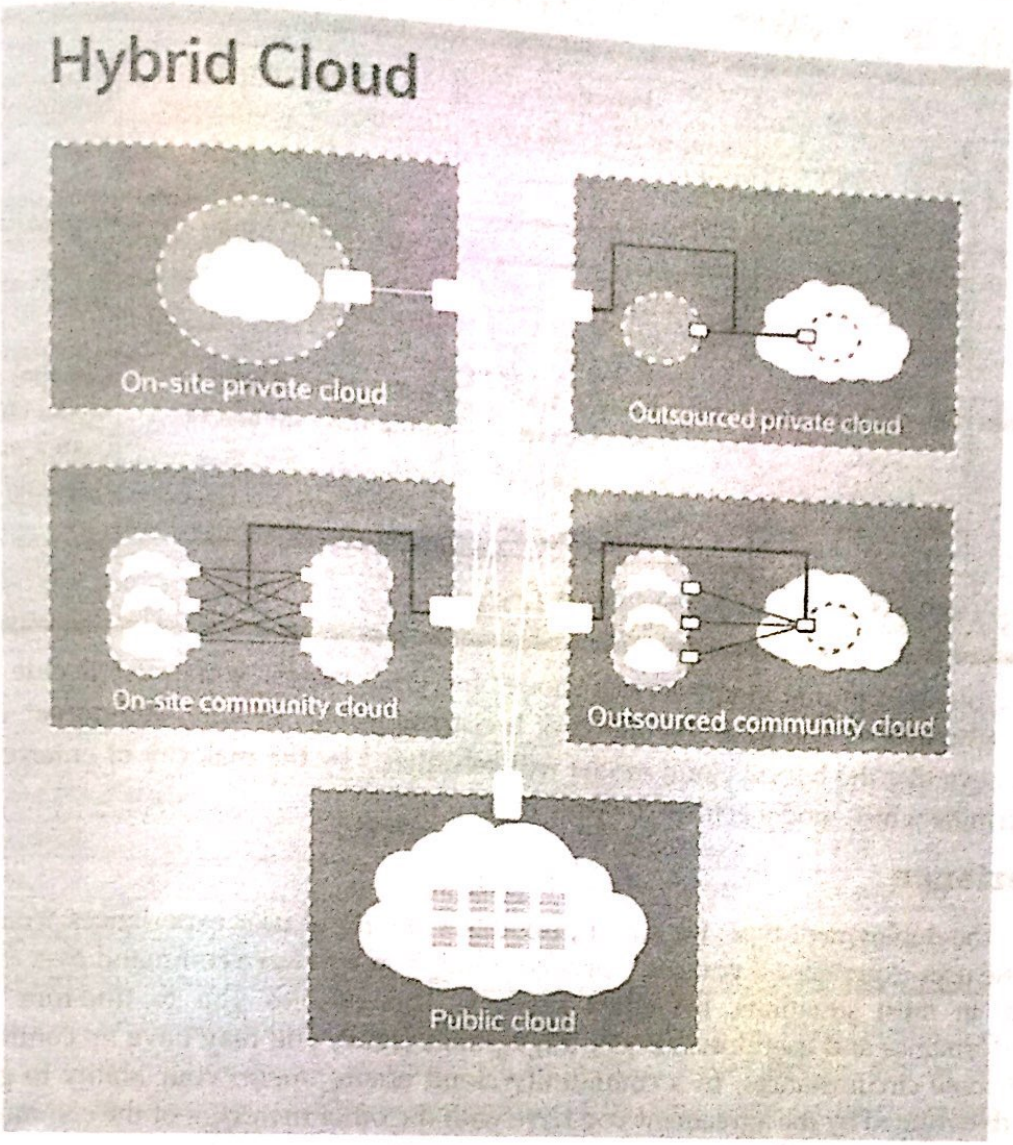


Figure 2.12 Detailed view of Hybrid Cloud

The disadvantages of a hybrid cloud:

- Only suitable if companies can split their data into mission-critical and non-sensitive.

	Type	Properties
1.	Private cloud	• Outsource or own • Lease or buy • Separate or virtual data center
2.	Community cloud	• Private cloud for a set of users with specific demands • Several stakeholders
3.	Public cloud	• Mega scaleable infrastructure • Available for all
4.	Hybrid cloud	• Combination of two clouds • Usually private for sensitive data and strategic applications

Figure 2.15: Different types of cloud and their properties

THE COMPARATIVE ANALYSIS OF THE BEST CLOUD DEPLOYMENT MODELS

Parameters	Public	Private	Community	Hybrid
Ease of setup & use	Easy	Requires IT proficiency	Requires IT proficiency	Requires IT proficiency
Data security and privacy	Low	High	Comparatively high	High
Data control	Little to none	High	Comparatively high	Comparatively high
Reliability	Vulnerable	High	Comparatively high	High
Scalability and flexibility	High	High	Fixed capacity	High
Cost-effectiveness	The cheapest one	Cost-intensive, the most expensive one	Cost is shared among community members	Cheaper than a private model but more costly than a public one
Demand for in-house hardware	No	Depends	Depends	Depends

CHOOSING A CLOUD DEPLOYMENT MODEL

After deciding on the optimal cloud service model for your needs, you must decide on your clou deployment methodology. You have the option of becoming public, private, communal, or hybrid. Mos individuals believe that the hybrid cloud model will be utilized by the majority of enterprises. You must however, determine which model is ideal for your firm.

User Experience

Depending on the deployment type, the cloud provides a variety of user experiences. You will have tota control over the user experience if you use a private cloud. You will have command over the program, the network, and, in most situations, the client systems. This enables you to fine-tune everything for maximum performance and usefulness. If you use a public cloud, you may have no control over the user experience in some circumstances. In a community cloud environment, your ability to govern the user experience is determined by the agreement you have with the other members of the community.

Security

Security is always a difficult subject. It becomes considerably more challenging when working with the cloud. It all boils down to faith. Who do you put your security in the hands of? Many businesses would prefer to rely on a third party than on themselves. There is nothing wrong with that at all. Because security is such an essential matter, you must stick with what you know.

Responsibilities

Responsibilities vary widely depending on the cloud model you choose. This might be an important consideration in your selection. One of the primary motivators for enterprises to use public clouds is a desire to eliminate internal obligations.

SAAS RESPONSIBILITIES BY CLOUD DEPLOYMENT MODEL

Parameter	Public	Private	Community	Hybrid
Application Updates	Provider	Consumer	Consumer	Varies
OS Updates	Provider	Consumer	Consumer	Varies
Antivirus	Provider	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

PaaS Responsibilities by Cloud Deployment Model

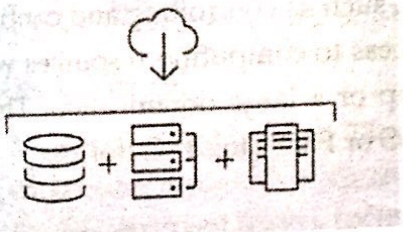
Parameter	Public	Private	Community	Hybrid
Application Updates	Consumer	Consumer	Consumer	Varies
OS Updates	Provider	Consumer	Consumer	Varies
Antivirus	Varies	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

IaaS Responsibilities by Cloud Deployment Model

Parameter	Public	Private	Community	Hybrid
Application Updates	Consumer	Consumer	Consumer	Varies
OS Updates	Varies	Consumer	Consumer	Varies
Antivirus	Consumer	Consumer	Consumer	Varies
Storage	Provider	Consumer	Consumer	Varies
Networking	Provider	Consumer	Consumer	Varies
Physical Server Hardware	Provider	Consumer	Consumer	Varies
Client Application	Consumer	Consumer	Consumer	Varies
Client System	Consumer	Consumer	Consumer	Varies

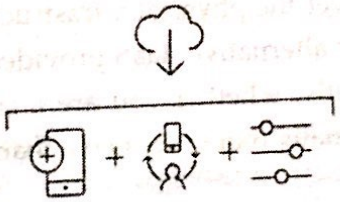
Cloud Service Models

There are three sorts of cloud models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) (Software as a Service). Each cloud model has its own set of advantages that may be tailored to the demands of diverse enterprises. Choosing amongst them necessitates a grasp of various cloud models, as well as an evaluation of your needs and a comprehension of how the selected model can offer your planned set of operations.



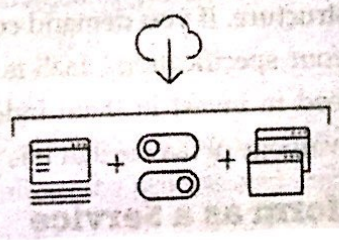
Infrastructure as a service (IaaS)

A vendor provides clients pay-as-you-go access to storage, networking, servers and other computing resources in the cloud.



Platform as a service (PaaS)

A service provider offers access to a cloud-based environment in which users can build and deliver applications. The provider supplies underlying infrastructure.



Software as a service (SaaS)

A service provider delivers software and applications through the internet. Users subscribe to the software and access it via the web or vendor APIs.

Figure 2.16: Cloud Service Models

Infrastructure as a Service

IaaS, or Infrastructure as a Service, is cloud-based virtual provisioning of computing resources. An IaaS cloud provider may supply you with a full variety of computing infrastructures, including storage, servers, and networking gear, as well as maintenance and support. Businesses may choose the computing resources they demand without having to deploy hardware on their premises. Some of the main IaaS cloud service providers are Amazon Web Services, Microsoft Azure, and Google Compute Engine.

Key features of IaaS

- Instead of purchasing hardware completely, users pay for IaaS on demand.
- Infrastructure is scalable depending on processing and storage needs.
- Saves enterprises the costs of buying and maintaining their hardware.
- Because data is on the cloud, there can be no single point of failure.
- Enables the virtualization of administrative tasks, freeing up time for other work.

Benefits of IaaS

- **Minimize Costs**: Using an IaaS cloud architecture eliminates the need to deploy on-premises hardware, lowering expenses.
- Enhanced Scalability: IaaS, being the most adaptable cloud computing paradigm, enables you to scale computing resources up or down based on demand.
- Simple Deployment: IaaS allows you to quickly install servers, processing, storage, and networking to get it up and running.

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

IaaS, being the most adaptable cloud architecture, provides the greatest alternative for IT hardware infrastructure. If you demand control over the physical infrastructure, such as controlling and configuring it to your specifications, IaaS is the best alternative. IaaS provides access to computing resources without the need to invest in them independently, whether you are a startup or a large organization. The only disadvantage of IaaS is that it is substantially more expensive than SaaS or PaaS cloud platforms.

Platform as a Service

PaaS, or Platform as a Service, is simply a cloud basis where you can create, test, and organize various apps for your organization. Implementing PaaS streamlines the company's software development process. PaaS's virtual runtime environment provides a conducive environment for creating and testing applications. The full set of resources available in the form of servers, storage, and networking can be managed by the organization or a platform provider. PaaS services such as Google App Engine and AWS Elastic Beanstalk are common examples. PaaS is also subscription-based, giving you various pricing options based on your business's needs.

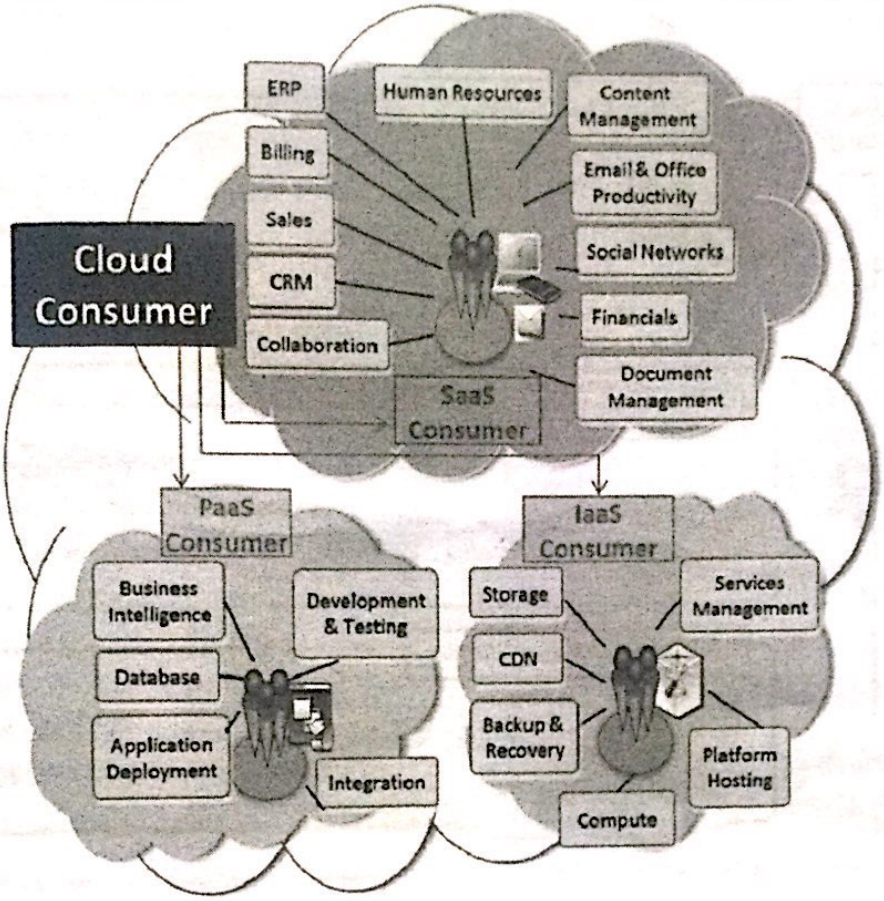


Figure 2.17: Cloud Consumer

Key features of PaaS

- PaaS is a platform that includes tools for testing, developing, and hosting applications all in the same environment.
- Allows enterprises to focus on development rather than underlying infrastructure.
- Security, operating systems, server software, and backups are all managed by providers.
- Allows for collaborative work even when teams operate remotely.

Benefits of PaaS

- **Minimal Development Time**: PaaS decreases development time since the vendor supplies all computing resources such as server-side components, which streamlines the process and improves the development team's focus.
- **Multiple Programming Language Support:**PaaS supports many programming languages, which a software development business may use to create apps for various projects.
- **Enhanced Collaboration:** With PaaS, your company may benefit from improved cooperation, which will aid in the integration of your team members who are distributed across many locations.

If your project involves several developers and vendors, PaaS is the best alternative. Because PaaS rents all of the necessary computing and networking resources, it is simple to construct bespoke apps. PaaS, as a new paradigm, streamlines the app development process, lowering your organization's costs. Furthermore, it is adaptable and provides the essential speed in the process, which will significantly increase your development time. One common downside of PaaS is that, because it is based on virtualized technology, you will have less control over data processing. Furthermore, it is less versatile than the IaaS cloud paradigm.

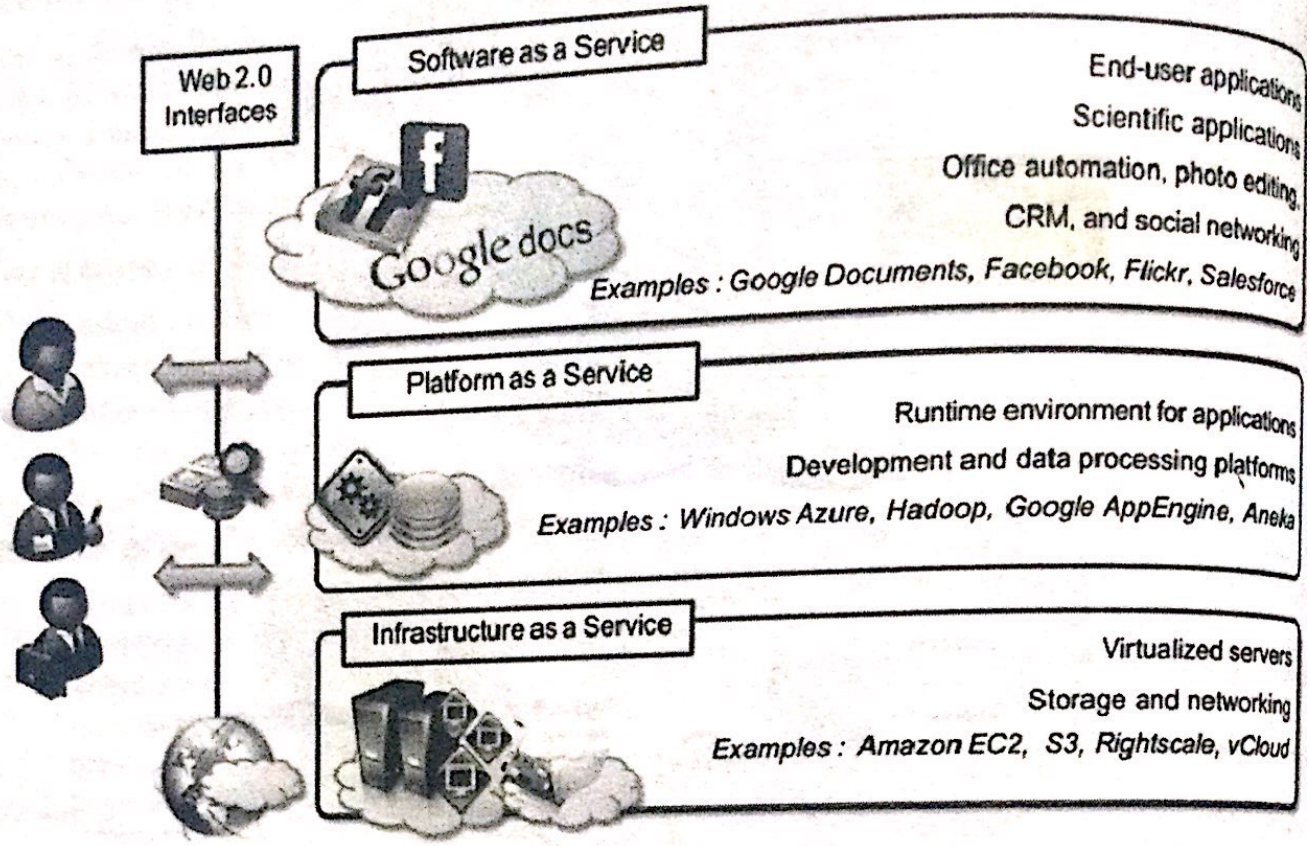


Figure 2.18: Cloud Service Models with Examples

Software as a Service

SaaS, or Software as a Service, is a business model that provides instant access to cloud-based online applications. The vendor is in charge of the complete computer stack, which may be accessed via a web browser. These programs are hosted in the cloud and may be accessed via a paid licensed subscription or for free with limited access. SaaS does not necessitate any installs or downloads to your current computer infrastructure. This eliminates the need to install apps on each of your PCs, with the vendor handling maintenance and support. SaaS examples include Google G Suite, Microsoft Office 365, Dropbox, and many others.

Key features of SaaS

- Software and apps are delivered to consumers via a subscription model by SaaS companies.
- Users are not required to manage, install, or upgrade software; this is handled by SaaS providers.
- Data is secure in the cloud; failure of equipment does not result in data loss.
- Resource use may be scaled based on service requirements.
- Applications may be accessed from practically any internet-connected device, anywhere in the globe.

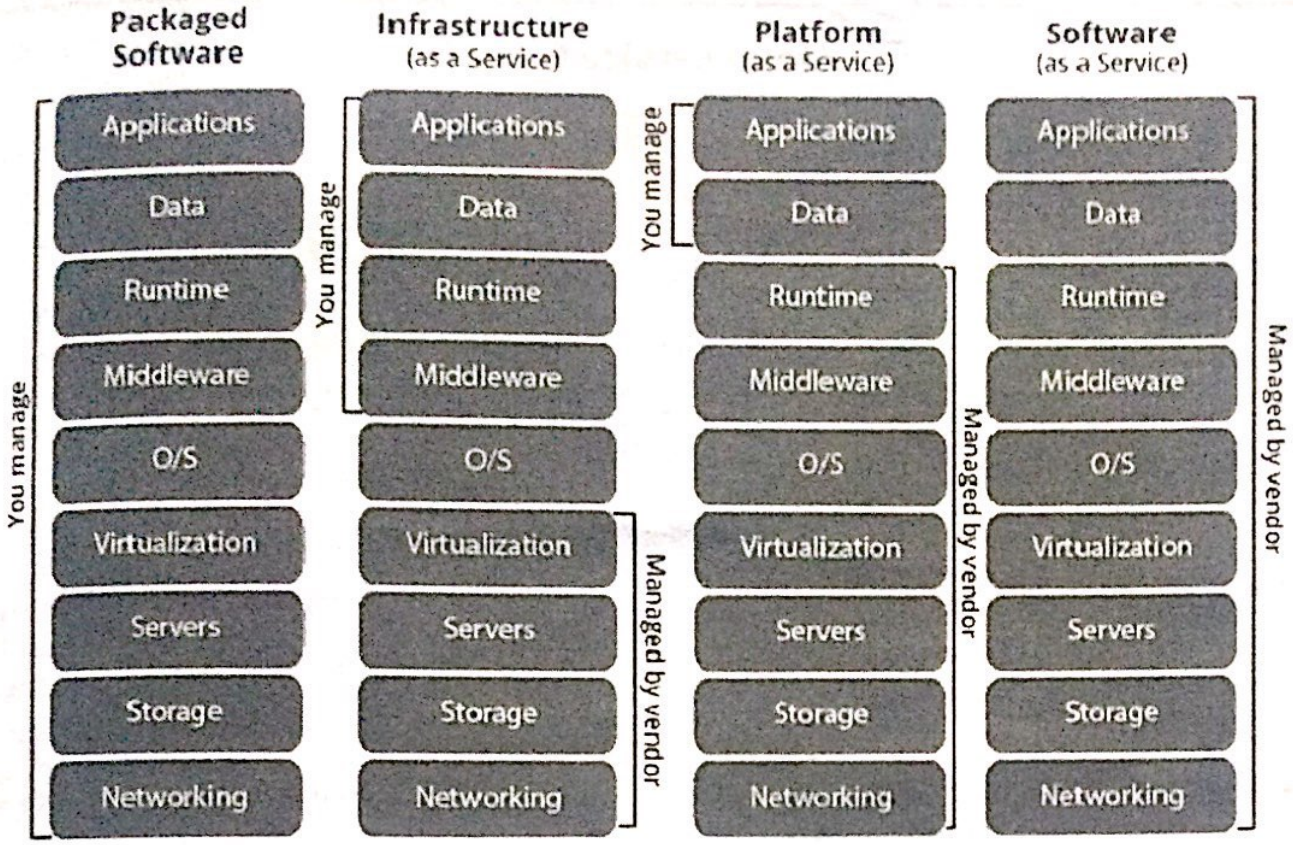


Figure 2.19: Differences between Packaged software, IaaS, PaaS, and SaaS in context to who manages the components.

Benefits of SaaS

- **Affordable:** SaaS is cost-effective because it reduces the costs associated with purchasing, installing, maintaining, and upgrading computer hardware.
- **Accessibility from Anywhere**: With SaaS, you may access the services from anywhere using any device, including smartphones, removing the limits imposed by on-premises software.
- **Ready to Use**: You may rapidly set up SaaS services so that they are ready to use. You only need to sign up for the service to have access to quick and powerful computing resources.

SaaS has its shortcomings, such as the fact that you have no control over the hardware assigned to you because only the seller can handle the software. Communication, material transmission, and meeting schedules are all made easier with SaaS. SaaS is an excellent option for small organizations that lack the funds and resources to build on-premises hardware. Furthermore, SaaS systems would be beneficial to businesses that demand regular communication on their projects.

Along with three important services IaaS, PaaS and SaaS offered in the cloud environment, various other services can also be used in the cloud. Those additional services include Identity, Network, Communication, Monitoring, etc.

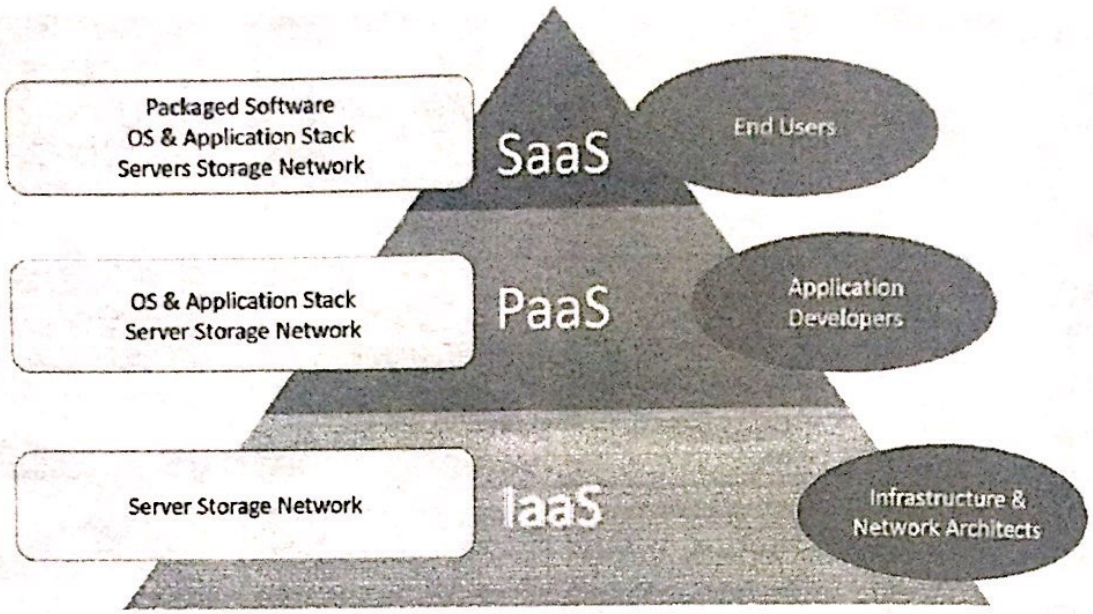


Figure 2.20 Cloud Service Models

- Software as a Service (SaaS) - The consumer is given the ability to use the provider's apps that are hosted on a cloud architecture.
- Platform as a Service (PaaS) - The capacity supplied to the user is the capacity to deploy applications generated or bought by the customer into the cloud infrastructure utilizing programming languages, libraries, services, and tools offered by the provider.
- Infrastructure as a Service (IaaS) - The capacity supplied to the customer is the capacity to supply processing, storage, networks, and other essential computing resources on which the customer can deploy and execute arbitrary software, such as operating systems and applications.

IDENTITY-AS–A-SERVICE (IDAAS)

Identity as a Service (IDaaS) is a third-party authentication infrastructure that is designed, hosted, and maintained by a service provider. IDaaS may be thought of as a cloud-based single sign-on (SSO). A business IDaaS is often acquired as a subscription-based managed service. A cloud service provider may also charge a subscription to host apps and give users role-based access to certain programs or even full virtualized desktops via a secure portal.

Employees at a corporation must log in to the system to execute numerous duties. These systems may be hosted on a local server or in the cloud. The following are some of the issues that an employee may encounter:

- Keeping track of various login and password combinations for accessing many servers.
- When an employee quits the organization, it is necessary to disable all of that user's accounts.

To address the aforementioned issues, a new technology called Identity-as-a-Service evolved (IDaaS).

As a digital entity, IDaaS manages identification information. This identity can be used for online transactions. Identity-as-a-Service - to solve the identity problem, the service essentially leverages the SaaS model and provides single sign-on for web applications, strong authentication and federation across boundaries, integration with internal identities, and identity monitoring, compliance, and management tools and services as appropriate.

The more cloud services you use, the more IDaaS you require, which should also include governance, risk management, and compliance (GRC) as part of the service. GRC is a growingly recognized phrase that represents a new method for enterprises to take an integrated approach to these three areas. However, this

phrase is frequently used to describe a single business activity when, in reality, it encompasses many overlapping and related activities, such as internal audit, compliance programs such as Sarbanes-Oxley, enterprise risk management, operational risk, and incident management.

Gartner defines IDaaS as, "a predominantly cloud-based service in a multi-tenant or dedicated and hosted delivery model that brokers core identity governance and administration (IGA), access and intelligence functions to target systems on customers' premises and in the cloud."

Gartner states the core aspects of IDaaS as:

- **IGA**: Provisioning of users to cloud applications and password reset functionality.
- **Access**: User authentication, Single Sign-On (SSO), and authorization supporting federation standards such as SAML.
- **Intelligence**: Identity access log monitoring and reporting.

Because you cannot become compliant if you cannot manage your identities and associated access privileges consistently in the cloud, IDaaS is a precondition for most other elements of cloud computing. That extends well beyond authentication. Approaches for consistent policy management across different cloud services will necessitate the development of new standards that go beyond federation standards like SAML, authorization standards like eXtensible Access Control Markup Language (XACML), and other standards like the Identity Governance Framework (IGF) currently provide.

Ping Identity, Symplified, TriCipher, and Arcot Systems are some of the current IaaS companies. The most serious challenge to cloud computing is manageability. By far the most serious hazard to the company is handling IDs, authentication, authorization, and all regulatory auditing obligations. An identity access strategy is a critical component and a requirement in any cloud environment. As companies continue to accelerate and manage the adoption of cloud and mobile services, native cloud-basedIDaaS solutions from vendors such as Okta and Centrify, as well as VMware with its new Identity Manager service, have begun to gain popularity.

Identity

The term "identity" refers to a set of characteristics that are connected with something for it to be recognized. Although all things may share the same qualities, their identities cannot be the same. The unique identification feature is used to provide a unique identity. Several identification services are used to authenticate services such as websites, transactions, transaction participants, clients, and so on. The following services may be provided as part of the Identity-as-a-Service:

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

Single Sign-On (SSO)

An authentication procedure in a client/server connection in which the user, or client, enters one name and password and has access to several applications or resources inside a business. When going from one application to another, 'Single Sign On' eliminates the need for the user to enter additional authentications. Companies increasingly utilize Single Sign-On software to overcome the problem of utilizing the separate username and password combinations for multiple servers. This software allows the user to log in only once and control access to other systems. As indicated in the picture below, SSO uses a single authentication server to manage numerous accesses to other services.

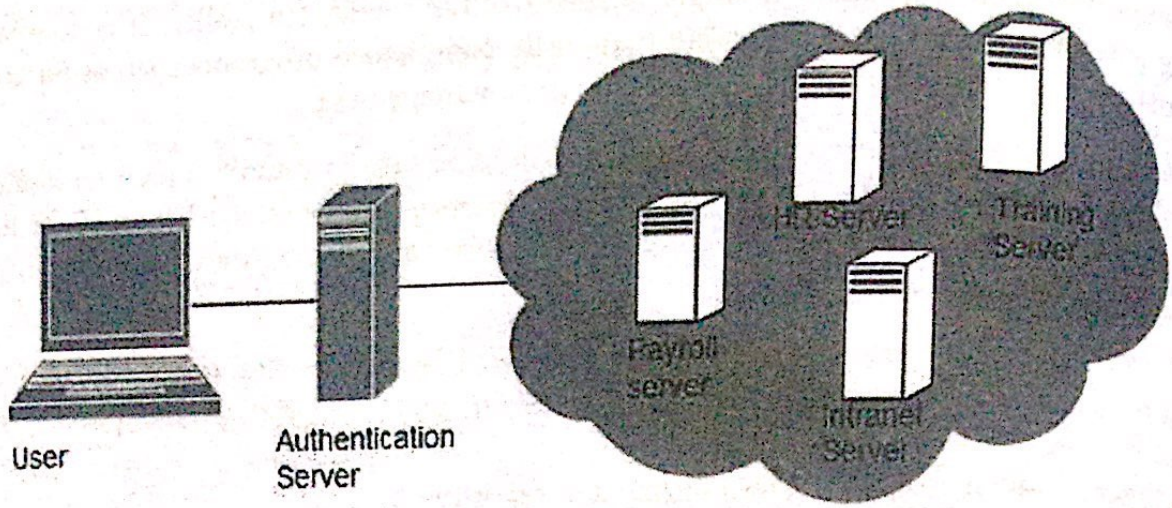


Figure 2.21: SSO

Working Mechanism of SSO

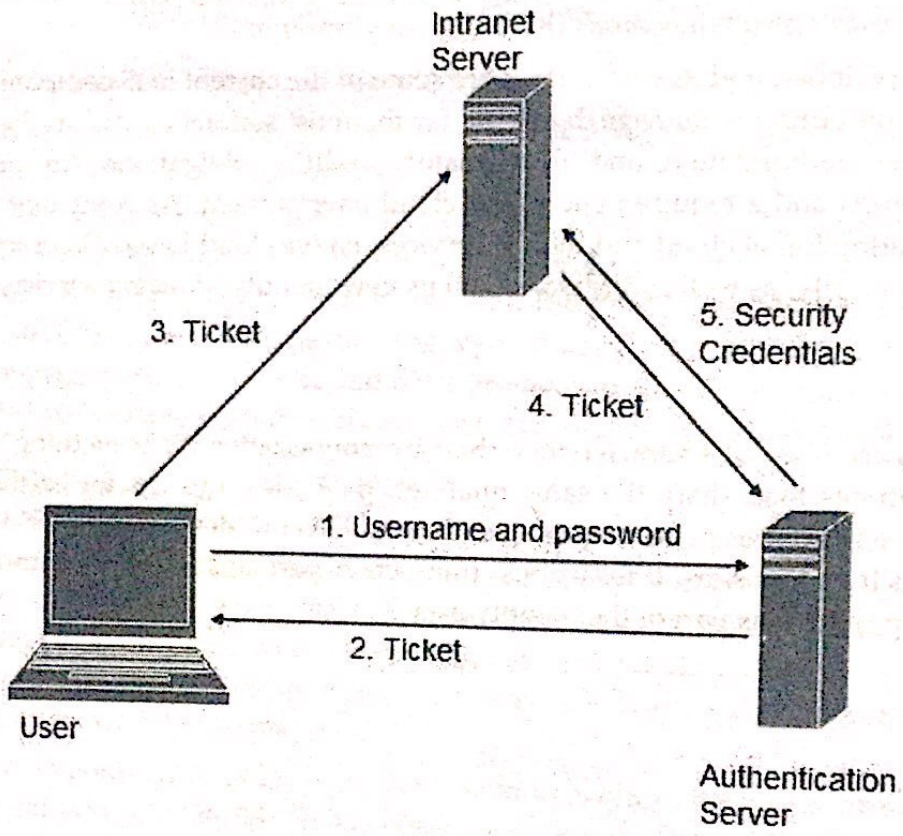


Figure 2.22 Working of SSO

The following steps describe how Single Sign-On software works:

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

If an employee quits the organization, deactivating the user account at the authentication server prevents the person from accessing any of the firm's systems.

FEDERATED IDENTITY MANAGEMENT (FIDM)

The term FIDM refers to the technologies and protocols that allow a user to package security credentials across security domains. It uses Security Markup Language (SAML) to bundle a user's security credentials, as seen in the figure below:

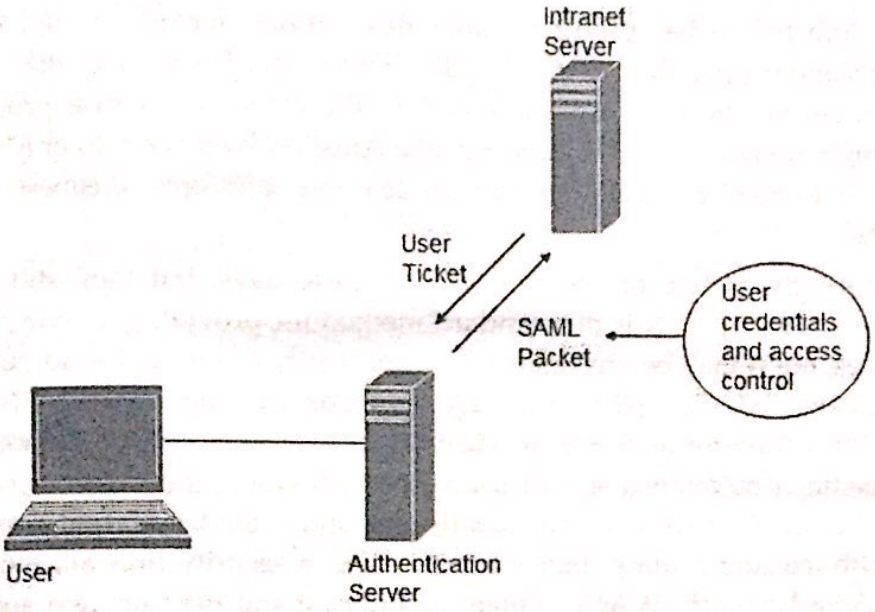


Figure 2.23 FIDM

OpenID

OpenID allows users to utilize a single account to log in to several websites. OpenID is supported by corporations such as Google, Yahoo!, Flickr, and WordPress.com, etc.

Benefits of OpenID

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

Such IDaaS solutions provide a range of identity and access management services such as:

- Single Sign-On (SSO) functionality through the cloud
- Federated Identity Management for Access Governance
- Password Management

Five key capabilities are required to make enterprise IDaaS solutions possible:

1. Single Sign-on (SSO): With SSO, employees, partners, and customers have simple, quick, and secure access to all SaaS, mobile, and enterprise apps with a single login utilizing corporate credentials.
2. Multi-factor Authentication (MFA): Adaptive authentication methods—options to scale up as risk grows depending on scenario changes, user behavior, or application sensitivity—are common in MFA.
3. Access Security: Access security is policy-based access control for apps and APIs that goes beyond SSO to improve security.
4. Directory: While most organizations choose to link IDaaS with their current user databases, a cloud directory may be used, particularly to assist customers and/or partners.
5. Provisioning: User data is synchronized with online and corporate apps via SCIM support and connection with on-premises provisioning.

NETWORK-AS-A-SERVICE (NAAS)

Over the last two decades or more, traditional networking topologies have prescribed that the network hub be built around a single place, such as a data center or a company's headquarters building. This site holds the majority of the computing, storage, communications, and security equipment, and it is where corporate applications are generally housed. Traffic from branch offices and other remote sites is often routed through this hub before being sent to other destinations, including the cloud. Though such a mechanism has been standard practice for many years, it no longer fits the way many businesses function today. For starters, there has been a significant shift to the cloud. Enterprise programs that drive the business are increasingly housed in cloud platforms like Amazon Web Services or Microsoft Azure, either as proprietary apps or as SaaS programs like Office 365 and Salesforce. Businesses frequently employ various cloud systems.

Employees are increasingly mobile or remote workers these days, but they still want safe access to company apps and resources. A VPN is the standard method for providing mobile personnel with access to IaaS or PaaS services, but it may be time-consuming and costly to set up. Cloud migration and mobility are becoming increasingly popular, putting a huge strain on existing networks. Network as a Service (NaaS), along with Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), is sometimes mentioned as a distinct Cloud provider. This excludes networking, firewalls, and related security from IaaS. NaaS can feature a flexible and extended Virtual Private Network (VPN), on-demand bandwidth, custom routing, multicast protocols, a security firewall, intrusion detection and prevention, a Wide Area Network (WAN), content monitoring and filtering, and antivirus. There are no set criteria for what is contained in NaaS so the implementation mechanism varies. Some Network as a Service (NaaS) implementation is also referred to as Telco as a Service (TaaS).

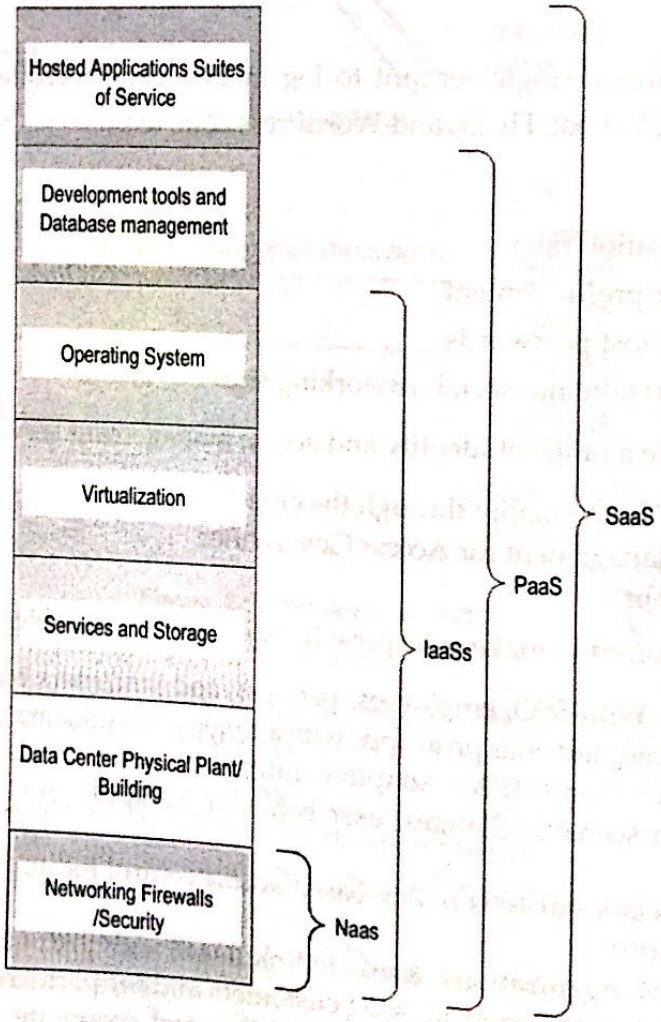


Figure 2.24: NaaS, IaaS, PaaS and SaaS

Service models of NaaS

1. **Virtual private network (VPN):** VPN Extends a private network and the resources it contains across networks such as the Internet. It lets a host computer send and receive data over shared or public networks as if they were private networks, with all of the capabilities and regulations that come with them.
2. **Bandwidth on Demand (BoD):** The process of allocating network capacity based on the needs of different nodes or users. Connection rates can be dynamically modified to the traffic demands of the nodes connected to the link under this architecture.
3. **Mobile network virtualization:** A telecommunications manufacturer or independent network operator creates and runs a network and offers communication access capabilities to third parties, who are often mobile phone carriers on a capacity usage basis. A Mobile Virtual Network Operator (MVNO) is a supplier of mobile communications services that does not own the radio spectrum or wireless network equipment over which it operates.

   Example:Senet - LoRaWAN is a NaaS for IoT and machine-to-machine communication.

COMMUNICATION-AS-A-SERVICE (CAAS)

Communications as a Service (CaaS) is a single vendor's outsourced enterprise communications solution. Voice over IP (VoIP or Internet telephony), instant messaging (IM), collaboration, and videoconference programs employing fixed and mobile devices are examples of such communications. CaaS has evolved in the same way as Software as a Service has (SaaS). The CaaS provider is in charge of all hardware and software administration and provides assured Quality of Service (QoS). CaaS enables enterprises to choose to install communication devices and modes on an as-needed, pay-as-you-go basis. This method avoids the high initial investment and continuous costs associated with a system whose capacity may frequently exceed or fall short of current demand.

CaaS provides flexibility and expandability that small and medium-sized businesses may not be able to afford otherwise, allowing for the addition of devices, modes, or coverage on demand. If required, the network capacity and feature set can be modified from day to day to ensure that functionality keeps up with demand and that resources are not squandered. There is no danger of the system becoming obsolete and necessitating costly modifications or replacement regularly.

CaaS service offerings are frequently bundled and may include integrated access to traditional voice (or VoIP) and data, advanced unified communications functionality such as video calling, web collaboration, chat, real-time presence, and unified messaging, a handset, local and long-distance voice services, voice mail, advanced calling features (such as caller ID, three-way and conference calls, and so on), and a handset. A CaaS solution incorporates redundant switching, network, POP and circuit diversity, customer premises equipment redundancy, and WAN fail-over that is tailored to the needs of their clients. For high availability and survivability, all VoIP transport components are housed in geographically diversified, secure data centers. CaaS provides flexibility and scalability that small and medium-sized businesses may not be able to afford otherwise. CaaS service providers are often prepared to handle peak loads for their clients by offering services that allow for increased capacity, devices, modes, or geographic coverage as customer demand dictates.

Network capacity and feature sets may be modified dynamically, allowing functionality to keep up with customer demand while preventing provider-owned resources from being wasted. From the perspective of the service provider's client, there is very little to almost no risk of the service becoming obsolete because the provider should make periodic updates or replacements of hardware and software to maintain the platform technologically up to date.

Customer management and monitoring of CaaS are minimal to non-existent. It removes the requirement for any capital investment in infrastructure by the business user, as well as the expenditure for ongoing maintenance and infrastructure operations overhead. Customers may use a CaaS solution to access

enterprise-class communication services without having to create their on-premises solution. This enables those clients to reallocate financial and people resources to areas where their company may benefit the most.

Advantages of CAAS

1. **Hosted and Managed Solutions:** Most businesses used to consider remote administration of infrastructure services offered by third parties to be an unsatisfactory option. However, with improved technology, networking, and software over the last decade, the mindset has shifted. This is due to the cost reductions realized by employing such services. CaaS, on the other hand, gives a full communications solution that is controlled by a single vendor, as opposed to the "one-off" services supplied by specialized suppliers. Along with VoIP and unified communications, the integration of fundamental PBX capabilities with enhanced capabilities is managed by a single vendor, who is responsible for all integration and service delivery to customers.
2. **Fully Integrated, Enterprise-Class Unified Communications:** With CaaS, the vendor maintains LAN/WAN, security, routers, email, voice mail, and data storage in addition to providing voice and data access. The vendor can provide constant quality of service from a user's desktop across the network and back by administering the LAN/WAN. Chat, Multimedia conferencing, Microsoft Outlook integration, Real-time presence, "Soft" phones (software-based telephones), Video calls, Unified messaging, and mobility are common advanced unified communications technologies included in a conventional CaaS setup.

   CaaS providers are continually improving their services (in terms of both performance and functionality). The development process, as well as the subsequent deployment of new features in apps, is significantly faster, simpler, and less expensive than ever before. This is due to the service provider performing work that benefits a large number of end customers via the provider's scalable platform architecture. Because numerous end-users of the provider's service eventually share this cost (which, in their opinion, is minor compared to shouldering the load alone), services can be supplied to individual consumers at a price that is appealing to them.
3. **No Capital Expenses Needed:** When a company outsources its unified communications needs to a CaaS service provider, the provider provides a full solution tailored to the company's specific requirements. Customers are charged a price (typically invoiced monthly) for the services they utilize. There is no capital investment because customers are not obliged to acquire equipment. These sorts of services include continuous maintenance and upgrade fees borne by the service provider.

   The utilization of CaaS services enables businesses to collaborate across any workspace. Advanced collaboration technologies are now employed throughout any business to build high-quality, secure, and adaptable work environments. This enables employees, partners, vendors, and consumers of a company to communicate and cooperate more efficiently. Better communication enables businesses to respond rapidly to market developments and gain a competitive edge. CaaS may also help an organization's decision-making process. Innovative unified communications features (such as presence, instant messaging, and rich media services) aid in ensuring that information reaches those who require it as soon as possible.
4. **Flexible Capacity and Feature Set:** Customers that outsource communications services to a CaaS provider only pay for the capabilities they require at the time they use them. The service provider can spread the cost of services and delivery among a wide number of customers. As previously indicated, this reduces the cost of implementing shared feature capabilities for clients. Economies of scale offer service providers enough flexibility to avoid being bound to a single vendor investment. They can use best-of-breed suppliers like Avaya, Cisco, Juniper, Microsoft, Nortel, and ShoreTel more cost-effectively than any individual firm.

5. **No-Risk of Obsolescence:** Rapid technological developments, anticipated long ago and known as Moore's law, have resulted in product obsolescence in ever-shorter periods. Moore's law highlights a tendency that he identified and that has stayed true since the introduction of integrated circuits (ICs) in computing technology. Since the creation of the integrated circuit in 1958, the number of transistors that can be placed cheaply on an integrated circuit has grown rapidly, doubling every two years.

   In contrast to IC components, the average life cycle of PBXs and essential communications equipment and **systems** ranges from five to ten years. With the frequent development of newer models for all forms of technology (PCs, mobile phones, video software and hardware, and so on), these types of devices now have considerably shorter life cycles, often as little as a year. CaaS companies bear this burden for the customer by updating the equipment in their products regularly to suit changing market needs.

6. **No Facilities and Engineering Costs Incurred:** CaaS providers host all of the equipment required to offer their services to consumers, removing the need for users to maintain data center space and infrastructure. There is no additional cost for the continual power usage that such a facility would necessitate. Customers benefit from numerous carrier-grade data centers with complete redundancy—all of which are included in the monthly charge.

7. **Guaranteed Business Continuity:** Would your company's disaster recovery strategy allow your organization to continue functioning without interruption if a catastrophe occurred at its physical location? How long might your organization continue if there was a significant or prolonged communication outage? For the vast majority of firms, the answer is "not for long." Risk distribution through the use of geographically separated data centers is already the standard. It reduces risk and enables businesses in a disaster-affected area to recover as quickly as feasible. CaaS providers adopt this method since most businesses do not even consider voice continuity in the event of a disaster. Unlike data continuity, removing single points of failure in a voice network is frequently prohibitively expensive due to the project's vast scale and managerial complexity. A CaaS solution incorporates many levels of redundancy into the system, ensuring that there is no single point of failure.

MONITORING-AS-A-SERVICE (MAAS)

Monitoring-as-a-Service (MaaS) is the supply of security as a service, mainly on corporate platforms that use the Internet to do business. MaaS has grown in popularity during the previous decade. Its popularity has expanded much more since the introduction of cloud computing. Protecting an organization or government client from cyber-attacks is what security monitoring entails. A security team is critical in ensuring the confidentiality, integrity, and availability of IT assets. However, for most businesses, time and budget restrictions restrict the efficacy of security operations. This necessitates continuous monitoring of the security infrastructure and important information assets.

To protect the integrity of these systems, several industry standards require firms to monitor their security environment, server logs, and other information assets. Effective security monitoring, on the other hand, may be a demanding endeavor since it necessitates modern technology, qualified security specialists, and scalable processes—none of which are inexpensive. MaaS security monitoring services provide real-time, 24/7 monitoring and near-instant incident response throughout a security infrastructure, assisting clients in protecting key information assets. Before the introduction of electronic security systems, security monitoring and response relied mainly on human resources and capabilities, limiting the accuracy and efficacy of monitoring operations. The incorporation of information technology into facility security systems, as well as their capacity to connect to security operations centers (SOCs) via corporate networks, has significantly altered that image during the last two decades.

This indicates two things:

Conventional SOCs have a substantially higher total cost of ownership (TCO) than contemporary technology SOCs; and Obtaining reduced security operations expenses and improved security effectiveness requires contemporary SOC design to employ security and IT technologies to solve security concerns.

Customers can also benefit from security monitoring services by automating the gathering and reporting of certain occurrences of interest, such as log-in failures. Log monitoring of key servers is frequently required by regulations and industry norms to maintain the integrity of confidential data. The security monitoring services provided by MaaS providers streamline this time-consuming operation.

CLOUD INTEROPERABILITY AND STANDARDS

Interoperability refers to the capacity of information and communication technology (ICT) systems and the business processes they support to interchange data and share information and knowledge.Interoperability across clouds, as well as file portability from one cloud to another, has been a stumbling block in cloud computing's widespread adoption. The lack of interoperability has become a hurdle to the adoption of cloud services.

Interoperability refers to the capacity of the Cloud ecosystem to communicate information between distinct cloud platforms. It entails being able to share data at various tiers amongst cloud service providers in a smooth manner. Interoperability is the capacity of two systems to comprehend each other's intentions in a communication exchange. Interoperability is a prerequisite for interchangeability. The purpose of standards is interoperability; however, standards do not ensure interoperability.

"Interoperability facilitates portability."

Motivations for Interoperability

- To increase customer choice, competition, and innovation
- To allow more players in the market

INTEROPERABILITY

The ability of two or more systems or components to communicate information and utilize that information. Interoperability in cloud computing refers to the capacity of public and private cloud services to comprehend each other's APIs, configuration, data formats, and authentication and authorization methods. The interfaces are standardized "so that you, as a client, may transition from one cloud provider to another with as little or no harm to your systems as feasible.

PORTABILITY

Portability refers to a cloud client's ability to move apps and data between on-premises and cloud systems, as well as between cloud services supplied by numerous providers. Program portability and data portability are the two types of portability. Application portability refers to the ability to move an application "from one cloud service to another cloud service or between a cloud service customer's system and a cloud service."

It is vital to be able to do this with ease. "The goal is to make as few changes to the application code as possible." Cloud data portability refers to the ability to transfer data between cloud and on-premises systems. This should be done in a generally understood electronic format, and there should be a way for data to be imported into the desired cloud service - usually an API.

Policy Objectives

- Right to move applications between Cloud providers
- Right to move data quickly between Cloud providers
- Right of the user to own their data
- Keep overhead of certification and compliance to a minimum
- Apply open access/open-source policies that allow extension of APIs and specs
- Demand-side: Interoperability between Cloud services from different providers to prevent vendor lock-in
- Open and flexible market to provide choice for consumers
- Transparency and technology neutrality

Functional Scope

Interoperability in the context of Cloud Computing refers to the capacity of individuals and organizations to extensively embrace Cloud Computing technology and related services in such a way that disparate Cloud platforms may share information in a unified manner and eventually function together flawlessly. Interoperability examples include solutions operating on many different Cloud instances and the utilization of resources in other heterogeneous Cloud instances. To achieve the desired interoperability, standards at all levels are necessary, including infrastructure, platform, application, service, data, and management.

Use Cases

- The user of one Cloud accessing storage in another Cloud (to provide elastic storage)
- Applications and services running on (and communicating between) heterogeneous cloud platforms
- Application using resources (CPU, storage) in another heterogeneous cloud platform (resource bursting)
- Resource sharing across different time zones
- Demonstration of data portability (across Service Providers)
- Transfer a running STATEFUL service from Cloud Provider A to B
  - Moving a file sharing service between Cloud providers
  - Moving a streaming service between Cloud providers
- B2B procurement from Buyer Cloud vs. Supplier Cloud
- End customer going through the broker (IT Provider) to Cloud
- Move of the on-premises server to/from public, private or hybrid Cloud
- Demonstration of need for integration/federation of Clouds
- Demonstration of the use of Trans-National / Trans-Regional Clouds

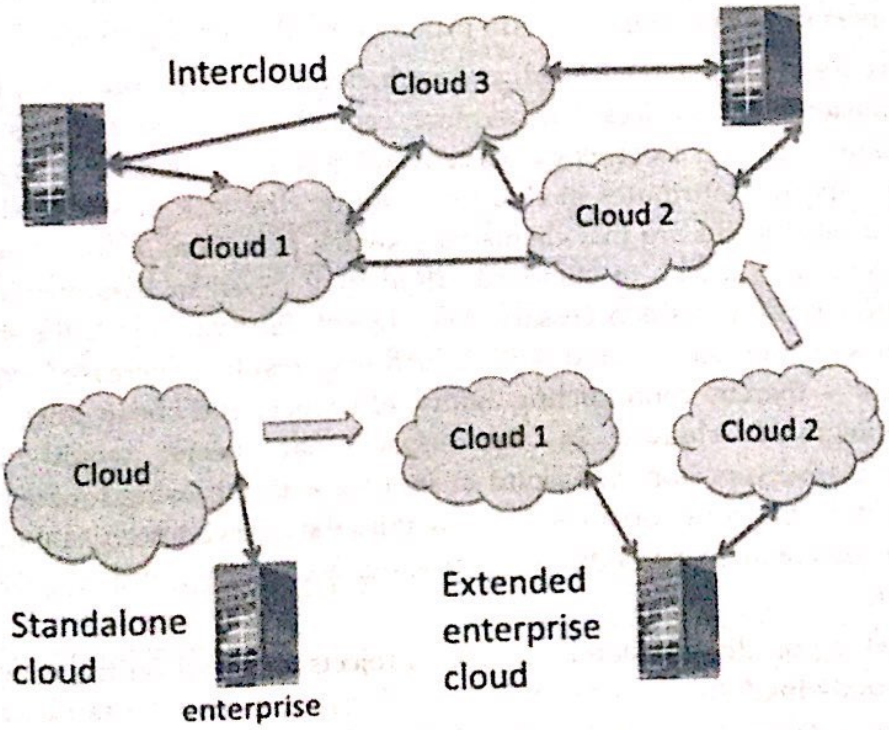


Figure 2.25 Cloud Interoperability

The primary purpose of cloud computing standardization is to make cloud applications more scalable, interoperable, and secure.

This entails:

- A cloud computing interoperability and integration standard which relates to cloud interoperability and an integrated interface standard.
- A cloud computing service interface and application development standard is a standard for exchanging data across cloud computing and service layers.
- An interface standard for distinct layers of cloud computing refers to an interface standard for the architecture layer, platform layer, and application software layer.
- A standard for cloud computing business indexes includes enhanced user asset utilization, resource and performance optimization, and performance-price ratio.
- Design, planning, architecture, modeling, deployment, management, supervision, operation support, quality control, and service level agreements are all part of a cloud computing architecture management standard.
- A security and privacy guideline for cloud computing refers to the physical and logistical standards that are important for data integrity, availability, and secrecy.

When using various clouds, interoperability is required for at least three reasons:

- safeguarding end-user investments in development
- growth of the cloud ecosystem and market
- make full use of flexibility and the pay-as-you-go idea

At design and runtime, the problem is multidimensional. Individual or coordinated actions are being taken by the standardizing bodies. However, present solutions only partially solve the problem, and adoption is minimal. One of the fundamental differences between cloud computing and traditional corporate computing is the ability of the infrastructure to be programmable. Most physical resources in business computing systems, such as servers, storage, and network connections, should be installed manually. Nonetheless, depending on the development demands, cloud computing developers can define how these identical components are virtually organized or interconnected, how the virtual infrastructure architecture is established, and how they interact with each other. To perform this virtual deployment and maintenance, developers must manipulate an API provided by the cloud provider.

However, cloud APIs are not yet standardized, and each cloud provider today has its specialized API for delivering and administering its services. Furthermore, each cloud provider has its solution, which tends to lock consumers onto a certain technology. Given that elements such as agility, efficiency, and low related cost are also important attributes in cloud computing, the lack of standards is unquestionably a disadvantage. The reasons for this are that clients may switch providers or mix them optimally based on their needs. In this situation, a lack of standardization may result in disadvantages when relocating, integrating, or exchanging resources is necessary. The biggest disadvantage is the requirement to rework programs to conform with alternative cloud APIs, which may result in increased expenses, various types of delays, and hazards – thereby contradicting agility, efficiency, and cheap prices. Another issue is the requirement for integrated clouds, in the sense that users would be able to move information/applications/servers from one cloud to another without losing functionality.Even if the lack of a standardized API is the most obvious issue within the cloud interoperability subject, it is also necessary to arrange for common procedures for pricing, accounting, and monitoring various metrics across cloud boundaries.

Many groups are working on diverse standardization projects centered on the common issue of clouds. Among them are the following:

- **Service modeling**: Open SCA, USDL, SoaML, CloudML, EMML
- **Service interfaces**: OCCI, CIMI, EC2, TOSCA, CDMI
- **Infrastructure**: OVF

CLOUD SOLUTIONS

Cloud Ecosystem

A cloud ecosystem is a complex structure of interconnected components that work together to provide cloud services. An ecosystem in nature is made up of living and nonliving elements that are linked and collaborate. The ecosystem in cloud computing includes hardware and software, as well as cloud customers, cloud engineers, consultants, integrators, and partners.

A public cloud provider is at the heart of a cloud ecosystem. It might be an IaaS firm like Amazon Web Services (AWS) or a SaaS company like Salesforce. Software firms that use the provider's core platform, as well as consultants and organizations that have developed strategic agreements with the provider, are at the heart of the cloud. There is no vendor lock-in since various firms overlap, thus complicating the ecosystem. AWS, for example, is the hub of its ecosystem, but it is also a component of the Salesforce ecosystem. Salesforce operates a number of its services on AWS's infrastructure, and Salesforce clients may acquire access to AWS components such as its Simple Storage Service via devices known as connectors.

A vibrant ecosystem makes it simple for a cloud provider's clients to identify and acquire business apps, as well as to adapt to changing business demands. When applications are offered through a provider's app store, such as AWS Marketplace or Microsoft Azure Marketplace, the consumer gains access to a library of different vendors' software and services that have previously been checked and vetted for security, risk, and pricing.

The Benefits

A cloud ecosystem may be used by businesses to create new business models. A medical device maker, for example, may easily build a heart-monitoring service on the cloud infrastructure of its cloud service provider and then offer the service alongside its primary business of making heart monitors for hospitals.

It is also easy to collect data and study how each component of the system impacts the others in a cloud ecosystem. For example, if an ecosystem has patient data, smart device logs, and healthcare provider data, it is feasible to examine trends across a large patient population.

Cloud Business Process Management (Cbpm)

Cloud-based business process management software offers strategic process optimization, lower technology costs, and greater IT alignment with business goals. The new IT paradigm and business model may promote new growth prospects, enhance profit margins in the private sector, and help government agencies achieve more efficient and successful missions.

The benefits of CBPM:

- Low initial costs
- Rapid deployment with no human maintenance
- Predictable expenses throughout the application's life cycle
- Rapid return on investment

CBPM automates business rules to organize human workflow, traditional enterprise systems, and cloud computing. An example of CBPM would be an iBOLT system that connects JD Edwards ERP systems, SharePoint, Salesforce.com, Amazon Web Services, Google Docs, and social media sites such as Twitter, and arranges procedures between these systems in either synchronous (real-time system-to-system) or asynchronous (system to human workflow) mode, or some combination of the two.

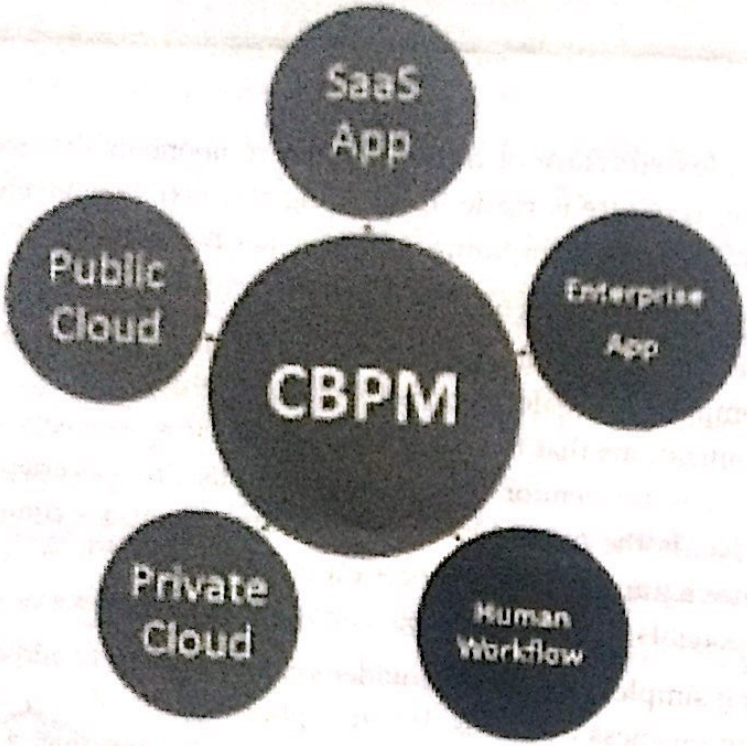


Figure 2.26 Cloud BPM

As a growing portion of commercial software is hosted privately in the cloud or given as SaaS apps, the requirement for BPM on the cloud becomes critical. Many analysts make the error of considering cloud integration as a one-time event; these analysts mix up cloud integration with cloud migration. Consider a corporation that decides to employ a SaaS-based HRIS solution while keeping an on-premises ERP system. To transfer information from the present enterprise HRIS database to the SaaS HRIS application, a cloud migration project will be required.Cloud integration is also required to manage the continuing data interchange between the HR system and the major ERP system, which is deployed in the enterprise data center. With such a huge installed base of ERP systems, the need for this type of ERP connection with cloud-based or SaaS applications will undoubtedly continue for a long time.

Advantages of CBPM

- Even if you are certain that implementing BPM would be a good decision for your company, deploying BPM in the cloud allows you to test the waters without making a full-fledged commitment.
- You will be employing BPM software as a service (SaaS) provided via the cloud, rather than constructing a massive and complex IT infrastructure. When there is no infrastructure to develop, there is also no infrastructure to maintain.
- Due to the lack of a huge internal infrastructure, you will be able to implement business process management in your firm quickly. Investors are more confident as a result of the shorter time to market. Furthermore, because cloud-based apps and data are simpler to coordinate, the operations you oversee will be more efficient.
- The way we work is changing as a result of mobile technologies. Employees may now work from mobile devices, and they are not simply checking email or managing their calendars. They were managing core company operations.

CLOUD SERVICE MANAGEMENT

The provision of dynamic, cloud-based infrastructure, platform, and application services does not take place in a vacuum. Cloud service management and cloud monitoring technologies, in addition to best practices for successful administration of all aspects related to cloud service delivery, enable providers to keep up with the constantly shifting capacity demands of a highly elastic environment.

Cloud monitoring and management solutions enable cloud providers to maintain peak performance, continuity, and efficiency in virtualized, on-demand settings. These tools, which are software that maintains and monitors networks, systems, and applications, allow cloud providers to not only ensure performance but also better coordinate and automate resource supply. Cloud monitoring solutions, in particular, enable cloud providers to track the performance, continuity, and security of all components that support service delivery: the hardware, software, and services in the data center and across the network infrastructure.

Cloud providers may leverage service quality to differentiate themselves in what remains a crowded market by successfully managing and monitoring their cloud services. Effective cloud service management also reduces the likelihood of frequent cloud outages, which can jeopardize security systems. The technologies also assist cloud providers to save expenses and improve profit margins by enhancing operational efficiency. However, attaining these objectives might be challenging in a complicated virtual delivery system with little visibility and control.

Performance monitoring (response time, latency, uptime, etc.), security and compliance audits and management, and starting and managing disaster recovery and contingency plans are all common duties in cloud management techniques.

Some fundamental ideas of cloud service management are shared with those of traditional IT service management. Cloud management solutions assist service providers in administering the systems and applications that support the on-demand service delivery paradigm. The purpose of these practices is to increase the efficiency of the cloud environment while also providing a high degree of customer happiness.

Cloud service management, in essence, uses the customer viewpoint as the measure of service assurance and manages all individual IT resources to support that. This entails altering the operations and rules of all virtual environment assets that support and affect the on-demand service delivery model as needed. Servers, software, and services that offer access and connectivity to these cloud services are examples of such assets.

CLOUD OFFERINGS

Cloud Analytics

Cloud analytics is a marketing phrase for firms that use cloud computing to do analysis. It employs a variety of analytical tools and methodologies to assist businesses in extracting information from vast amounts of data and presenting it in a way that is simply categorizable and accessible via a web browser. Cloud analytics is intended to organize and make official statistics data easily accessible via the user's web browser.

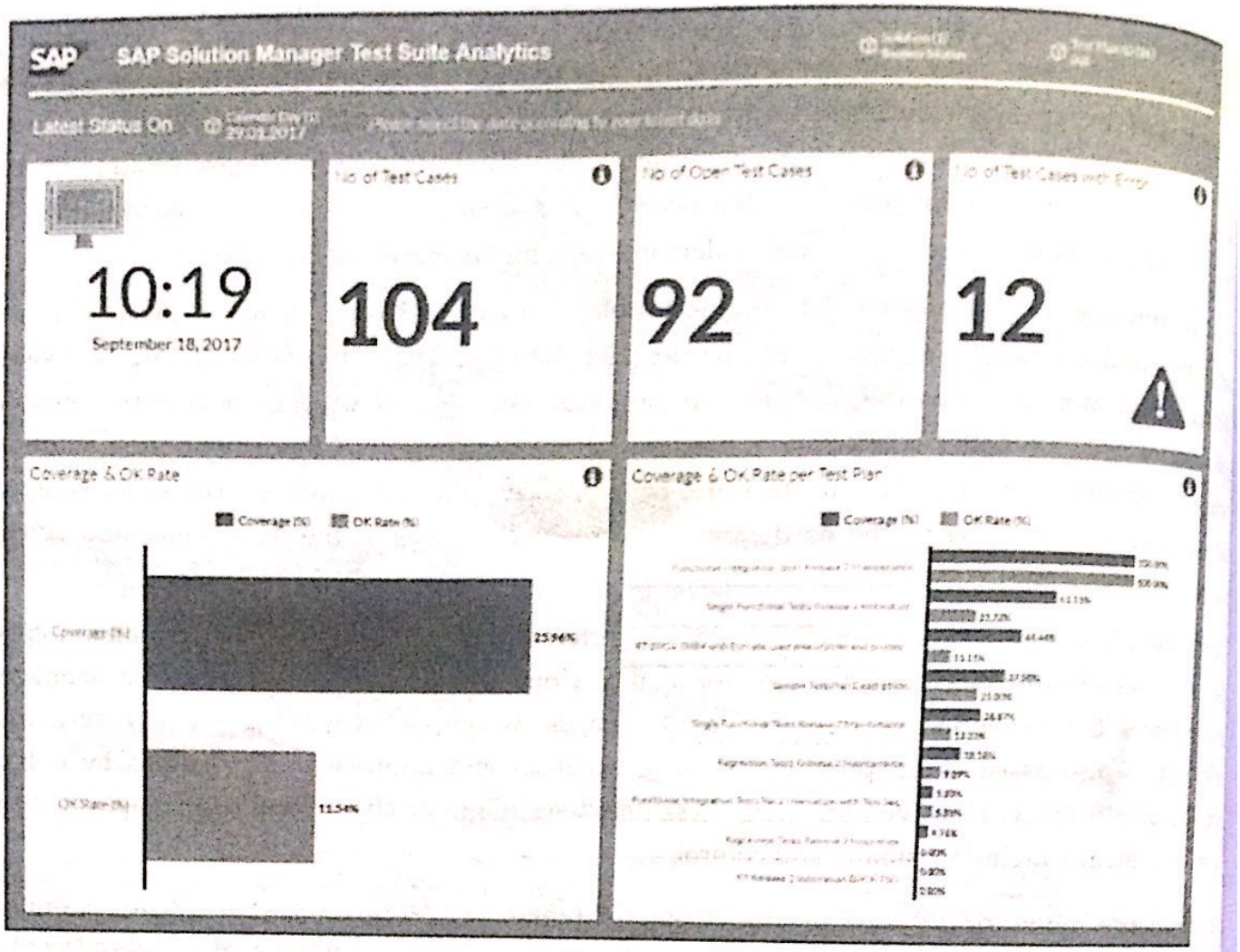


Figure 2.27 Analytics shown on SAP Solution Manager Test Suite Analytics

Cloud analytics is a service paradigm in which components of the data analytics process are delivered via a public or private cloud. Cloud analytics apps and services are often priced on a subscription or utility (pay-per-use) basis.

Data sources, data models, processing applications, computing power, analytic models, and sharing or storage of findings are the six fundamental parts of analytics. Any analytics initiative "in which one or more of these elements are implemented in the cloud" qualifies as cloud analytics.

Hosted data warehouses, software-as-a-service business intelligence (SaaS BI), and cloud-based social media analytics are examples of cloud analytics products and services. SaaS BI (also known as on-demand BI or cloud BI) is the distribution of business intelligence (BI) applications from a hosted location to end-users. Although this strategy is scalable and makes startup easier and less expensive, the product may not have the same functionality as an in-house program.

Cloud-based social media analytics entails the remote delivery of tools such as apps for picking the finest social media sites for your needs, distinct programs for data harvesting, storage services, and data analytics software. A hosted data warehouse is a consolidated repository for corporate data that is accessible to users from a distant site managed by the service provider rather than on the organization's systems.

Before investing in cloud analytics, a company must properly understand the scope of the project. The risk is that individuals will proceed down this path without fully comprehending the implications. Investing in cloud analytics may be beneficial to a company, but careful preparation is required to guarantee that all six analytics aspects are addressed.

Best Cloud Analytics

- Microsoft Power Bi
- Host Analytics
- Zoho Reports
- SAP Solution Manager Test Suite Analytics
- IBM Watson Analytics

TESTING UNDER CONTROL

Cloud testing is a subtype of software testing in which cloud-based online applications are tested using simulated, real-world online traffic. Cloud testing also evaluates and verifies certain cloud features, such as redundancy and performance scalability. Cloud solutions have been used by several small to medium-sized IT firms. As a result, cloud testing is required to confirm functional system and business requirements. In addition to cloud experience, cloud testing engineers must be familiar with various types of testing and technologies.

Cloud testing often includes monitoring and reporting on real-world user traffic situations, as well as load balancing and stress testing for a variety of simulated usage scenarios. Load and performance testing on cloud computing applications and services, particularly the ability to use these services, to guarantee optimal performance and scalability under a wide range of scenarios. Cloud computing presents various difficulties, such as management, dependability, and security. Before doing actual cloud testing, businesses often outline a test plan.

> Cloud testing, also known as cloud-based testing, is the evaluation of a Web application's performance, dependability, scalability, and security in the cloud computing environment of a third party. Cloud models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are critical components of a cloud testing approach.

Cloud test environments may be deployed quickly and easily by eliminating the need for sharing environments among test teams, which helps to avoid environment-related schedule delays. Built-in collaboration tools enable geographically dispersed development teams to work in a cloud testing environment 24 hours a day, seven days a week, and testers can scale application workloads to thousands or millions of concurrent users to identify performance issues before an application goes live.

Cloud testing, as opposed to traditional on-premises environments, provides consumers with pay-per-use pricing, flexibility, and a shorter time-to-market. The test techniques and technology used to do functional testing against cloud-based apps are not materially different from those used to test traditional in-house systems, but understanding the non-functional risks associated with the cloud is crucial to success. If testing includes production data, for example, adequate security and data integrity protocols and procedures must be in place and validated before functional testing can commence.

Key cloud testing elements include:

- Identifying appropriate testing types
- Recognizing cloud features and doing a risk/challenge analysis
- Creating a cloud-based testing environment
- Simulating real-world difficulties through the use of the appropriate testing technique

Objectives of cloud testing:

- To assess the functional services, business processes, and system performance of cloud-based app to ensure their quality.
- To analyze a software program in a cloud-based environment in terms of performance, security scalability, and economic assessment.
- To examine the services provided by the cloud environment.
- To ensure interoperability, the software application's compatibility with multiple cloud-based components must be tested.

CLOUD TESTING STRATEGY COMPONENTS INCLUDE

- **Performance and Load Testing:** Ascertain that a cloud solution fits the business needs unique to cloud computing.
- **Stress Testing and Recovery Testing:** Ensure data recovery following a hardware failure.
- **Security Testing:** Ensures that a cloud solution fulfills data security standards.
- **System Integration Testing:** Addresses functional aspects of the system.
- **User Acceptance Testing:** Ensures that the cloud solution satisfies the businesses or personal user's documented needs.
- **Interoperability and Compatibility Testing:** Guarantees cloud service and vendor migration

In addition to identifying relevant testing types, cloud testing teams focus on the following aspects:

- Security risks
- Multiple Web browser support
- User interface issues
- User data accessibility

Advantages of Using Cloud-Based Testing Tools

- When compared to traditional test automation tools, the total cost of ownership of cloud-based testing technologies is quite low. Cloud-based products offer lower hardware requirements and do not require pricey per-seat license fees.
- Cloud-based technologies provide for a high degree of reusability of test components. Because they are extremely scalable, they are perfect for load and performance testing scenarios. Pay as you go allows you to easily scale up and down your cloud use based on your testing needs.
- Cloud-based technologies enable virtualization benefits. They help businesses to make the most use of their resources, resulting in more flexible and efficient testing.
- Cloud-based automation technologies enable teams in multiple locations to effortlessly work with one another. Testers may simply test from various places and get test findings from anywhere in the globe without having to upload and download them.
- Tools provide benefits such as increased productivity and shorter test cycles. Cloud-based automation technologies have the added benefit of rapid setup and tool deployment. They do not require a long setup and installation process, as do traditional tools. Testing may begin virtually quickly from any location.
- Cloud-based tools eliminate many of the IT administration duties inherent in conventional solutions, such as installation, licensing, adding/replacing users, and simultaneous execution of upgrades in systems across geographies, among others.

VIRTUAL DESKTOP INFRASTRUCTURE

Virtual desktop infrastructure (VDI) is a data center virtualization technique that runs a desktop operating system on a centralized server. VDI is a variant of the client-server computing technology, sometimes known as server-based computing. VMware originated the phrase. VDI is divided into two approaches: persistent and nonpersistent. Persistent VDI gives each user his or her desktop image, which may be altered and stored for future use in the same way that a typical physical desktop can. Nonpersistent VDI creates a pool of consistent desktops that users can access as required. When a user logs out, nonpersistent desktops revert to their previous state.

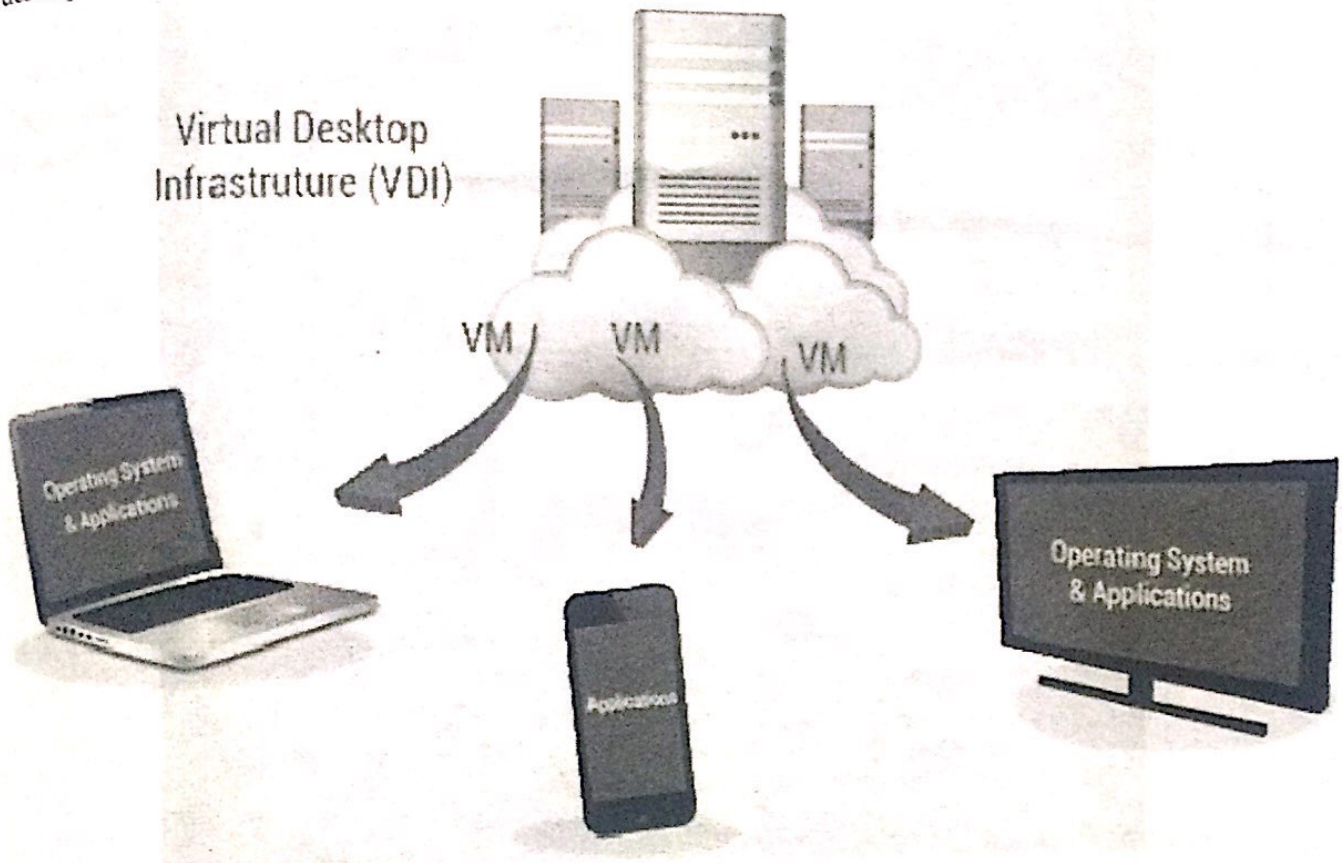


Figure 2.28 Virtual desktop infrastructure

Benefits

- Cost efficiency
- Instant backup capabilities
- Reduced lag time
- Added security features
- Simplified management
- Fewer compatibility issues

Best virtual desktop infrastructure applications

Amazon WorkSpaces, IBM Cloud, Cisco VXI, VMware Horizon Cloud, Red Hat Virtualization, Citrix Virtual Apps & Desktops, SolarWinds Virtualization Manager, etc.

CLOUD COMPUTING MANAGEMENT

The cloud provider should manage the resources and their performance. Resource management encompasses several areas of cloud computing, such as load balancing, performance, storage, backups, capacity, and deployment. Management is required to access the full capability of those cloud resources.

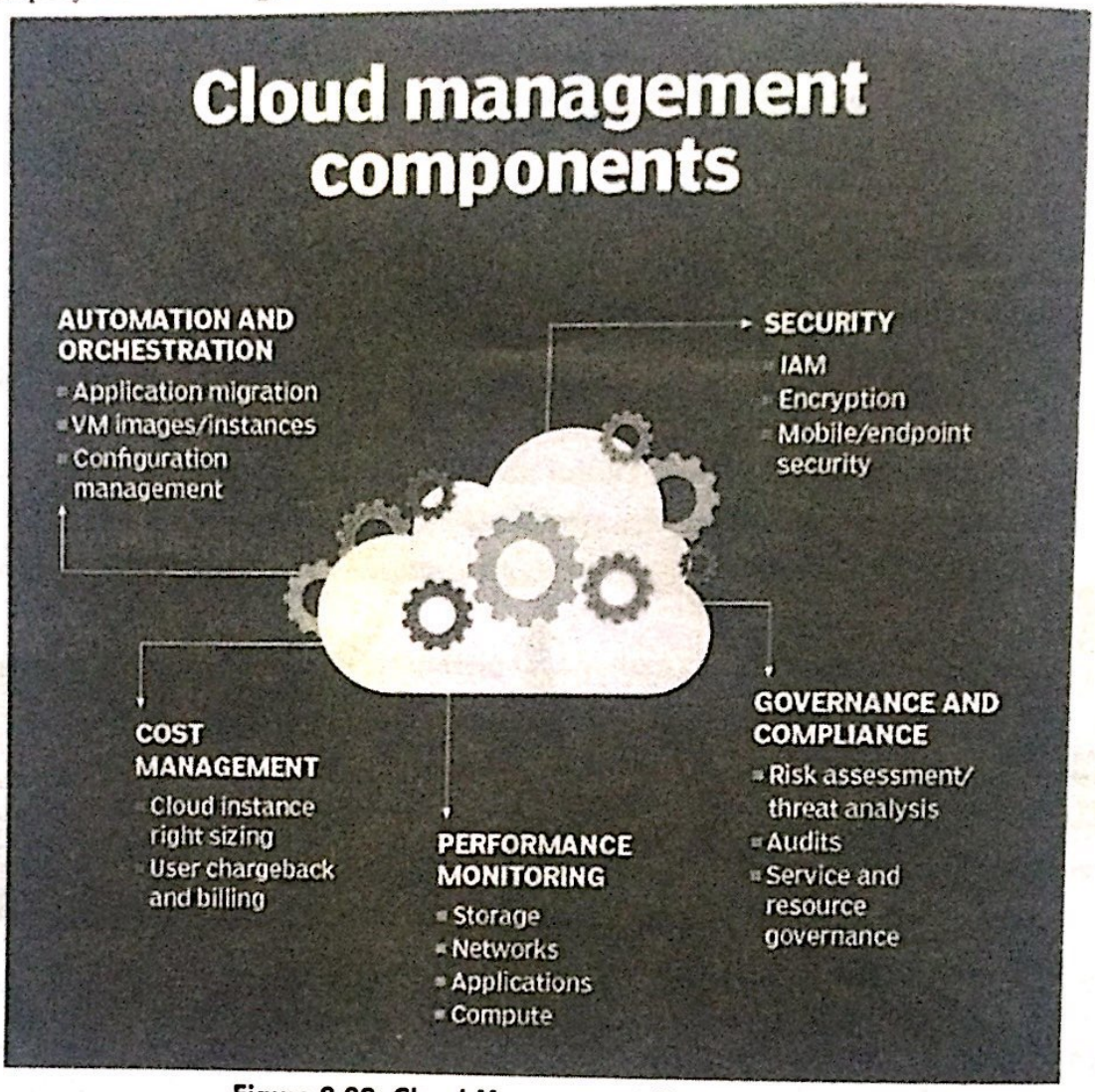


Figure 2.29: Cloud Management Components

Cloud management is the process of reviewing, monitoring, and optimizing cloud computing systems and services to achieve the desired efficiency, performance, and overall service quality. Cloud management is the practice of overseeing the cloud environment from start to finish by an organization, a cloud service vendor, or both. It guarantees that cloud computing services are supplied and operated in the most efficient manner possible.

The exercise of administrative control over public, private, and hybrid clouds is referred to as cloud management. Users may keep control over these dynamic and scalable cloud computing environments with a well-implemented cloud management approach.

RESILIENCY

The ability of a server, network, storage system, or an entire data center to recover rapidly and continue operations in the event of an equipment failure, power loss, or other disturbance is referred to as resilience. Resiliency is a deliberate component of a facility's design, and it is typically coupled with other disaster planning and data center disaster-recovery issues, such as data protection. The term robust implies "capable of bouncing back."

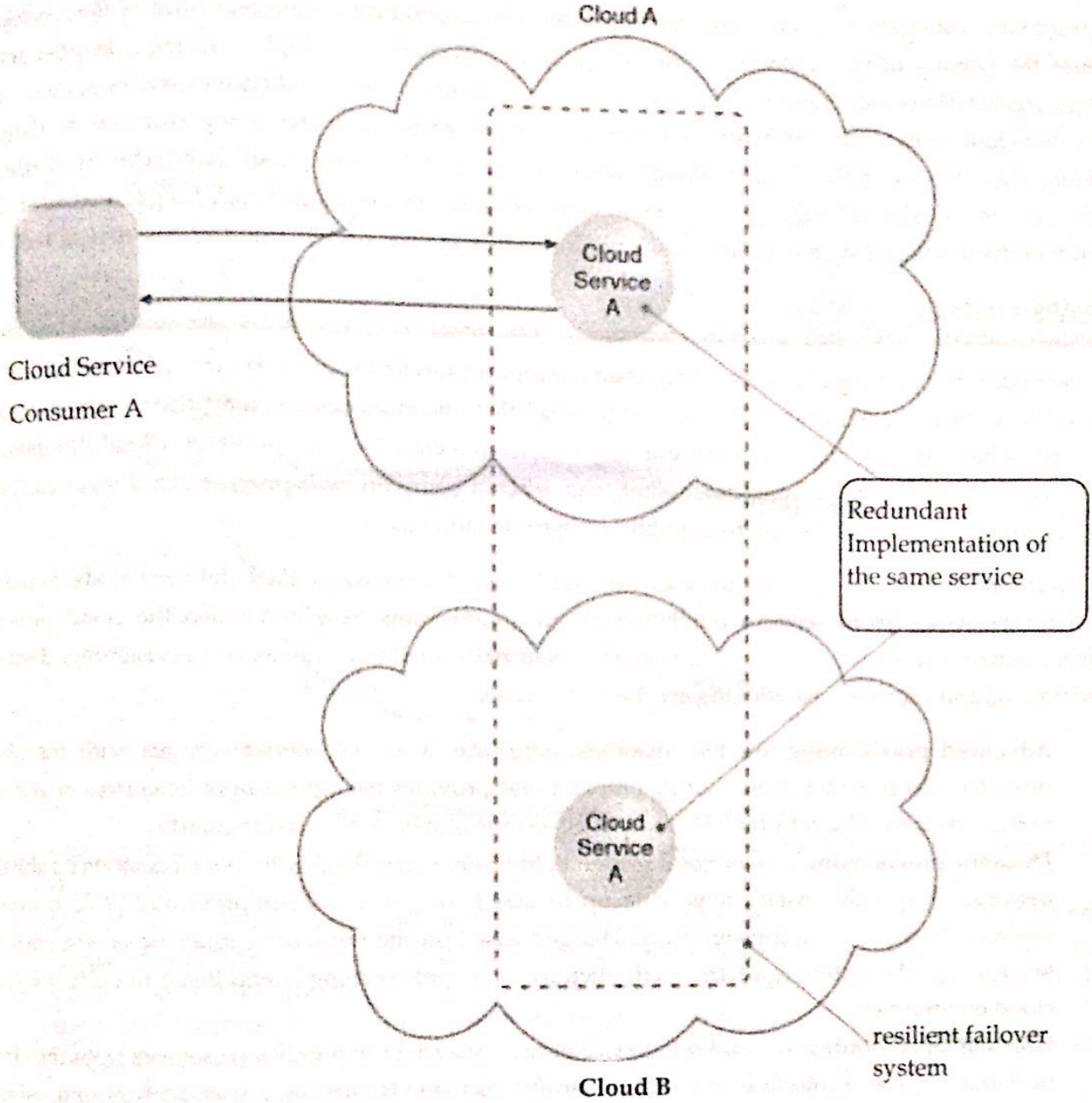


Figure 2.30 Demonstration of Resiliency

Resilient computing is a type of failover that spreads redundant IT resource implementations across physical locations. IT resources can be pre-configured such that if one fails, the processing is immediately transferred to a redundant implementation. The term "resiliency" in cloud computing can apply to redundant IT resources inside the same cloud (but in various physical locations) or across various clouds. By exploiting the resiliency of cloud-based IT resources, cloud customers may improve the dependability and availability of their applications.

Resiliency is frequently achieved by utilizing redundant components, subsystems, systems, or facilities. When one part fails or is disrupted, the redundant element easily takes over and continues to provide computing services to the user base. Users of a resilient system should never be aware that an interruption has occurred.

For example, if a standard server's power supply breaks, the server fails, and any workloads on that server become unavailable until the server is repaired and restarted. If the server has a redundant power supply, the backup power supply keeps the server operational until a technician can repair the failed power supply. Techniques like server clustering enable redundant workloads to run on many physical servers. When one of the cluster's servers dies, another node takes over with its redundant duties. The same idea holds for whole data center installations. For example, a company may power its data center with two independent utility feeds from different utility suppliers to have a backup supplier accessible if the first utility source fails.

The resilience strategies used in a data center might vary depending on the relevance of the workload. Because the penalty of not sustaining vital computing services is often higher during a lengthy service outage, organizations with mission-critical workloads will employ more resilience measures at more levels inside the data center. Critical business services, such as transaction processing software or database systems, may, for example, be constructed with extensive data center resiliency, such as clustering, snapshots, and off-site redundancy. Nonessential workloads, on the other hand, that can survive some amount of disturbance, may receive less resilience, or simply remain down until they can be restored.

PROVISIONING

The methods for deploying and integrating cloud computing services into a corporate IT infrastructure are referred to as cloud provisioning. This is a wide word that encompasses an enterprise's rules, processes, and goals when sourcing cloud services and solutions from a cloud service provider. Cloud provisioning is largely concerned with defining how, what, and when a company will provide cloud services. These services and solutions might be internal, public, or hybrid cloud based.

The cloud provisioning procedure can be carried out in one of three ways. Each delivery model is unique based on the resources or services purchased by an organization, how and when the cloud provider delivers those resources or services, and how the client pays for them. Advanced provisioning, dynamic provisioning, and user self-provisioning are the three models.

- **Advanced provisioning** lets the customers enter into a formal service contract with the cloud provider. The provider subsequently prepares and provides the agreed-upon resources or services to the consumer. The consumer is charged a one-time cost or is invoiced regularly.
- **Dynamic provisioning** allows cloud resources to be delivered flexibly to meet a customer's shifting demands. Typically, installations scale up to match surges in consumption and scale down as demand decreases. The consumer gets charged based on the number of times he or she uses the service. Cloud bursting is a term used when dynamic provisioning is employed to build a hybrid cloud environment.
- **User self-provisioning** or cloud self-service permits the client to purchase resources from the cloud provider via a web interface or portal. Typically, this entails creating a user account and using a credit card to pay for resources. These resources are then rapidly turned up and made accessible for usage, often within hours, if not minutes. An employee purchasing cloud-based productivity products like the Microsoft Office 365 suite or Google Apps for Business is an example of this sort of cloud provisioning.

Process Flow

Users who are members of virtual provisioning groups conduct cloud management duties. Members of the groups govern the whole process, from setup through provisioning and, finally, service catalog requests for virtual resources. Following diagram shows the process flow:

All required tasks within Cloud Management are performed by members of these groups:

- **Virtual Provisioning Cloud Administrator:** Cloud administrators are in charge of setting the virtualization providers utilized by Cloud Management and own the cloud provisioning environment. Using the Cloud Admin Portal, cloud administrators may create service catalog entries, authorize virtual machine requests, and monitor the Cloud Management environment.

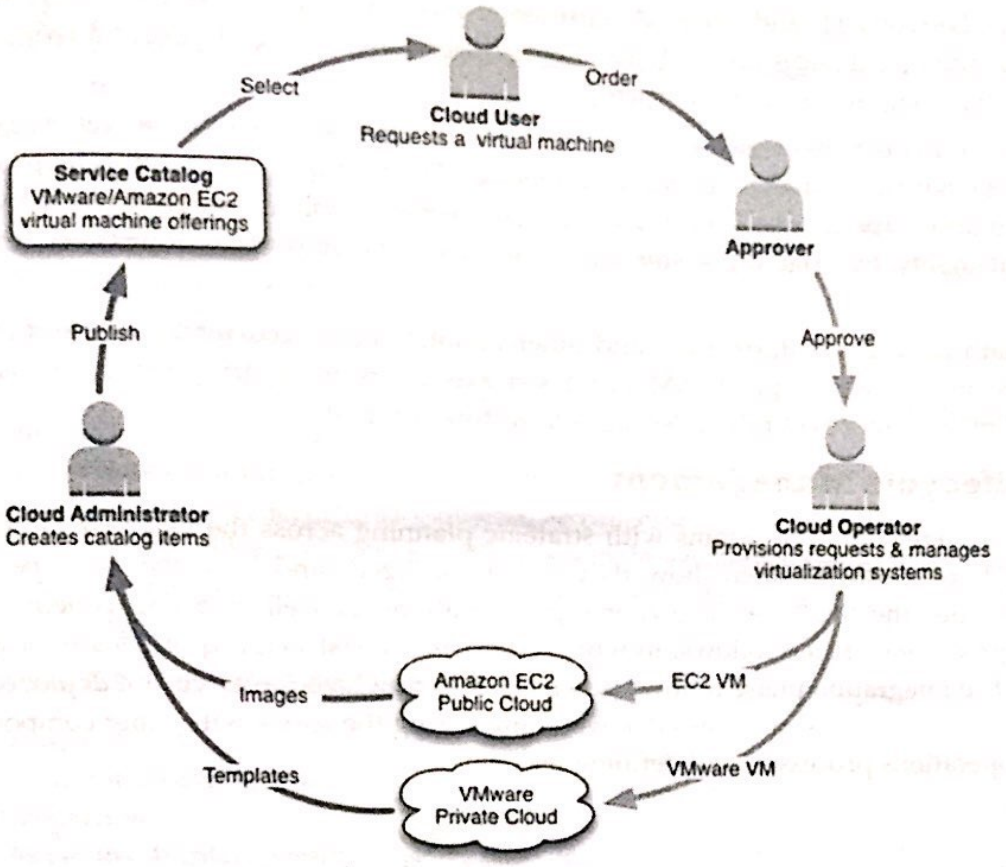


Figure 2.31 Process flow of cloud provisioning

- **Virtual Provisioning Cloud Approver:**Cloud Approvers have the authority to accept or reject requests for virtual resources. Approvers are not responsible for any technical aspects.
- **Virtual Provisioning Cloud Operator:**Users' provisioning requests are fulfilled by cloud operators. Cloud operators do activities that occur in the Cloud Operations Portal to complete the day-to-day job of Cloud Management. Cloud operators are allocated to certain Cloud Management Providers and must be technically knowledgeable about the providers they assist.
- **Virtual Provisioning Cloud User:**Cloud customers may request virtual machines from the service and manage any virtual machines assigned to them using the My Virtual Assets site.

ASSET MANAGEMENT

Information Technology Asset Management (ITAM) is a collection of business processes that integrates financial, inventory, and contractual operations to optimize expenditures and support lifecycle management and strategic decision-making inside the IT system. Any company-owned information, system, or hardware that is employed in the course of business activities is defined as an IT asset. The IT asset management process often entails compiling a complete inventory of an organization's hardware, software, and network assets and then using that data to make educated business choices regarding IT-related purchases and redistribution. It generally entails acquiring thorough hardware and software inventory information, which is then utilized to make hardware and software purchasing and redistribution choices. IT inventory management enables firms to manage their systems more efficiently while also saving time and money by avoiding needless asset acquisitions and making the greatest use of current resources.

ITAM is more than merely keeping track of assets. It is about constantly utilizing the acquired asset data to enhance returns, reduce risk, and produce greater company value. IT asset managers can reduce software license and maintenance costs, remove waste, and increase efficiency by avoiding needless asset acquisitions and making the greatest use of existing resources. ITAM also enhances communications and

understanding between IT and other departments, ensures compliance with cybersecurity rules a regulatory standards, enhances productivity through technological assistance, and reduces overhead co associated with managing the IT infrastructure.

Effective IT asset management increases visibility and control of IT assets, as well as quickly locate a replace missing hardware and software components. ITAM may help other ITIL processes by givi precise information about assets impacted by an event, problem, or change. ITAM also improv organizational agility by enabling faster and more accurate migrations, upgrades, and companywi changes.

In the aftermath of natural catastrophes and other unanticipated occurrences, IT asset and configurati data might be important. Proper ITAM can assist executives in swiftly identifying the effects of suc incidents and making more confident decisions to restore services.

It Asset Lifecycle Management

The IT asset management cycle begins with strategic planning across the business to decide what asse are required, how to obtain them, how they will be utilized, and how they will be supported. Thi frequently includes the total cost of ownership calculations as well as a cost-benefit analysis of othe options. The procurement step follows, in which companies construct, acquire, lease, or license the asse they require. The integration phase follows purchase, during which the assets are deployed and integrate into the IT environment. This involves effectively integrating the assets with other components, setting u support and operations processes, and defining user access.

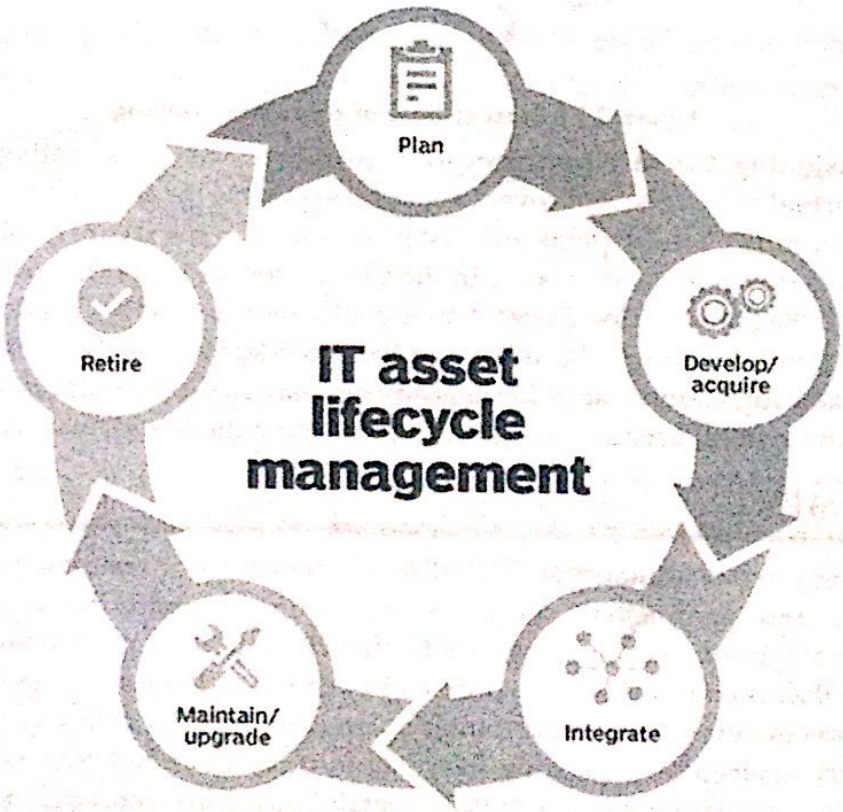


Figure 2.31 Lifecycle of IT Asset Management

The next stage of the IT asset lifecycle is asset maintenance and upgrade. Maintenance, repair, and major overhauls may be required to optimize the asset's value and prolong its life, as well as limit hazards and decrease support costs. The last phase is asset retirement and disposal when the asset has reached the end of its useful life. This frequently entails "transitioning users to alternative resources, updating asset records, canceling support agreements, ending license renewals, and commencing replacement asset planning."

CLOUD GOVERNANCE

Cloud governance refers to the decision-making processes, criteria, and rules that are involved in the design, architecture, purchase, deployment, operation, and administration of Cloud computing capacity. Simply said, Cloud Governance refers to the people, processes, and technology that are involved with your Cloud Infrastructure, Security, and Operations. The Cloud Governance Lifecycle defines the end-to-end requirements of Cloud Governance, from planning, architecture, and implementation through bursting, moving Cloud providers, and exiting a Cloud.

Reasons for Cloud Governance

- Enable *"Business at Cloud Speed"* and establish a Cloud-Centric IT operating model based on the speed, agility, and cost of Cloud computing.
- Enable appropriate Cloud decision-making without friction
- Integrated with existing Enterprise IT Governance processes, policies, boards, and tools
- Appropriate coverage for key decisions, investments, and risks while achieving the benefits of Clouds
- Proactive to anticipate and prevent Shadow Clouds and Unauthorized Cloud activities that expose organizational risks

Risks of Poor/No Cloud Governance

- Cloud Security Risks
- Cloud Proliferation and Sprawl
- Cloud Integration
- Cloud Portability & Interoperability
- Cloud Vendor Lock-In

CLOUD MANAGEMENT TASKS

Cloud management, as an IT service, comprises the majority of the underlying duties and methodologies from IT service management. It comprises responsibilities ranging from the most fundamental to the most complicated, such as ensuring resource availability, delivering fully working software/systems, and establishing standardized security controls and procedures. Some businesses now provide vendor-neutral cloud management software/services to help businesses successfully manage and run cloud services. Although the customer or end-user is also accountable for their share, cloud administration is generally a vendor-end process that covers any job that has an impact on the cloud environment, whether directly or indirectly. It is the cloud provider's responsibility to manage resources and their performance. The management of resources encompasses many areas of cloud computing, including load balancing, performance, storage, backups, capacity, deployment, and so on. Management is required to get the full capability of cloud resources. The cloud provider completes a variety of steps to ensure that cloud resources are being used efficiently. The following are some of the cloud management duties performed by cloud providers:

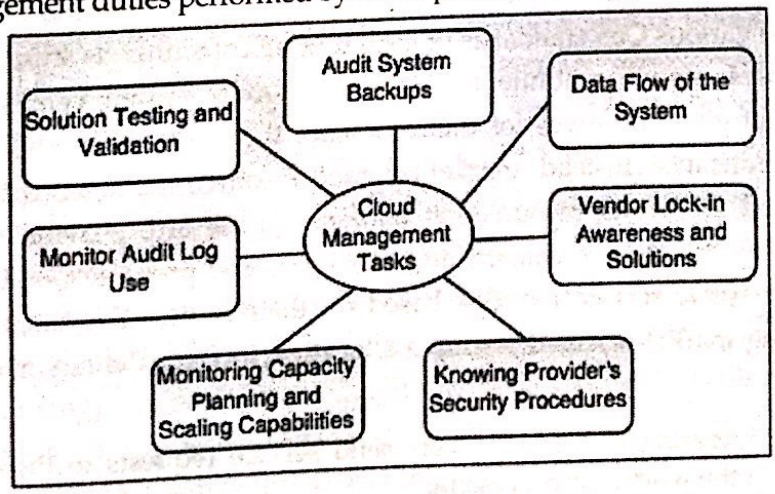


Figure 2.32: Cloud management duties performed by cloud providers

- **Audit System Backups:** It is necessary to check backups regularly to assure the restoration of randomly selected files from various users. Backups can be done in the following ways:
  - The corporation backs up files from on-site PCs to drives in the cloud.
  - The cloud provider backs up files.
  - It is vital to know whether the cloud provider has encrypted the data, who has access to that data, and if the backup is taken in many places, the user must be aware of the details of those places.
- **Data Flow of the System:** It is the managers' responsibility to create a diagram depicting a complete process flow. This process flow depicts the transportation of an organization's data throughout the cloud solution.
- **Vendor Lock-In Awareness and Solutions:** Managers must be aware of the method for terminating services from a certain cloud provider. Procedures must be created to allow cloud administrators to export data from an organization's system to another cloud provider.
- **Knowing Provider's Security Procedures:** Managers should be aware of the provider's security plans for the following services:
  - Multitenant use
  - E-commerce processing
  - Employee screening
  - Encryption policy
- **Monitoring Capacity Planning and Scaling Capabilities:** Managers must understand capacity planning to determine whether the cloud provider is matching his/her company's future capacity needs. Managers must manage scaling capabilities to guarantee that services can be scaled up or down as needed by users.
- **Monitor Audit Log Use:** Managers must regularly audit logs to discover faults in the system.
- **Solution Testing and Validation:** When a solution is offered by the cloud provider, it is important to test it so that it produces the right output and is error-free. This is required to make a system resilient and trustworthy.

MARKET-BASED MANAGEMENT OF CLOUDS

Market Oriented Cloud Computing (Mocc)

As customers rely on Cloud providers to cover all of their computing needs, they will expect certain QoS from their providers to fulfill their objectives and continue their operations. Cloud providers must examine and satisfy the various QoS standards of each unique consumer as stipulated in unique SLAs. To do this, cloud providers cannot continue to install traditional system-centric resource management architectures that do not give incentives for them to share their resources while still treating all service requests as equal insignificance. Instead, market-oriented resource management is required to maintain the supply and demand for Cloud resources at market equilibrium, provide feedback in the form of economic incentives for both Cloud consumers and providers, and promote QoS-based resource allocation mechanisms that differentiate service requests based on their utility. The diagram depicts a high-level architecture for enabling market-oriented resource allocation in Data Centers and Clouds.There are four main entities involved:

1. **Users/Brokers:** Operating Users or brokers send service requests to the Data Center and Cloud from anywhere in the world for processing.

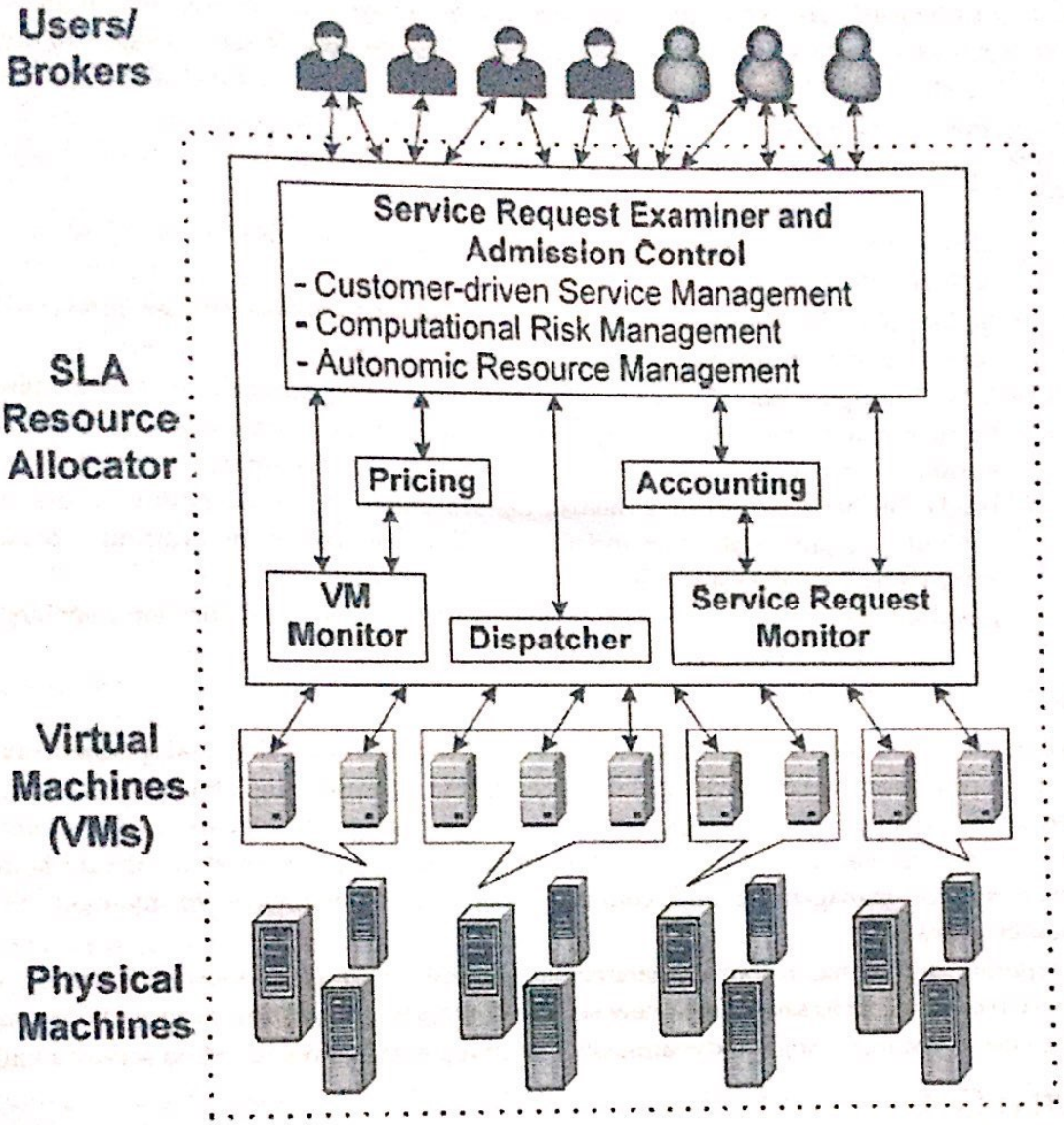


Figure 2.33: Architecture of Market Based Management of Clouds

2 **SLA Resource Allocator:**The SLA Resource Allocator serves as a liaison between the Data Center/Cloud service provider and external users/brokers. To support SLA-oriented resource management, the following systems must interact:

- *Service Request Examiner and Admission Control*: When a service request is initially made, the Service Request Examiner and Admission Control mechanism evaluates the supplied request for QoS criteria before deciding whether to accept or refuse the request. As a result, it prevents resource overload, in which numerous service requests are unable to be delivered properly due to a lack of available resources. It also requires up-to-date status information on resource availability from the VM Monitor and workload processing from the Service Request Monitor to make appropriate resource allocation choices.It then distributes requests to VMs and determines resource entitlements for assigned VMs.
- *Pricing*: The Pricing mechanism determines how service requests are billed. Requests, for example, might be charged depending on submission time (peak/off-peak), price rates (fixed/changing), or resource availability (supply/demand). Pricing serves as a foundation for regulating the supply and demand for computing resources inside the Data Center and aids in the proper prioritization of resource allocations.

- *Accounting*: The Accounting mechanism keeps track of the real utilization of resources by requests so that the ultimate cost may be calculated and charged to the consumer. Furthermore, the Service Request Examiner and Admission Control mechanism may use the stored previous usage data to optimize resource allocation choices.
- *VM Monitor*: The VM Monitor mechanism monitors the availability of VMs as well as their resource entitlements.
- **Dispatcher**: The Dispatcher mechanism begins executing accepted service requests on assigned VMs.
- *Service Request Monitor*: The Service Request Monitor mechanism monitors the status of service requests as they are being executed.
- **VMs:** Multiple VMs may be started and terminated dynamically on a single physical system to satisfy accepted service requests, enabling maximum flexibility to design multiple partitions of resources on the same physical system to match particular service request needs. Furthermore, because each VM is separated from one another on the same physical computer, many VMs can execute applications based on various operating system environments on the same physical computer at the same time.
- **Physical Machines**: The Data Center is made up of several computer servers that supply resources to satisfy service demands.

Commercial offerings of MOCC must be able to:

- assist with customer-driven service management based on customer profiles and specified service criteria
- establish computational risk management techniques for identifying, assessing, and managing risks associated with application execution in terms of service requirements and customer demands
- develop appropriate market-based resource management strategies that include both customer-driven service management and computational risk management to maintain SLA-oriented resource allocation
- incorporate autonomic resource management models that effectively self-manage changes in service requirements to satisfy both new service demands and existing service obligations.
- make use of VM technology to dynamically assign resource shares based on service requirements.

FEDERATED CLOUDS/INTERCLOUD

The terms cloud federation and InterCloud, which are sometimes used interchangeably, refer to an aggregation of cloud computing providers with independent administrative domains. It is critical to understand what these two phrases signify and how they relate to cloud computing. The term "federation" refers to the formation of an organization that transcends the decisional and administrative authority of individual organizations and functions as a whole. Within the context of cloud computing, the term federation does not have such a strong meaning, but it does imply that there exist agreements between the various cloud providers that allow them to exploit each other's services in a privileged manner.

> Cloud federation provides consistency and access restrictions when two or more geographically separate independent Cloud exchange authentication, files, computing resources, command, and control, or access to storage resources.

InterCloud is a phrase that is frequently used interchangeably to represent the notion of Cloud federation. Cisco introduced it to define a composition of clouds that are integrated using open standards to create a universal environment that uses cloud computing services. As the Internet is often referred to as the "network of networks," InterCloud represents a "Cloud of Clouds" and expresses the same concept of federating together clouds that belong to various administrative organizations.

InterCloud is a worldwide concept in which interoperability across different cloud providers is defined by standards, resulting in an open platform where applications can move workloads and freely build services from many sources. A cloud federation, on the other hand, is a broader term that covers ad hoc aggregations of cloud providers based on private agreements and proprietary interfaces.

The key distinction between the InterCloud and federation is that the InterCloud is built on future standards and open interfaces, whereas the federation employs a vendor-specific control plane. All Clouds will have a similar concept of how applications should be delivered under InterCloud. Workloads sent to a Cloud will eventually include enough of a definition (resources, security, service level, geo-location, etc.) for the Cloud to execute the request and install the application. This will result in a pure utility model, where the specification meets all of the requirements, and the application may run "as is" on any Cloud with the resources to serve it."

CLOUD FEDERATION STACK

The creation of a cloud federation needs research and development at several levels, including conceptual, logical, and operational, as well as infrastructure. The figure below depicts the obstacles encountered in creating and executing an organizational structure that coordinates cloud services from multiple administrative domains and allows them to function within the framework of a single unified service middleware. Each level of cloud federation brings unique issues and works at a different layer of the IT stack. It thus necessitates the application of various methodologies and technology.When the answers to the issues faced at each of these levels are combined, they provide a reference model for a cloud federation.

The **CONCEPTUAL LEVEL** tackles the difficulties in presenting a cloud federation as a beneficial option for the usage of services leased by a single cloud provider. At this stage, it is critical to highlight the benefits of joining a federation for either service providers or service customers, as well as the additional opportunities that a federated environment brings in comparison to a single-provider solution. The conceptual level tackles the difficulties in presenting a cloud federation as a beneficial alternative for using services leased by a single cloud provider.

At this stage, it is critical to highlight the benefits of joining a federation for either service providers or service customers, as well as the additional opportunities that a federated environment brings in comparison to a single-provider solution. Elements of concern at this level are:

- Motivations for cloud providers to join a federation
- Motivations for service consumers to leverage a federation
- Advantages for providers in leasing their services to other providers
- Obligations of providers once they have joined the federation
- Trust agreements between providers
- Transparency versus consumers

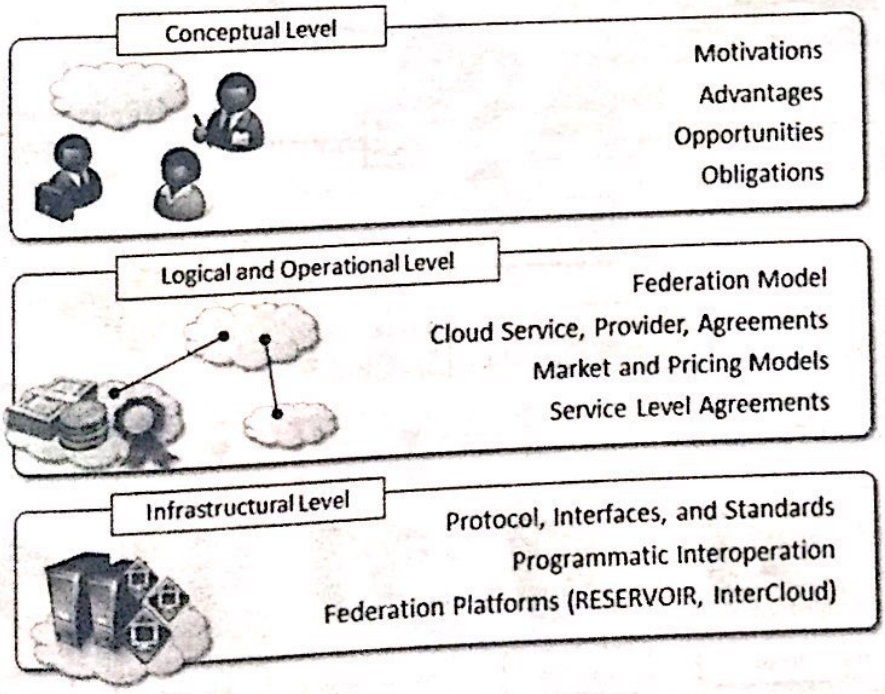


Figure 2.34: Cloud federation reference stack.

The **LOGICAL AND OPERATIONAL LEVEL** of a federated cloud identifies and resolves the issues designing a framework that enables the aggregation of providers from various administrative domains within the context of a single overlay infrastructure, which is the cloud federation. Policies and guidelines for interoperability are specified at this level. Furthermore, this is the layer at which decisions are made about how and when to lease service to—or leverage a service from—another provider. The logical component sets the setting in which agreements among providers are established and services are negotiated, whereas the operational component describes and forms the federation's dynamic behavior as a result of the single providers' choices. This is the stage at which MOCC is put into action and achieved. The **INFRASTRUCTURAL LEVEL** covers the technological problems involved in enabling diverse cloud computing platforms to easily interoperate. It addresses the technological constraints that prevent independent cloud computing systems from belonging to distinct administrative domains. These restrictions can be eliminated by using standardized protocols and interfaces. In other words, this level is for the federation what the TCP/IP stack is for the Internet. The IaaS and PaaS layers of the Cloud Computing Reference Model serve as the foundation for the infrastructure level. Interoperation and interface services may also be implemented at the SaaS level, particularly for the realization of agreements and federated clouds.

THIRD-PARTY CLOUD SERVICES

One of the most important aspects of cloud computing is the ability to combine services from multiple suppliers or integrate with existing software systems. The service-oriented model, which is the foundation of cloud computing, promotes such an approach and allows for the development of a new class of services known as third-party cloud services. These are the results of adding value to pre-existing cloud computing services, therefore offering clients a more unique and complex solution. Added value may be provided by intelligently coordinating existing services or by integrating new features on top of an existing core service. Aside from this broad description, there is no distinguishing attribute of this type of service. Examples of third-party cloud services are explained below:

METACDN

MetaCDN delivers a Content Delivery Network (CDN) service to consumers by using and exploiting heterogeneous storage clouds.

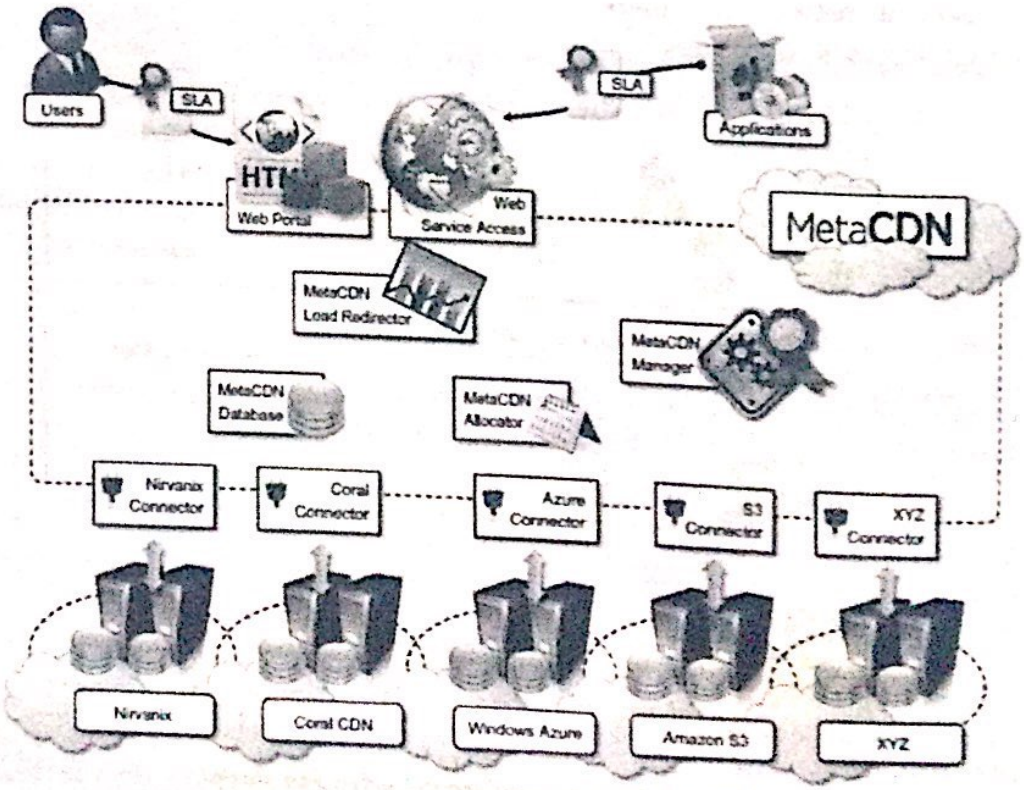


Figure 2.35: Architecture of CDN

MetaCDN employs mass distributed elastic storage to store user material and employs a software overlay that coordinates the service offers of several cloud storage companies. MetaCDN offers consumers the high-level services of a CDN for content distribution and interacts with the low-level interfaces of storage clouds to efficiently position user content based on the predicted geography of its demand. By utilizing the cloud as a storage backend, small businesses may now access a complex—and typically expensive—content delivery service.

SPOTCLOUD

SpotCloud is not only an enabler for IaaS providers and resellers, but it also serves as a mediator for all transactions linked with the utilization of resources. Users fund their SpotCloud accounts with credit, while capacity sellers are compensated using the standard pay-per-use mechanism. SpotCloud keeps a portion of the money charged to the user. Furthermore, employing a consistent runtime environment and virtual machine management layer offers customers a vendor-agnostic solution that may be important for particular applications.

The two previously mentioned examples demonstrate how diverse third-party services may be: MetaCDN offers a different service to end-users than simple cloud storage options; SpotCloud does not modify the sort of service that is ultimately delivered to end-users, but it enriches it with extra capabilities that result in more effective usage. These are only two instances of the market sector that is currently emerging as a result of the consolidation of cloud computing as a means of making better use of IT resources.

PROTECTION AGAINST INTERNAL AND EXTERNAL THREATS

By continually evaluating logs and warnings from infrastructure devices around the clock and in real-time, SOC-based security monitoring services may increase the performance of a client security infrastructure. Monitoring teams combine data from numerous security devices to give security analysts the knowledge they need to remove false positives and respond to genuine risks to the company. Consistent access to the skills required to sustain the quality of service required by an organization for enterprise-level monitoring is a major concern. The information security team can evaluate system performance regularly and make recommendations for enhancements as needed.

The following are typical services offered by several MaaS vendors:

1. **Early Detection:** An early detection service finds and discloses new security vulnerabilities as soon as they are discovered. In general, dangers are associated with third-party sources, and consumers are provided an alert or report. This report is typically emailed to the company's authorized recipient. Aside from a full explanation of the vulnerability and the platforms impacted, security vulnerability reports also provide information on the impact of exploiting this vulnerability on the systems or applications previously specified by the firm receiving the report. Most of the time, the report also specifies specific measures to be done to mitigate the impact of the vulnerability, if it is recognized.
2. **Platform, Control, and Services Monitoring:** Platform, control, and service monitoring are frequently implemented as a dashboard interface, allowing you to know the operating state of the platform being watched at all times. It is accessible through a web interface, allowing for remote access. Each operational element that is monitored typically produces an operational status indication, always taking the crucial impact of each element into mind. This service assists in determining which elements may be functioning at or near capacity or beyond the parameters that have been defined. By recognizing and recognizing such issues, preventive steps may be implemented to avoid service disruption.

3. **Intelligent Log Centralization and Analysis:** Intelligent log centralization and analysis is monitoring system that relies heavily on log entry correlation and matching. This type of study a in the establishment of a baseline of operational performance and gives a security threat inde Alarms can be triggered if an occurrence exceeds the predefined baseline parameters by more th a certain amount. Once such a threshold has been crossed and the danger has created an alarm warning picked up by security analysts monitoring the systems, these advanced tools are deploye by a team of security specialists who are responsible for incident response.
4. **Vulnerabilities Detection and Management:** Vulnerability detection and management offer automated verification and administration of information system security levels. The service runs series of automated tests regularly to identify system weaknesses that may be exposed over th Internet, such as the possibility of unauthorized access to administrative services, the existence o not updated services, the detection of vulnerabilities such as phishing, and so on. The service delivers reports that may be used to build a strategy for continuous development of the system security level and perform periodic follow-up on duties completed by security experts managing information system security.
5. **Continuous System Patching/Upgrade and Fortification:** Continuous system patching and upgrade of systems and application software improve security posture. To maintain sufficient security levels and support new versions of installed products, fresh patches, upgrades, and service packs for the equipment's operating system are required. Keeping up with all of the changes to all of the software and hardware necessitates a concerted effort to keep aware and explain security flaws that may develop in installed systems and applications.
6. **Intervention, Forensics, and Help Desk Services:** When a threat is recognized, a quick response is critical for reducing its impacts. This necessitates security experts with an extensive understanding of numerous technologies and the capacity to support applications and infrastructures 24 hours a day, seven days a week. Customers of MaaS platforms are frequently provided with this service. When an identified threat is investigated, forensic analysis is frequently required to establish what it is, how much work will be required to fix the problem, and what repercussions are likely to be noticed. When difficulties arise, customers' first instinct is to dial a phone number. Help desk services give answers to concerns or problems about the functioning of operational systems. This service includes support with creating failure reports, addressing operational issues, and so forth.

JERICHO CLOUD CUBE MODEL

The Cloud Cube model helps classify a four-dimensional factor cloud network. Its concentration is on protecting and safeguarding the cloud network. This cloud cube model lets you securely pick cloud formation. This model serves to provide a safe and secured Internet network for IT administrators, enterprises, and business leaders.

Jericho Forum is an international independent group of information security leaders & their focus is on how to protect and secure cloud networks. They put forward a model that helps to categorize a cloud network based on four-dimensional factors. The Jericho Cloud Cube Model describes the multidimensional elements of cloud computing, framing not only cloud use cases, but also how they are deployed and used.

The Cloud Cube Model, established and developed by the Jericho Forum, assists in categorizing cloud networks based on four dimensions:

- Internal/External
- Proprietary/Open
- Perimeterised/De-perimeterized
- Insourced/Outsourced

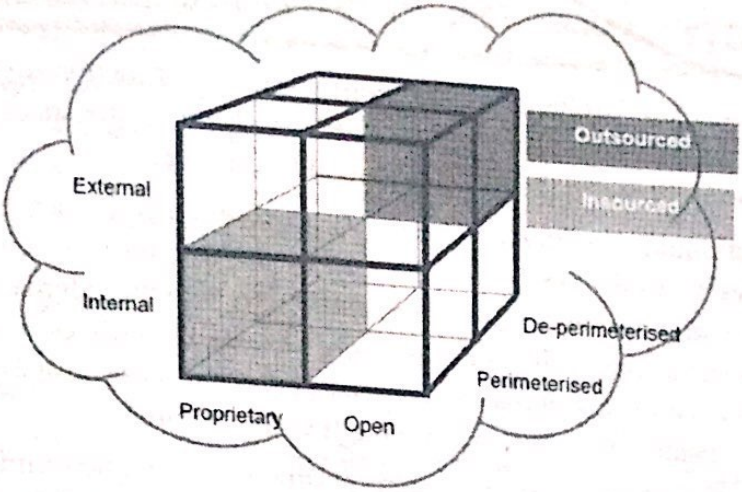


Figure 2.36: Jericho Cloud Cube Model

Four-Dimensional of the model:

1. **Physical Location of Data:** Data can be stored inside or outside, which ultimately establishes the organization's boundaries.
2. **Ownership:** Ownership can be proprietary or open; it not just measures the ownership of technology but also its interoperability, data use, and ease of data transfer, as well as the degree of vendor application lock-in.
3. **Security Range:** The range can be perimeterized or de-perimeterized; which determines whether actions take place within or outside of the security border, firewall, etc.
4. **Sourcing:** Services can be in-sourced or out-sourced and that refers to whether the service is provided by the client or the service provider.

Dimension: Physical Location - Internal or External

The internal and external cloud forms are the most fundamental cloud types. The physical placement of the data is defined by the internal and external dimensions. It recognizes if the data lives within or outside of your organization's boundaries. If it is within your physical border, it is Internal; if it is outside of your physical border, it is External. In this case, data kept in a private cloud deployment is deemed internal, whereas data kept outside the private cloud is deemed external. It is critical to stress that the idea that the internal is always more secure than the exterior is incorrect. The most secure usage model makes use of both internal and external cloud types.

For example, virtualized hard drives in a company's data center are internal, whereas Amazon SC3 is external.

Dimension: Ownership - Proprietary or Open

This is the dimension that specifies the 'ownership' of cloud technologies, services, interfaces, and so on. It denotes the degree of interoperability, as well as permitting "data/application transportability" between your systems and other cloud forms, as well as the freedom to withdraw or upload data from or to a cloud. It also highlights any limitations on the ability to distribute apps.

Proprietary indicates that the entity delivering the service retains control of the means of provision. As a result, when operating in proprietary clouds, you may be unable to switch to another cloud provider without substantial work or expenditure. The most inventive technological developments are frequently made in the proprietary sector. As a result, the proprietor may choose to impose limitations through patents and by making the underlying technology a trade secret.

Open clouds use non-proprietary technology, which means that there are more suppliers, and you are not as limited in your ability to exchange data and interact with chosen parties utilizing the same open technology. Open services are widely used and have a documented open standard. An untested notion is that the clouds that best facilitate cooperation among many enterprises will be Open.

DIMENSION: SECURITY RANGE - PERIMETERISED OR DE-PERIMETERISED

The third dimension indicates the "architectural mentality" - are you functioning within or outside of your typical IT perimeter? De-perimeterisation has always been associated with the progressive failure/removal/shrinkage/collapse of the old silo-based IT perimeter.

Perimeterisation entails continuing to function inside the conventional IT perimeter, which is frequently signified by "network firewalls." Collaboration is hampered by this approach. When working in perimeterised regions, you may easily extend your own organization's perimeter into the external cloud computing domain via a VPN and running the virtual server in your IP domain, utilizing your directory services to regulate access. When the computation process is over, you may return your perimeter to its original conventional location. This sort of system perimeter is considered a traditional, although virtual, perimeter.

The term "de-perimeterised" indicates that the system perimeter is designed under the concepts specified in the Jericho Forum's Commandments and Collaboration Oriented Architectures Framework. The Cloud Cube Model's de-perimeterised spaces utilize both internal and exterior domains, although data cooperation and sharing should not be considered internal or external. Rather, it is regulated and limited to the parties chosen by the organizations that use it.

DIMENSION: SOURCING - INSOURCED OR OUTSOURCED

This dimension answers the question, "Who do you want to operate your clouds?"

- **Insourced**: the service is performed by your employees under your supervision.
- **Outsourced**: a third party provides the service.

These two states indicate who is in charge of delivering the cloud service(s) you utilize. This is essentially a policy problem (i.e., a business choice, not a technical or architectural choice) that must be incorporated into a contract with the cloud provider.

It is vital to remember that few firms that have traditionally provided bandwidth, software, or hardware will be able to move seamlessly to become cloud service providers. Organizations seeking cloud services must acquire the capacity to quickly establish legally enforceable cooperation agreements and dissolve them just as quickly once they are no longer required. To reduce the danger of a data breach or leak, while ending a contract with a provider, an organization should verify that the data is properly erased from the service provider's infrastructure (including backups).

OBJECTIVE QUESTIONS

1) Point out the correct statement.

a. Cloud architecture can couple software running on virtualized hardware in multiple locations to provide an on-demand service
b. Cloud computing relies on a set of protocols needed to manage inter-process communications
c. Platforms are used to create more complex software
d. All of the mentioned

2) Which of the following is the property of the composable component?

a. stateful b. stateless c. symmetric d. all of the mentioned

3) From the standpoint of a _____ it makes no sense to offer non-standard machine instances to customers.

a. CaaS b. AaaS c. PaaS d. IaaS

4) Which of the following is the highest degree of integration in cloud computing?

a. CaaS b. AaaS c. PaaS d. SaaS

5) **Which of the architectural layers is used as a front end in cloud computing?**
a. client b. cloud c. soft d. all of the mentioned

6) **Which of the following is true about cloud computing?**
a. Cloud computing is platform dependent
b. Cloud Computing makes our business applications mobile and collaborative.
c. Cloud Computing provides us with means of accessing the applications as utilities over computers only.
d. all of the above

7) **Which of the following is the working model for cloud computing?**
a. Deployment Models b. Configuring Model
c. Collaborative Model d. All of the above

8) **The _____ allows systems and services to be accessible by a group of organizations.**
a. Private cloud b. Public cloud
c. Community cloud d. Hybrid cloud

9) **Which of the following is a type of Service Model?**
a. Public-as-a-Service b. Platform-as-a-Service
c. Community-as-a-Service d. Public-as-a-Service

10) **_____ provides the runtime environment for applications, development, and deployment tools, etc.**
a. IaaS b. PaaS c. SaaS d. XaaS

11) **Which cloud is deployed when there is a budget constraint, but business autonomy is most essential?**
a. private cloud b. public cloud
c. hybrid cloud d. community cloud

12) **IaaS offers non-standard machines to customers.**
a. True b. False
c. It depends upon the use d. None of the above

13) **Point out the wrong statement:**
a. Due to the vast number of users in the public cloud SLA cannot be strictly followed
c. A community cloud may be managed by the constituent organization(s) or by a third party
c. Private clouds may be either on- or off-premises.
c. None of the above

14) **SaaS supports multiple users and provides a shared data model through the.....model.**
a. single tenancy b. multi-tenancy
c. multiple instances d. All of the above.

15) **..... refers to the location and management of the cloud's infrastructure.**
a. Service b. Deployment
c. Application d. None of the above

16) **Which is not an advantage of Grid?**
a. Scalable b. Uses unused computing power
c. Provide standard and high CPU d. Multi-tenancy

17) **..... enables batch processing, which greatly speeds up high-processing applications.**
a. Scalability b. Reliability
c. Elasticity d. Utility

18) **What is the biggest disadvantage of the community model?**
a. Collaboration has to be maintained with other participants
b. Fewer security features
c. Cloud is used by many organizations for different purposes
d. Organization losses business autonomy

19) **Which of the following is owned by an organization selling cloud services?**
a. Public b. Private c. Community d. Hybrid

20) Point out the wrong statement:

a. Except for tightly managed SaaS cloud providers, the burden of resource management is still in hands of the user

b. Cloud computing vendors run highly reliable networks

c. All cloud computing applications combine their resources into pools that can be assigned on demand to use

d. None of the above

21) You cannot count on a cloud provider maintaining ..... in the face of government actions.

a. Scalability b. Reliability

c. Privacy d. None of the above.

22) All cloud computing applications suffer from the inherent ..... that is intrinsic in their WAN connectivi

a. Propagation b. Latency c. Noise d. None of the above

23) Which of the following is the specified parameter of SLA?

a. Response times b. Responsibilities of each party

c. Warranties d. All of the above

24) Which of the following is used to define the service component that performs the service?

a. WSDL b. SCDL

c. XML d. None of the mentioned

25) A service provider reselling an ____ may have the option to offer one module to customize the information

a. CaaS b. AaaS c. PaaS d. SaaS

26) _____ allows different operating systems to run in their own memory space.

a. VMM b. VMC c. VMM d. All of the mentioned

27) Which of the following is a classic example of an IaaS service model?

a. AWS b. Azure d. Cloudera d. All of the mentioned

28) Which of the following describes a message-passing taxonomy for a component-based architecture that provides services to clients upon demand?

a SOA b. EBS c. GEC d. All of the above

29) Point out the correct statement:

a. Service-Oriented Architecture (SOA) describes a standard method for requesting services from distributed components and managing the results

b. SOA provides the translation and management layer in an architecture that removes the barrier for a client obtaining desired services

c. With SOA, clients, and components can be written in different languages and can use multiple messaging protocols

d. All of the mentioned

30) Which of the following is a repeatable task within a business process?

a. service b. bus c. methods d. all of the mentioned

31) Point out the wrong statement.

a. SOA provides the standards that transport the messages and makes the infrastructure to support them possible

b. SOA provides access to reusable Web services over an SMTP network

c. SOA offers access to ready-made, modular, highly optimized, and widely shareable components that can minimize developer and infrastructure costs

d. None of the mentioned

32) Which action should they take first?

a. Create a service registry.

b. Define an SOA governance model.

c. Perform an SOA maturity assessment

d. Create an SOA Center of Excellence (CoE).

33) Services can be referred to as _____ because of the enterprise-centric design considerations of service-orientation and SOA.
   a. enterprise architectures
   b. enterprise resources
   c. enterprise definitions
   d. enterprise-centric business models

34) Which of the following is the most important feature of cloud storage listed below?
   a. Login authentication
   b. Bare file
   c. Multiplatform support
   d. Adequate bandwidth

35) When is an SOA implementation most appropriate?
   a. Real-time performance is critical.
   b. An immediate Return on Investment (ROI) is required.
   c. The application interfaces require a high degree of customization.
   c. Business functionality is required by many parts of the organization

QUESTION

1. Define cloud computing. Explain different entities that are depicted in a cloud computing reference model.
2. What does Infrastructure-as-a-Service refer to? Explain.
3. Which are the basic components of an IaaS-based solution for cloud computing? Provide some examples of IaaS implementations.
4. What are the main characteristics of a Platform-as-a-Service solution?
5. Describe the different categories of options available in a PaaS market.
6. What does the acronym SaaS mean? How does it relate to cloud computing?
7. Give the name of some popular Software-as-a-Service solutions.
8. Classify the various types of clouds. Give an example of the public cloud.
9. Which is the most common scenario for a private cloud?
10. What kinds of needs are addressed by heterogeneous clouds?
11. Describe the fundamental features of the economic and business model behind cloud computing.
12. How does cloud computing help to reduce the time to market for applications and to cut down capital expenses?
13. List some of the challenges in cloud computing.
14. Describe the cloud reference model.
15. Explain the architecture of Cloud computing in detail.
16. What resources are provided by infrastructure as a service? Describe.
17. How important is the platform as a service for the developers? Explain.
18. What does software as a service provider do? Explain its importance for general users.
19. What is the difference between traditional data centers and the cloud?
20. How are cloud services measured? Explain.
21. Explain the working principle of Cloud Computing.
22. Explain the term 'server consolidation'.
23. Explain public, private, hybrid, and community cloud.
24. How does cloud computing provide on-demand functionality?
25. What is the difference between scalability and elasticity? Describe.
26. What are the different components required by cloud architecture?
27. What does private cloud offer in building an infrastructure?
28. What are the basic characteristics of cloud computing?
29. What are the advantages of cloud services?
30. Explain the technologies on which cloud computing relies?
31. What are the fundamental components introduced in the cloud reference model?

32. What does the acronym XaaS stand for?
33. What does Infrastructure-as-a-Service refer to?
34. Which are the basic components of an IaaS-based solution for cloud computing?
35. Provide some examples of IaaS implementations.
36. What are the main characteristics of a Platform-as-a-Service solution?
37. Describe the different categories of options available in a PaaS market.
38. What does the acronym SaaS mean? How does it relate to cloud computing?
39. Give the name of some popular Software-as-a-Service solutions.
40. Classify the various types of clouds. Explain.
41. Explain the most common scenario for a private cloud.
42. What kinds of needs are addressed by heterogeneous clouds?
43. Describe the fundamental features of the economic and business model behind cloud computing.
44. How does cloud computing help to reduce the time to market for applications and to cut down capital expenses?
45. What are Web desktops? What is their relationship to cloud computing?
46. Describe market-oriented cloud computing, cloud federation, and InterCloud.
47. Define cloud computing. Explain different entities that are depicted in a cloud computing reference model.
48. Briefly discuss various issues in the interoperability of cloud resources.
49. Clarify in brief, how the cloud helps reduce capital expenditure? Explain the cloud services provided by Amazon infrastructure from the perspective of a developer.
50. What is the cloud cube model? Explain in context to the Jericho cloud cube model along with its various dimensions.
51. "With cloud computing, individuals and small businesses can snap their fingers and instantly set up enterprise-class services." Justify the statement.
52. Clarify in brief, how the cloud helps reduce capital expenditure? Explain the cloud services provided by Google infrastructure from a perspective of a user.
53. List the characteristics of cloud computing as per NIST. Explain the reference model of cloud computing.
54. "Line-of-business leaders everywhere are bypassing IT departments but still using enterprise-class services." Explain how this became possible.
55. Describe the services models of the cloud with examples.
56. Describe distributed computing and cloud computing. Explain the characteristics of cloud computing as per NIST.
57. Explain the reference architecture of cloud computing along with the interacting mechanism of involved components.
58. Describe Monitoring-as-a-Service. Briefly explain the components of the Jericho Cube Model along with the proper figure.
59. Explain various cloud service models. Clarify in brief, how the cloud helps reduce capital expenditure in context to the cloud services provided by Microsoft.
60. How Identity-as-a-Service (IDaaS) acts as an effective way of providing authentication to cloud services. Explain Single Sign-On (SSO) and Federated Identity Management (FIDM).
61. What is a cloud federation? Explain its importance.
62. Explain InterCloud and Cloud Federation?
63. What are the differences between InterCoud and Cloud Federation?
64. Describe a federated cloud along with its characterization. Explain cloud federation stack.
65. Briefly discuss various issues in the interoperability of cloud resources.
66. Clarify in brief, how the cloud helps reduce capital expenditure? Explain the cloud services provided by Amazon infrastructure from the perspective of a developer.
67. What is the cloud cube model? Explain in context to the Jericho cloud cube model along with its various dimensions.
68. Explain market-Oriented Cloud computing architecture.
69. **Write short notes:**
    a. Cloud business process management
    b. Single Sign-On (SSO) and Federated Identity Management (FIDM)
    c. Network-as-a-Service((NaaS) and Communication-as-a-Service (CaaS)

Explain: a. MOCC
b. Cycle-scavenging
c. Performers in cloud computing
d. Hybrid cloud

□□□