New Scheme previous year Question Paper -2023

Printed Pages – 3

Roll No. ....

CS100645

B.Tech.(Sixth Semester) Examination,

Apr-May 2023

(Computer Science & Engineering)

[CSE, CSE (AI), CSE (AIML), CSE (DS), CSE (IOT), CSE (IOT&CSBCT), CSE (BDA), CSE (GT)]

CLOUD COMPUTING

Time Allowed: 3 hours

Maximum Marks: 100

Minimum Marks: 35

Note: *All five units are compulsory. Part (a) is compulsory carry 4 marks. Attempts any two parts from (b),(c) & (d) carry 8 marks each.*

Q. No		Questions	Marks	CO	BL	PI
Q.1	a)	Illustrate the essential characteristics of cloud computing?	4	CO1	L1	1.6.1
	b)	Compare private, public and hybrid cloud computing with example.	8	CO1	L2	2.6.3
	c)	Define cloud computing? Explain evolution of cloud computing in detail.	8	CO1	L1	2.6.3
	d)	What fundamental advantages does cloud computing technology bring to scientific applications?	8	CO1	L1	2.6.3
Q.2	a)	What are the most important advantages of cloud technologies for social networking application?	4	CO2	L2	1.4.1
	b)	Describe the basic component of an IaaS-based solution for cloud computing?	8	CO2	L2	1.4.1

	c)	What does the acronym SaaS mean? How does it relate to cloud computing?	8	CO2	L4	1.4.1 2.4.2
	d)	The procurement process is a great time for MSPs to help their customers align business goals with the right cloud tools and services. And customers are bound to have a few questions. Give answer to the following questions. i) Is my data safe in the cloud? ii) Should I use a public or private cloud model? iii) What if security fails? iv) How can I save money?	8	CO2	L4	1.4.1 2.4.2
Q.3	a)	Discuss the use of hypervisor in cloud computing.	4	CO3	L2	1.4.1
	b)	What is virtualization? Explain applications of virtualizations in enterprises.	8	CO3	L3	1.4.1
	c)	Explain in detail mobile interoperability implementation for accessing various mobile web services in cloud.	8	CO3	L4	1.4.1
	d)	Discuss about Migration, its need and uses of wave approach.	8	CO3	L2	1.4.1
Q.4	a)	Discuss the Concept of Virtualization and Load Balancing	4	CO4	L2	1.4.1
	b)	Illustrate basic types of cloud services and the AWS products that are built based on them?	8	CO4	L2	1.4.1
	c)	What exactly does the n-tier architecture in cloud systems entail? Describe using a relevant diagram?	8	CO4	L2	1.4.1

		Give an example of a cloud service provider that makes advantage of n-tier architecture as well.				
	d)	Explain the following challenges in cloud. i) Security. ii) Data lock-in and Standardization. iii) Fault tolerance and Disaster recovery.	8	CO1	L2	2.6.3
Q.5	a)	Describe Amazon EC2 and its basic features?	4	CO5	L1	1.4.1
	b)	Describe how cloud computing technologies can be applied to support remote ECG monitoring?	8	CO5	L2	1.4.1
	c)	Describe some examples of CRM and ERP implementation based on cloud computing technologies.	8	CO5	L3	1.4.1
	d)	Describe the architecture of Windows Azure.	8	CO5	L2	1.4.1

CO- Course Outcomes, BL- Bloom's Taxonomy Levels, PI- Performance Indicator

****

Question Bank for 1 unit

1. Discuss the historical development of technologies for distributed computing that have influenced cloud computing

   Or

   Discuss the key enabling technologies in cloud computing systems
2. Different between distributive and computing and cloud computing
3. What is a benefits of cloud computing over traditional computing

   Or

   What are the benefits of adopting cloud computing? List some of them

   Or

   Discuss the benefits of cloud adoption and rudiments
4. Discuss the advantages and disadvantages of cloud computing. Also write down the limitation of cloud computing
5. Describe the characteristics of cloud computing environment

   Or

   What are the characteristics of cloud computing

   Or

   List the characteristics of cloud computing

   Or

   Discuss the characteristics of cloud computing

   Or

   List the main characteristic of NIST cloud computing reference architecture

   Or

   What are the characteristics as per NIST
6. Describe various barriers of cloud computing in brief

   Or

   Discuss various problems associated with cloud computing
7. Explain different cloud services requirements
8. Explain cloud computing reference model

   Or

   What is cloud reference model? What are the applications of this models

   Or

   Define cloud references model
9. Discuss IBN cloud computing reference architecture

   Or

   Define cloud applications architecture

   Or

   Draw the architecture of cloud

   Or

   Explain the NIST cloud computing reference architecture

Unit 1: Introduction to cloud computing

Historical development
Vision of Cloud Computing
Characteristics of cloud computing as per NIST
Cloud computing reference model
Cloud computing environments, Cloud
services requirements,
its advantages and limitations
Cloud and dynamic infrastructure
Cloud Adoption and rudiments.

- The notes have been prepared by using book mention in your syllabus i.e Mastering cloud computing by Buyya, selvi
- I have also incorporated a 2023 previous year question paper
- To get more previous year question paper visit library
- The paper patter shows the university ask out of syllabus question, so I've also added some questions
- The question that highlighted by yellow color, they should be your top priority for preparation
- As we move more further, I'll be updating the notes.

FAQs

Que: Do I have to use your notes for answer writing.

Ans:

- Nope the notes are prepared for students as for reference material, students who are too busy
- Yes, you can use these notes for answer writing.
- Or you can create your own notes or write answer in your word but it has to be specific
- Do not write YouTube answers or any website answer always follow university syllabus mention book for ref. so you score more marks.
- Ignore typo and spelling mistake, use discretion.
- I haven't added few answers search for them like edge computing and fog computing. (Assignment)

Historical development of cloud computing

An overview of the evolution of the technolog.es for distributed computing hat have influenced cloud computing is shown in fig 1.2 The five key technologies that played an important role in the realization of cloud computing are discussed below.

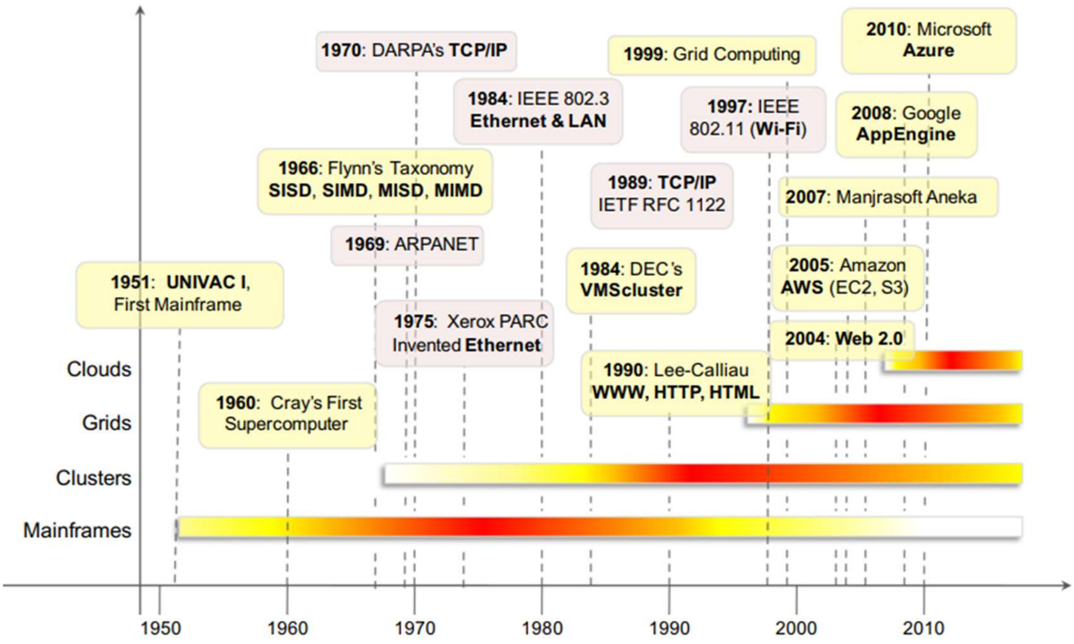


FIGURE 1.6

The evolution of distributed computing technologies, 1950s–2010s.

1. ***Distributed systems***- Clouds are large distributed computing facilities that provides their services to third parties when required. The definition of a distributed system is -

"A distributed system is a collection of independent computers that appears to its users as a single coherent system."

This definition includes two facts

(a) it is made of multiple independent components and

(b) these components are understood as a single entity by users. This is specifically true in case of cloud computing, where cloud

Conceal the complicated architecture they depend on and offer a single interface to the users. The main objective of distributed systems is to share resources are to use them well. In case of cloud computing, this is true where this concept is taken to the extreme and resources are provided to users. In fact, the availability of large computing facility of IT giants is one of the driving factors for cloud computing. Other properties like heterogeneity, openness, transparency, concurrency, continuous availability and independent failures arc shown by distributed systems.

The major milestones in cloud computing are as follows –

(a) **Mainframes -** The first examples of large computational facilities leveraging multiple processing units are mainframes. Mainframes were computers specialized for large data movement and extreme I/O operations They were utilized by large companies to process bulk data like on-line transaction, enterprise resource planning, and other operations including the processing large amount of data. However, mainframes cannot be viewed as distributed systems, they were providing great computational power with the help of multiple processors, which were introduced as a single entity to user- The main application of mainframes was the batch processing.

(b) **Clusters -** A low-cost alternative to the use of mainframes and super computers was cluster computing. Clusters became the standard technology for parallel and high-performance computing by starting from the 1980s They were cheaper compared to main frames, and provided high performance computing to a large number of groups, including universities and small research labs. Cluster technology helped to the evolution of tools and framework for distributed computing a few of them are parallel virtual machine (PVM), condor, message passing interface (MPI). The computational power of commodity machines was one of the attractive features of clusters that could be leveraged to solve problems manageable only on costly super computers

(c) **Grid Computing -** As an evolution of cluster computing, grid computing was introduced, In the early 90s. Grid computing introduced a new approach to access extreme computational power, large storage facilities, and a range of services. Users can use resources similar to other utilities like power, gas, and water. By means of Internet connection, grids initially developed as aggregations of geographically dispersed clusters. A computing grid was a dynamic aggregation of heterogeneous computing nodes.

2. Virtualization - Another important technology for cloud computing is virtualization. Virtualization include a collection of solutions permitting the abstraction of some of the basic elements for computing like hardware, runtime environment, networking, and storage. This technology permits creation of different computing environments. These environments are called as virtual, since they simulate the interface that is hoped by guest. Hardware virtualization is the most common example of virtualization. This technology permits simulating the hardware interface required by an operating system. This technology permits the coexistence of various software stack, on top of the identical hardware. These stacks are contained inside virtual machine instances and work completely separated from each other High performance server can host a number of virtual machine instances hence providing the opportunity of having customized software stack on demand. This base technology enables cloud computing solutions providing virtual server on demands, like Right Scale, Amazon EC2, VMware VC loud, and others For the emulation of IT infrastructure, storage and network virilization along, with hardware virilization complete the range of technologies.

Also, virtualization technologies are utilized for replicating runtime environments for programs. The process virtual machines incorporate the foundation of technologies like Java or NET, where applications are run by a specific program known as virtual machine. A higher level of abstraction with respect to the hardware virtualization is provided by process virtual machines because the guest is only formed by an application instead of a complete software stack. In order to give a platform for sealing applications on demand, like Windows Azure and Google App engine, this approach is used.

(iii) Web 2.0 - The key interface through which cloud computing provides its services is the Web. The Web includes a set of technologies and services that makes simple interactive information sharing, collaboration, application, and user-centered design. This has converted the Web into a rich platform, called as Web 2.0, for application development.

Web 2.0 offers interactivity and flexibility into Web pages, which offer increased user experience by doing Web-based access to all the functions that exist is desktop applications. By integrating a collection of standards and technologies like XML, Web services, Asynchronous Javascript and XML (AJAX), and others, these capabilities are achieved. Web 2.0 applications are very dynamic They enhance continuously and new features and updates are integrated at a constant rate. It is not required to deploy new software releases on the installed base at the client side. By interacting with cloud applications users can lake benefit of the new software features. For effective support of such dynamism, light weight deployment and programming models are very significant. Another fundamental property is loose coupling. The synthetization of new application can be done by composing existing services and integrating them together, hence giving added value.

Google Documents, Google Maps, Facebook, Flicker, Twitter, Blogger, YouTube, de.li.cious, and Wikipedia are examples of Web 2.0 applications.

(iv) Service-oriented Computing –

The core reference model for cloud computing systems is service origination. Service orientation is based on the concept of services as primary building blocks of application is based on the concept of service as primary building blocks of application and system development. Service-oriented computing (SOC) helps the development of faster, cheaper, flexible, evolable, and incorporable applications and systems

An abstraction expressing a self-describing and platform agnostic component that can carry out any function is a service. It is assumed that, service can be reusable, loosely coupled, programming language independent and location transparent.

Service oriented computing prov ides and diffuses two important concept -quality of service (QoS) and software as a service (SaaS). QoS rectum a set of functional and non-functional attributes to evaluate the behavior of a service from different perspectives. These can be performance metrics like response time or security attributes, transactional integrity, availability, scalability, and reliability. QoS requirements are determined between the client and the provider between a Sen ice Level Agreement (SLA) that determines the minimum values for the QoS attributes.

Software as a service provides a new delivery model for applications The application service provider (ASP) maintains the infrastructure and make^ available the application, and the client is independent from maintenance cost and complex upgrades. This software delivery model is possible due to economies of scale are reached with the help of multitenancy.

(v) ***Utility-oriented Computing* -** A vision of computing, defining a service provisioning model for compute services in which resources like storage, compute power applications, and infrastructure are packaged and provided on a pay-per-use basis is called as utility computing. The idea of providing computing as a utility like natural gas, water, power and telephone connection has become a reality today with the advent of cloud computing

Very similar to the traditional real world public utilities (such as electricity water, gas and telephone), their availability and usage charges, this model of computing services and resources are available to the users whenever the; need them and they will be charged based on the amount of usage. This system of packaging the storage with computational resources requires minimal or no initial hardware costs. However, the mentioned resources are rented such that they should be paid to be used. The utility computing environments are currently deployed by establishing service-oriented grids. In this ease the present resources in grids are generally clusters, where clusters are formed from the high-speed interconnection of several standalone machine

Grid computing

As an evolution of cluster computing, grid computing was introduced in the early 90s. Grid computing introduced a new approach to access extreme computational power, large storage facilities, and a range of services. Users can use resources similar to other utilities like power, gas, and water. By means of Internet connection, grids initially developed as aggregations ol geographically dispersed clusters. A computing grid was a dynamic aggregation of heterogeneous computing nodes.

Characteristics of grid computing

There are four major characteristics of grid computing as follows -

(i) Each grid node has its own ownership and management according to the distributed nature of the infrastructure. This suggests that no centralized authority is needed to control all the nodes.

(ii) Some open standards are used for the nodes to interact and exchange information.

(iii) Since the users are provided with the possibility to access distributed resources as if they were local, they can easily interact and cooperate together (e.g. exchanging data). Also, the plug and play concept assists on the fly service creation by aggregating codes, data and software components. A good example is the integration of web applications while utilizing multiple CPUs

(iv) Applications can usually be grid enabled but not all of them will maintain scalability. Moreover, no tools are available to convert applications to fully benefits from the capabilities of a grid.

Advantage of grid computing

The advantages of grid computing are as follows -

(i) The grid software acts as the brain behind the whole grid. Thus, it can centrally manage all the policies.

(ii) A high level of scalability is achieved according to the modular plug and play nature of the grid. Any desktop or server can be attached to or removed from the network based on the preference.

(iii) Upgrading does not force a downtime to the network. There are many resources to handle the ongoing tasks or projects while some resources go offline for any purpose.

(iv) The job execution performance increases, especially for the jobs that can be well split into small chunks.

(v) Applications can be split up among servers to be run and then the results can be smoothly combined and analyzed after the whole task is completed. Therefore, large SMP servers may be useless.

Disadvantages of grid computing

Some disadvantages of grid computing are as follows -

(i) Many applications should be inevitably upgraded in order to utilize the advantages of the model.

(ii) Since various administrative domains are involved, sharing resources may cause political challenges. Many parties are unwilling to share resources that benefit others.

(iii) Memory-hungry tasks and applications are usually required to be run on a large SMP.

(iv) The interconnection between the nodes (resources) is often required to be fast (gigabit Ethernet).

Cloud computing

The term cloud computing refers to the means of providing any and all information technology from computing power to computing infrastructure, applications, business processes and personal collaboration to end users as a service when they require it.

The term cloud in cloud computing means the set of software, hardware, networks storage, services, and interfaces that combine to provide aspects of computing as a service.

A definition given by American National Institute of Standards and Technology (NIST) is as follows-

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can he rapidly provisioned and released with minimal management effort or service provider interaction.

A single area of concern in cloud computing is undoubtedly be privacy and security. When your data travels over and rests on systems that are no longer under your control, you have increased risk due to the interception and malfeasance of others. You cannot count on a cloud provider maintaining your privacy in the face of government actions.

Vision of cloud computing

Cloud computing permits anybody having a credit card to provide virtual hardware, runtime environments, and services. The transformation of the whole stack is done into a collection of utilities, which can be provisioned and composed together to deploy systems in hours, instead of days. Now, this opportunity has become a practice across a number of application domains and business sectors. The demand has improved the set of services offered and fast tracked the technical development.

The usage of cloud computing is limited to a single service at time or a set of services provided by the same vendor. It is hard to move hosted services from one vendor to another due to lack of effective standardization efforts. The long term vision of cloud computing means that IT services are traded as utilities in an open market having no technological and legal barriers. Cloud service providers and consumers play a central role in this cloud market place.

There exist many technological elements contributing to this vision. For a range of services, different stakeholders leverage clouds. The most common reason to consider cloud computing is the requirement for ubiquitous storage and compute power on demand. One of the appealing factors for end-users is the capability of web-based access to documents and their processing using sophisticated applications.

In all these cases, such services are discovered by human intervention - a person looks over the Internet to recognize offerings that satisfy his/her requirements. In future, it will be possible to find the solution that matches our requirements by entering our request in a global digital market that trades cloud computing services. Such market will provide the automation of the discovery process and its integration into existing software systems, hence permitting users to leverage cloud resources in their systems and applications. For trading cloud services, a global platform will also aid service providers to become more visible, and hence to enhance their revenue. Also, a global cloud market decreases the barriers between service consumers and providers.

Properties of cloud computing

The properties of cloud computing are rapid elasticity, measured service, on demand service, ubiquitous network access and location independent

resource pooling

Benefits of cloud computing and rudiment

Or

Benefits of cloud computing over traditional computing

Or

Advantage of cloud computing

Benefits by adopting cloud computing are as follows -

(i) **Availability of Resource** - One of the most general advantages is facilitated by virtualization is resource availability. Also, resource availability helps to leverage and track resource pool under the same umbrella of resource units.

(ii) **Hosted Tools** - By using hosted tools, the developers and testers can simply log in to the tools and use the services over the network. Due to these tools, the tester and developers need not run, install, configure or maintain tools on their systems as they can log into the tools from any machine on the network maintaining the tools.

(iii) **Self-service Capability** - They are capable of self-service, once somebody deploys the cloud services. Now testing teams can use the same services over the cloud and do not have to purchase the computing services and it minimizes the procurement process. Thus, they can concentrate on the testing efforts and services.

(iv) **More Mobility** - Peoples can access information wherever they are, rather than having to remain at their desks.

(v) **Operating Efficiency** - Sometimes development teams and test teams may differ in their conventions and configuration. As a result, the application behavior to be different from the desired one also the delay services. The template-based approach is more transparent, with its solution stacks or hardware, configurable applications and operating system. This approach helps the teams to understand the environment better.

Disadvantages of cloud computing

When we use an application or service in the cloud, we are using something that is not essentially as customizable as we might wish. In addition, applications deployed on-premises still have so many features compared to their cloud counterparts, although many cloud computing applications are very capable.

All cloud computing applications have inherent latency which is intrinsic in their WAN connectivity. If your application demands huge amounts of data transfer, cloud computing may not be the best model for you. However, cloud computing applications excel at large-scale processing tasks.

In addition, cloud computing is a stateless system, as is the Internet. It is essentially unidirectional in nature in order for communication to survive on a distributed system.

Another concern is privacy and security. When data is travelling over and resting on systems that are no longer under your control, there is increased risk due to the interception and malfeasance of others.

Limitations of Cloud Computing - There are several limitations of cloud computing are given below -

(i) **Network Connection** - Network connection should be reliable at client side. Problem in network connectivity will affect the accessing capacity of cloud. Upload and download speeds are slower as compared to that of a local server.

(ii) **Control of Data Security** - The client data does not secure in public cloud because client cannot control security of his data. Hacker can affect the client data by hacking or phishing attacks in cloud. Malware can easily spread in cloud because all servers are connect to each other in cloud.

(iii) **Additional Costs** - Cloud computing offers many cost benefits yet there are some hidden or additional costs. Client has to pay extra for data transfer and other services.

(iv) **Peripherals** - Printers and scanners do not work with cloud. Many devices requires software to be installed locally to work on cloud.

(v) **Integration** - Integrating internal applications with those on cloud are difficult and many time it does not possible.

(vi) **Generic** - Public cloud provides very generic and multi-tenancy services So many organizations cannot comfortable with it. In-house cloud implementation is very difficult and onerous on internal resources if organization is not large.

Business functions suitable to cloud deployment are low-priority business applications, for instance, business intelligence against huge databases, partner-facing project sites, and other low-priority services. Cloud supports traditional Web applications and interactive applications that consist of more than one data sources and services and services with low availability requirements and smaller life spans, for instance, enterprise marketing campaigns require rapid delivery of a promotion that can be turned off immediately. It is also useful if high-volume, low-cost analytics and disaster recovery scenarios, business continuity, backup/recovery-based implementation are needed.

On the basis of technical characteristics, it can be said that it is appropriate for applications that are modular and loosely coupled, isolated workloads, single virtual appliance workloads and software development and testing and preproduction systems.

Applications requiring different levels of infrastructure throughout the day, should be deployed through cloud. The best examples of cloud deployments are applications that require different levels of infrastructure throughout the month, or that have seasonal demand, like those used during the end-of-the- quarter close or during a holiday shopping reason.

It is not appropriate for mission-critical and core business applications, transaction processing and applications relying on important data restricted to the company, or demanding a high level of auditability and accountability because these process cannot share the highly sensitive data, processing power and hardware with the third party Applications running 24 hours with steady demand, applications taking large amounts of memory, incorporating applications depending on large in-memory caches, databases or data sets are not appropriate for cloud. Applications taking benefit of multiple cores, like those that do an important amount of parallel processing and hence advantage from several cores on a sin8le server not suggested for cloud deployment.

It is not suggested for applications that need high-performance file system I/O requiring high-bandwidth inter-server communications, for instance, highly distributed applications. Cloud does not function properly with the applications scaling vertically on single servers.

Characteristics of cloud computing environment

The following characteristics differentiate cloud from any other cloud computing techniques -

(i) **Rapid Elasticity** - Capabilities can be elastically or rapidly provisioned. Capabilities can be added to the system by either scaling out systems or scaling up systems. In some cases, scaling may be manual or automatic. To the consumer, the cloud computing capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

(ii) **Measured Service** - Cloud systems automatically control and optimize resource use through leveraging a metering capability at some level of abstraction suitable to the type of service (e.g. storage, processing, bandwidth and active user accounts). Capabilities usage are monitored controlled and reported providing transparency for both the provider and consumer of the utilized service.

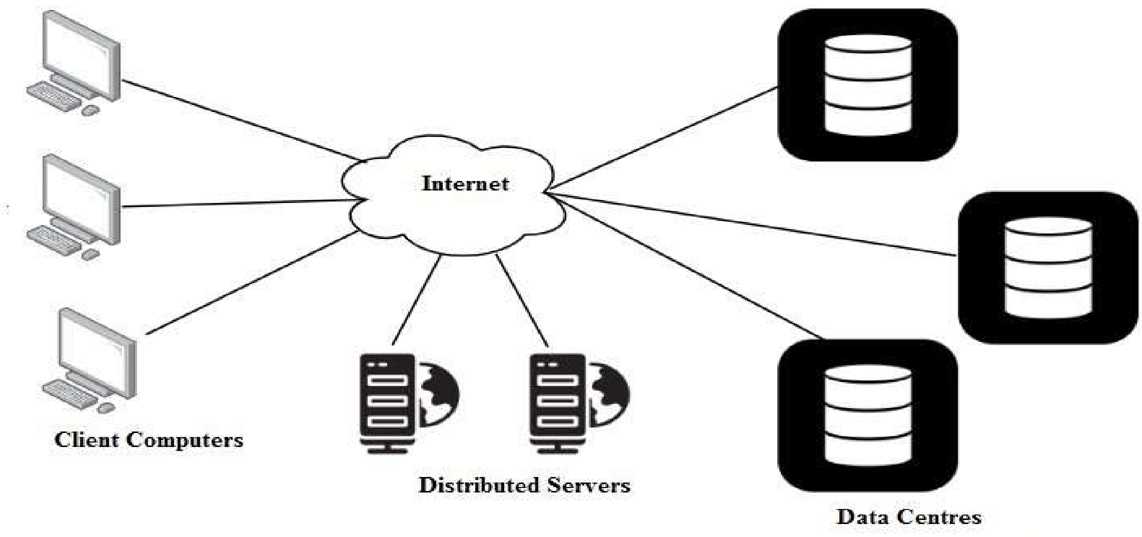
(iii) **On-demand Service** - A consumer can provision computing capabilities like network storage and server time, as needed automatically without requiring human interaction with each cloud service provider.

(iv) **Ubiquitous Network Access**- Resources in the cloud are available over the network and accessed through standard methods that promote used by heterogeneous thin or thick client platforms.

(v) **Location Independent Resource Pooling (Multi-tenant)** - The cloud service provider computing resources are pooled together in a system to serve multiple customers using a multi-tenant model. Virtual and physical resources are dynamically assigned or reassigned on demand. 1 here is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction. Examples of resources include network bandwidth, memory, storage virtual machines and processing.

Cloud components

A cloud computing solution is made up of several elements like client computers, distributed servers and the data center. These components make up the three parts of a cloud computing solution as shown in fig.



(i) Distributed Server - Clouds are large distributed computing facilities that provides their services to third parties when required. The definition of a distributed system is -

"A distributed system is a collection of independent computers that appears to its users as a single coherent system."

This definition includes two facts

(a) it is made of multiple independent components and

(b) these components are understood as a single entity by users. This is specifically true in case of cloud computing, where cloud

Conceal the complicated architecture they depend on and offer a single interface to the users. The main objective of distributed systems is to share resources are to use them well. In case of cloud computing, this is true where this concept is taken to the extreme and resources are provided to users. In fact, the availability of large computing facility of IT giants is one of the driving factors for cloud computing. Other properties like heterogeneity, openness, transparency, concurrency, continuous availability and independent failures arc shown by distributed systems.

The major milestones in cloud computing are as follows –

(a) **Mainframes -** The first examples of large computational facilities leveraging multiple processing units are mainframes. Mainframes were computers specialized for large data movement and extreme I/O operations They were utilized by large companies to process bulk data like on-line transaction, enterprise resource planning, and other operations including the processing large amount of data. However, mainframes cannot be viewed as distributed systems, they were providing great computational power with the help of multiple processors, which were introduced as a single entity to user- The main application of mainframes was the batch processing.

(b) **Clusters -** A low-cost alternative to the use of mainframes and super computers was cluster computing. Clusters became the standard technology for parallel and high-performance computing by starting from the 1980s They were cheaper compared to main frames, and provided high performance computing to a large number of groups, including universities and small research labs. Cluster technology helped to the evolution of tools and framework for distributed computing a few of them are parallel virtual machine (PVM), condor, message passing interface (MPI). The computational power of commodity machines was one of the attractive features of clusters that could be leveraged to solve problems manageable only on costly super computers

(c) **Grid Computing -** As an evolution of cluster computing, grid computing was introduced, In the early 90s. Grid computing introduced a new approach to access extreme computational power, large storage facilities, and a range of services. Users can use resources similar to other utilities like power, gas, and water. By means of Internet connection, grids initially developed as aggregations of geographically dispersed clusters. A computing grid was a dynamic aggregation of heterogeneous computing nodes.

(ii) **Clients** - In a cloud computing architecture, clients are the exact same things that they are in a plain, old, everyday local area network (LAN). They are, typically, the computers that just sit on your desk. But they might also be mobile phones, laptops, tablet computers, or PDAs all big drivers for cloud computing because of their mobility. Anyway, clients are the devices that the end users interact with to manage their information on the cloud. Clients generally divide into three types, mobile, thin and thick.

(iii) **Data Center** - The data center is the collection of servers where the application to which we subscribe is housed. It could be a large room in the basement of our building or a room full of servers on the other side of the world that we access via the Internet. A growing trend in the IT world is virtualizing servers. That is, software can be installed allowing multiple instances of virtual servers to be used. In this way, we can have half a dozen virtual servers running on one physical server.

Major characteristics of cloud computing as per NIST

The following characteristics differentiate cloud from any other cloud computing techniques by NIST -

(i) **Rapid Elasticity** - Capabilities can be elastically or rapidly provisioned. Capabilities can be added to the system by either scaling out systems or scaling up systems. In some cases, scaling may be manual or automatic. To the consumer, the cloud computing capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

(ii) **Measured Service** - Cloud systems automatically control and optimize resource use through leveraging a metering capability at some level of abstraction suitable to the type of service (e.g. storage, processing, bandwidth and active user accounts). Capabilities usage are monitored controlled and reported providing transparency for both the provider and consumer of the utilized service.

(iii) **On-demand Service** - A consumer can provision computing capabilities like network storage and server time, as needed automatically without requiring human interaction with each cloud service provider.

(iv) **Ubiquitous Network Access**- Resources in the cloud are available over the network and accessed through standard methods that promote used by heterogeneous thin or thick client platforms.

(v) **Location Independent Resource Pooling (Multi-tenant)** - The cloud service provider computing resources are pooled together in a system to serve multiple customers using a multi-tenant model. Virtual and physical resources are dynamically assigned or reassigned on demand. 1 here is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction. Examples of resources include network bandwidth, memory, storage virtual machines and processing.

Cloud computing is an emerging style of IT delivery in which applications, data and IT resources are rapidly provisioned and provided as standardized offerings to users over the Web in a flexible pricing model. Cloud computing can significantly reduce IT costs and complexities. It is a way of managing large numbers of highly virtualized resources such that they resemble a single large resource. There is a greater need for IT to help address business challenges and cloud computing can help you do all of these -

(i) **Reducing Risks** - Ensure the right level of security and resiliency across all business data and processes.

(ii) **Doing More with Less** - Reduce capital expenditures and operational expenses.

(iii) **Breakthrough Agility** - Increase ability to quickly deliver new services to capitalize on opportunities while containing costs and managing risk.

(iv) **Higher Quality Services** - Improve quality of service on deliver new services that help the business grow and reduce costs.

Cloud services today are delivered in a user-friendly manner and offered on an unprecedented scale. The payment model is pay-for-what-you-use and pay-as-you-go, eliminating the need for long-term contract and an up front

Investment. This presents a less disruptive business opportunity for businesses with spiky or unpredictable IT demands, as they are able to easily provision massive amount of resources on a moment's notice and release them back into the cloud just as quickly. Following are the some reasons for adopting the cloud -

(i) Pay per use

(ii) No hardware or software to install

(iii) No long-term commitments

(iv) Massive, Web-scale abstracted infrastructure

(v) Dynamic allocation, scaling, movement of applications.

This results in business and IT aligned benefits -

(i) Lower IT barriers to launch new business services

(ii) Provide an effective and creative service delivery model

(iii) Accelerate innovation projects that can lead to new revenue

(iv) Deliver services in a less costly and higher quality business model, while providing service access ubiquity

(v) Rapidly deploy applications over the Internet and leverage new technologies to services when, where and how your clients want them-before your competitors do.

Cloud computing environment

The creation of cloud computing environments includes both the development of applications and systems that use cloud computing solutions and the creation of frameworks, platforms, and infrastructures delivering cloud computing services.

(i) **Application Development**- Applications using cloud-computing take advantage from its capability of dynamically scaling on demand. One class oi applications that benefit from this feature is Web applications. The workload produced by different user demands affects their performance. Wi* the spread of Web 2.0 technologies, the Web has become a platform for developing good and difficult applications including enterprise applications that now use the Internet as the interested channel for service delivery and user- interaction. These applications are sensible to unsuitable sizing of infrastructure and service deployment or variability in workload.

Resource-intensive applications represent another class of applications that can take significant advantage by using cloud computing. These are either compute-intensive or data-intensive applications. In both cases, a significant amount of resources is needed to finish execution in a reasonable time frame. It is noted that there is no need of huge amount of resources constantly or for a long duration.

The solution for on demand and dynamic scaling is offered by cloud computing across the whole stack of computing. This is obtained by

(a) providing runtime environments designed for scalability and dynamic sizing

(b) offering methods for renting compute power, storage, and networking, and

(c) offering application services that imitate the behavior of desktop applications but that are totally hosted and managed on the provider side. All these capabilities use service orientation, which permit an easy integration into available systems.

(ii) **Infrastructure and System Development** - The core technologies enabling the provisioning of cloud services from anywhere in the globe are formed by distributed computing, service orientation, virtualization, and Web 2.0. It is required to have knowledge of all these techniques to develop applications and systems that use the cloud.

A foundation model for cloud computing is distributed computing, since cloud systems are distributed system. In addition, administrative tasks associated with the accessibility of resources in the cloud, the extreme dynamism of cloud systems forms the big challenge for engineers and developers. IaaS solutions allow the addition and removal of resources. PaaS solutions integrate into their core offering algorithms and rules that control the provisioning process and the lease of resources. These can be either subject to fine control or completely transparent to developers. Another element of concern is the integration between cloud resources and existing system deployment.

The interface is formed by Web 2.0 technologies. Cloud computing services are delivered, managed, and provisioned through interface. From a programmatic standpoint Web services have become the key access point to cloud computing systems.

Hence, service orientation is the underlying paradigm that describes a cloud computing system architecture.

Another element playing a fundamental role in cloud computing is virtualization. Virtualization is a core feature of the infrastructure utilized by cloud providers. Cloud applications developers should be aware of the limitations of the selected virtualization technology.

Cloud & dynamic infrastructure

Clients can access standardized IT resource through cloud computing to deploy new application, services or computing resources fastly without reengineering their infrastructure, therefore making it dynamic infrastructure depends on an architecture that contains

the following initiatives-

Asset Management - Provide maximum value of important business and IT assets over their life cycle with industry tailored asset management solutions.

Service Management - Across all the business and IT assets, offer visibility, control and automation to give higher value services.

Virtualization and Consolidation - Decrease operating costs, enhance responsiveness and fully use resources.

Energy Efficiency - Across the business and IT infrastructure, deals with environment, energy, and sustainability challenges and opportunities.

Information Infrastructure - Support businesses obtain objectives like information compliance, availability, retention and security.

Resilience - While quickly changing and responding to risks and opportunities, handle continuous business and IT operations.

Security - Offer end-to-end industry customized governance, risk management and compliance for businesses.

Barrier of cloud computing

Some major barriers identified by IT organizations to large scale adoption of cloud services are as follows -

(i) **Security** - Security concerns are similar to a traditional data center and network in a cloud environment. The overall security risks are perceived as higher for cloud services since most of the information exchange between the cloud service provider and the organization is done over the Web or a shared network, and because IT security is entirely handled by an external entity. Some additional factors cited as contributing to this perception are limited capabilities for monitoring access to applications hosted in the cloud, a belief that multi-tenant platforms are inherently less secure than single-tenant platforms, limited knowledge of the physical location of stored data and the use of virtualization as the underlying technology, where virtualization is seen as relatively new technology.

(ii) **Integration and Interoperability** - Identifying and migrating appropriate applications to the cloud is made complicated by the interdependencies typically associated with business applications. Integration and interoperability issues include a lack of standard interface or APIs for integrating legacy applications with cloud services. This is worse if services from multiple vendors are involved. It also includes software dependencies that must also reside in the cloud for performance reasons, but which may not be ready for licensing on the cloud. There are worries about how disparate applications on multiple platforms, deployed in geographically dispersed locations, can provide the expected levels of service and can interact flowlessly.

(iii) **Governance and Regulatory Compliance** - Large enterprises are ensuring data privacy, and still trying to sort out the appropriate data governance model for cloud services. For large organizations, quality of service is still cited as a major concern. Not all cloud service providers have well defined SLAs, or SLAs that meet stricter corporate standards. Recovery times may be stated as 'as soon as possible' instead of a guaranteed number of hours. In the cloud provider's SLAs, corrective measures are often fairly minimal and do not cover the potential consequent losses to the customer's business in the event of an outage. Another issue is the inability to influence

Cloud service

Any Web-based application or service offered via cloud computing is called a cloud service. Cloud services can include anything from calendar and contact applications to word processing and presentations.

Cloud service requirements

Cloud computing vendors provide point-solution and product offerings" On the other hand, one should provide comprehensive, asset-based solutions to deploy dynamic infrastructure, which is needed for a cloud delivery model These services are designed to provide business outputs to our clients. The following benefits should be provided by an approach to cloud computing -

(i) Services intended at specific infrastructure workloads to support accelerate standardization of services, providing productivity gains and fast client payback on their investment.

(ii) To offer visibility, control and automation in IT and business services, a service management system is embedded with cloud services.

There should be infrastructure strategy and planning services for cloud computing to support companies plan their infrastructure workloads through the suitable cloud delivery model. Cloud strategy, cloud assessment, design and development of a cloud roadmap and return on investment (ROI) assessment by workload are specific assistance. Clients should begin with a strategy and planning consulting engagement, and a pilot implementation of a key workload as well.

Different cloud service requirements

Major cloud services requirements are as follows -

(i) **Security** - The resource pooling characteristics of cloud computing permits users to dynamically share physical and virtual resources. High security concerns are usually associated with virtual environments which include virtual components like hypervisor for running virtual machines and virtual environments for virtual machines communications. An organization that contain] its own IT components in it premises can apply and monitor proper security policies and controls especially for identity management. As a result, it is a priority to choose a cloud service which supports suitable and adequate access control and authentication mechanisms.

(ii) **Privacy** - Organizations are often uncertain when it comes to managing and storing sensitive information in the cloud. Privacy is an important issue to be addressed in the direction of raising users' trust in the cloud computing paradigm The geographic location of data stored in a cloud environment is usually not revealed to users. This lack of transparency raises high concerns especially that privacy regulations and policies differ from one country to another

(iii) **Availability** - Most organizations need maximum availability levels of their computing resources provided by the cloud services. Cloud services have recently experienced failures resulting from several factors including security attacks, natural disasters and infrastructure outages. Cloud computing environments need to make serious provisions to react quickly and efficiently to such outages and ensure continuity of cloud services. Thus, the ability to efficiently and seamlessly recover from outages is an important factor to consider when comparing cloud services.

(iv) **flexibility** - Cloud computing service providers should be able to offer flexible plans and services that allow an enterprise to quickly and efficiently adapt to changes in their goals, customer demands and global changes.

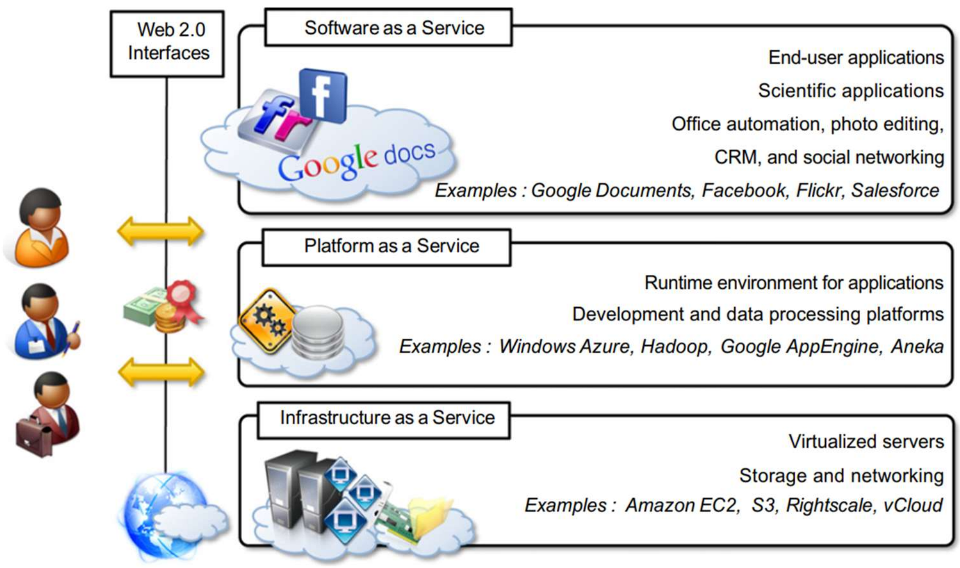
(v) **Archiving** - Archiving provides long term storage of data that is no longer momentarily needed keeping archived data imposes high storage demands and also require additional backup and restore feature for the consumers. It may also imposes some additional costs on the services. Hence, a cloud computing service with an archiving feature and easy access to archived data is among the essential requirements for many organizations.

(vi) **Scalability** - Cloud scalability is one of the most important factors in providing successful cloud services. It is mainly enabled by increasing the capacity and number of IT resources.

Cloud computing reference model

The capability to deliver on demand a range of IT services is a basic characteristic of cloud computing. This range of IT services provides a distinct perception of what cloud computing is among users.

Cloud computing services can be classified into three categories - Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). figure shows the relationship among these categories and provides an organic vie* of cloud computing. This diagram is referred to as cloud computing reference model This model shows a layered view of range of cloud computing services. This view walks the computing stack from bottom to top.



Infrastructure-as-a-Service solutions provide infrastructure on demand in the form of virtual hardware, storage, and networking at the base of the stack. Virtual hardware is used to offer compute on demand in the form of virtual machines instances. On user's request on the provider's infrastructure, these instances are created. Users are provided tools and interfaces to configure the software stack installed in the virtual machine. In terms of dollars per hours, the pricing model is defined, where the characteristics of the virtual hardware affect the hourly cost. Virtual storage is provided in raw disk space or object store form. The former complements a virtual hardware offering that needs persistent storage. The latter is a high-level abstraction to store entities instead of files. The collection of services is identified by virtual networking. These services manage the networking among virtual instances and their connectivity towards the Internet or private networks.

The next step in the stack is Platform-as-a Service solutions. These solutions provide scalable and elastic runtime environments on demand that host the execution of applications. These services are backed by a core middleware platform. The core middleware platform creates the abstract environment for deploying and executing applications. The service provider is responsible for offering scalability and managing fault-tolerance, while users are requested to concentrate on the logic of the application developed by leveraging the provider's API's and libraries.

Software-as-a-Service solutions are at the top of stack. They give applications and services on demand. The SaaS layer is the area of social networking Websites. These Websites use cloud-based infrastructures to bear the load produced by their popularity.

laaS solutions are sought by users to use cloud computing from building dynamically scalable computing systems needing a particular software stack. Hence, IaaS services are utilized to build scalable Websites or for background processing.

IBN cloud computing reference architecture

Or

Cloud application architecture

Or

Cloud reference architecture in details

Or

NIST cloud computing reference architecture

Or

NIST cloud computing reference architecture with a neat schematic diagram

All the cloud computing realizations can be organized into a layered structure that covers the whole stack from the hardware appliances to software systems as shown in fig.

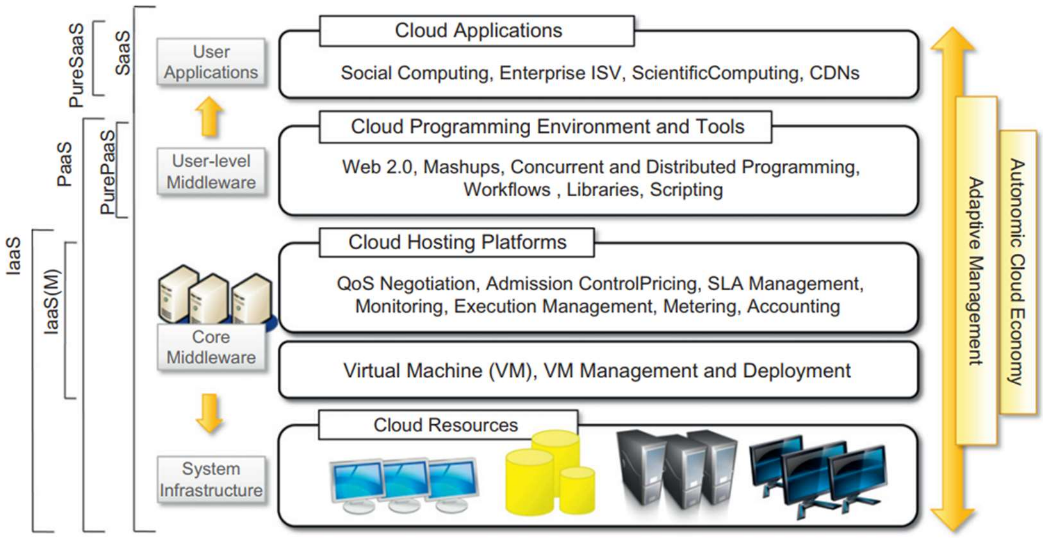


FIGURE 4.1

The cloud computing architecture.

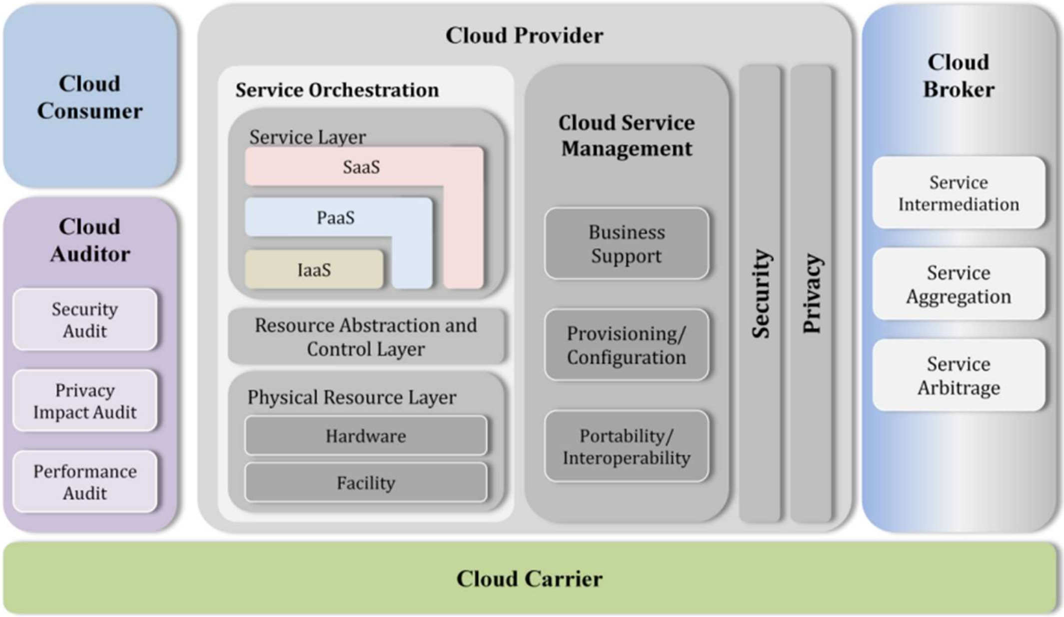


Figure 1: The Conceptual Reference Model

Cloud resources are deployed to provide computing/horse power needed for offering services. A data center in which several nodes are stacked together is used to implements this layer. Since different types of resources can be used to make cloud infrastructure, therefore it can be in heterogeneous nature. Some other parts of cloud infrastructure can be database systems and other storage services. The core middleware manages the physical infrastructure. The goals of core middleware are to offer a suitable runtime environment for applications and to use resources optimally. Virtualization technologies are employed to ensure runtime environment customization, sandboxing, quality of service and application isolation at the bottom of the stack. At this level, hardware virtualization is the most generally used. Hypervisors expose the distributed infostructure like a collection of virtual machines and manage the pool of resources. (Us feasible to divide the hardware resources by employing virtual machine technology, thus satisfying the need of users and applications. Generally, this solution is combined with network and storage virtualization strategies that enable the infrastructure to he fully virtualized and controlled. The prime function of core middleware is infrastructure management that supports capabilities like Quality of Service (QoS) negotiation, execution management, service level agreement management, admission control, monitoring, metering, accounting, billing, and pricing.

Generally, the combination of cloud hosting platforms and resources is known as Infrastructure-as-a-Service (IaaS) solution. For designing the system infrastructure, IaaS solutions are appropriate but offer limited services to construct applications. Such service is offered by cloud programming environments and tools that create a new layer for providing a development platform for applications to users. The range of tools entail Web based interfaces, frameworks for concurrent and distributed programming, scripting, libraries, mashups, workflows, and command line tools. Users create their applications particularly for the cloud by employing the application programming interface exposed at the user-level middleware in this scenario. That's why, this approach is also called as Platform-as-a-Service (PaaS), since the service provided to the user is a development platform instead of an infrastructure. Generally. PaaS solutions incorporate the infrastructure as well.

The services delivered at application level are known as Software-as-a- Service (SaaS) and are maintained at the top layer of cloud reference architecture. Mostly, these are Web based applications that depend on the cloud to offer service to end users. The cloud horse power enables independent software vendors to provide their application services over the Internet Other applications related to this layer are those using the Internet for their main functionalities that depend on the cloud to maintain several numbers of users.

Question Bank UNIT 2

1. Describe software-as-a- service (SaaS) solution. How is related to cloud computing?

Or

What do you understand by SaaS

2. Explain Platform-as-a-Service (PaaS) solution in details

3. Describe the basic components of an IaaS based solution

4. Explain cloud reference model in detail

Or

What is cloud reference model? What are the applications of this models

5. Explain in brief cloud desktop infrastructure in brief with its services

Or

Explain in detail about virtual desktop infrastructure

Or

What is virtual desktop infrastructure

6. Describe VMware infrastructure in details

7. write short note on

   a. Mist computing

   b. Fog computing

   c. scalability and fault tolerance

8. Classify different types of cloud

9. Explain hybrid cloud with schematic diagram

Or

What describes hybrid clod

Or

Explain hybrid cloud with example

10. Describe community cloud in details

Or

What describes a community cloud model

Unit 2: Cloud Computing Architecture

Cloud Reference Model
Concept of IaaS, PaaS, SaaS,AaaS, BaaS, FaaS, DaaS, STaaS, CaaS, NaaS, DBaaS, AaaS, aPaaS, iPaaS, apimPaaS, IoT PaaS, mPaaS, dbPaaS, and UIPaaS,
Types of Clouds
Cloud Interoperability & Standards,
Scalability and Fault Tolerance
Virtual Desktop Infrastructure
Fog computing
Mist(Edge) computing

Types of cloud

Clouds can be classified into following types -

(i) Public Clouds - Cloud computing environments that are open for public use alternatively for a large industry group. Some public clouds are Google, Amazon and IBM offerings.

(ii) Private Clouds - The cloud is implemented within the private premises of an institution and uses it to provide services to the users ot the institution or a subset of them.

(iii) Hybrid (Heterogeneous) Clouds - A computing environment which combines multiple clouds where those clouds keep their unique identities, hut are bound together as a unit. It identifies a private cloud that has been augmented with resources or services hosted in a public cloud.

(iii) Community Clouds -These clouds are particularly intended to address the requirements of a particular industry. The cloud is characterized by a multi-administrative domain encompassing various deployment models.

Public cloud in details

The first expression of cloud computing is formed by public clouds. Public clouds are a realization of cloud computing canonical view where the services provided are presented to anyone, at any instant and from anywhere using the Internet. They are a distributed system from a structural perspective and possibly formed by one or more data centers, on top of which the specific services provided by the cloud are implemented. Any user can easily sign-in with the cloud provider, enter details and utilize the services provided. The first class of clouds that were implemented and provided were public clouds. Public clouds provide as a feasible option for handling peak loads on the local infrastructure and provide solutions for reducing IT infrastructure costs. For small enterprises, they have become an interesting alternative. Small enterprises are able to begin their business without large upfront investments by entirely depending on public infrastructure for their IT requirements. Public clouds are used both to extend the IT infrastructure of enterprise on demand and to completely replace it.

Multi-tenancy is a basic feature of public clouds. A public cloud serves as a large number of users instead of a single one. It is required by a customer to have virtual computing environment that is separated, and possibly isolated, form the other uses. This is a basic requirement to offers an effective monitoring of users activities , the other Quality of Service (QoS) attributes negotiation with users, and ensure the required performance. In public clouds, QoS management is an important feature. As a result, a considerable portion of the software infrastructure is given to monitor the cloud resources, to bill them on the basis of the contract done with the user and to keep the complete history of the cloud usage for each customer. For public clouds, these features are basic since they help providers to provide services to users with full accountability A public cloud can provide various type of services like software/applications platform, and infrastructure/hardware. As an example, SalesForce com is a public cloud providing software as a service, Google AppEngine is a public cloud providing an application development platform as a service and Amazon EC2 is a public cloud providing infrastructure as a service. Finally, we can say that public clouds are large hardware and software infrastructure whose capability is sufficient to meet the requirements of multiple users, however, they suffer from security threats and administrative pitfalls.

Service consumed by public clouds

The services consumed by public cloud are –

(i) Lower cost

(ii) Ease of access

(iii) Discovery of services

(iv) Restful interface support

(v) Speed and availability

(vi) Security and data privacy.

Challenges to consumers in adopting a public cloud

There are few challenges that are preventing wide scale adoption of public clouds -

(i) Security

(ii) Reliability and performance

(iii) Vendor lock-in

(iv) Leveraging existing investment

(v) Corporate governance and auditing

(vi) Maturity of the solutions.

Major public cloud security issues in cloud model

The major public cloud security issues in cloud model are as

follows -

(i) **Network Attacks** - The main challenge in public cloud security is enterprises data which is stored somewhere in the cloud. In a private cloud, entire infrastructure is under direct control of the owner. In this situation secure protection of the data is applicable by the data owner. However in public cloud data is stored somewhere in the cloud which dedicates data security level profoundly. Moreover in order to alleviate the problem of under- utilization of the infrastructure and optimum usage of the computing power and storage capacity, the cloud service providers propose virtual machines to the users. Subsequently a number of customers are running their programs and storing their data on a multi-tenant situation which in this case using data leakage prevention (DLP) software is worthless to protect the sensitive data According to this fact, there would be some probabilities in the public cloud for data to be exploited by hackers. A hacker can steal or take under, control a virtual machine to host a malicious service or application to attack

against service provider or access customer's data. :

(ii) **Incompetency of Vendors** - In addition to the fact that securing customer's data strategies in public cloud are considerably poor because cloud computing is a new phenomenon in computing industry, many well known companies need to cut their investment on data protection to increase their benefits Aside from the vendors and their equipment’s, their employees are another considerable factor in public cloud security issues. Deploying novice c for reducing costs and so on will be very harmful in terms of handling and managing security incident. Besides neglecting in controlling the employees might persuade wavery ones of them to be hired by attackers to snoop the data. Finally a cloud vendor must be permanently available. That means failure of the vendor will lead to loss of customers' data in some cases.

(iii) **Data Access by Vendors** - Access of service provider to customer's data is undeniable yet cloud storage confidentiality needs to prevent vendor access to user's data. Highlighted data control by service providers as a factor for strengthening security and privacy concerns for customers. More over enterprises with sensitive data still have problems with monitoring privileged access, user authentication and creating business matrices and tracking operational performance on outsourced infrastructure. Access to information by vendors causes to failure of many information privacy protection plans such as - electronic communications privacy act (ECPA). USA PATRIOT act (UPA), health insurance portability and accountability act (HIPAA), fair credit reporting act (FCRA), video privacy protection act (VPPA), gramm leach bliley act (GLBA), cable communications policy act (CCPA).

(iv) **Data Access by Government** - The concept of cloud comes from uncertain location of infrastructure specially data storage provided by public cloud service providers. The data of an enterprise might be stored in various countries with different regulations and laws governing data storage ca and data access activities. Therefore, geographical data location is the indispensable part of cloud computing. However physical data location and ca unauthorized access to private data is an apprehension for many enterprises for absence of rules that be globally accepted about data security and privacy. Believed that one of the goals to achieve adequate security is control of the distributed computation over the data in public cloud.

(v) **Authentication and Virtualization** - With considering authentication issues as another drawback of public cloud, risk of cyber attacks could be amplified dramatically. This security vulnerability allows attackers and hackers to target non-guarded client data over the internet which were hosted in the private data centers previously. They also believed that in public cloud environments which share sources between different subscribers unauthorized access by attackers who posed as subscribers to other's data is facilitated. Sharing infrastructure between customers multiple organizations operating on a vendor s infrastructure are more attractive target than a single enterprise. This fact increases the risk of attack dramatically.

Private clouds

Private clouds offer internal users with dynamic provisioning of computing resources. They are virtual distributed system that depend on a private infrastructure. Private clouds use other schemes in place of a pay-as-you-go model. They keep in-house the core business operations by depending on the existing IT infrastructure and decreasing the burden of maintaining it once the cloud has been created. Here, sensitive information does not flow out of the private infrastructure, therefore, security concerns are less critical. As the private cloud can offer services to various types of users, existing IT resources can be better utilized. The possibility of testing applications and systems at a comparatively lower price is another important aspect that comes with private cloud.

When it is necessary to keep the processing of information within the premises, or it is necessary to use the existing hardware and software infrastructure, private clouds are the perfect solution. The major drawback of private deployments is the inability to efficiently address peak loads and to scale on demand.

Services provide by private clouds

The services provided by private cloud are -

(i) Virtualization

(ii) Multi-tenancy

(iii) Consistent deployment

(iv) Security and access control

(v) Chargeback and pricing

(vi) Government and management.

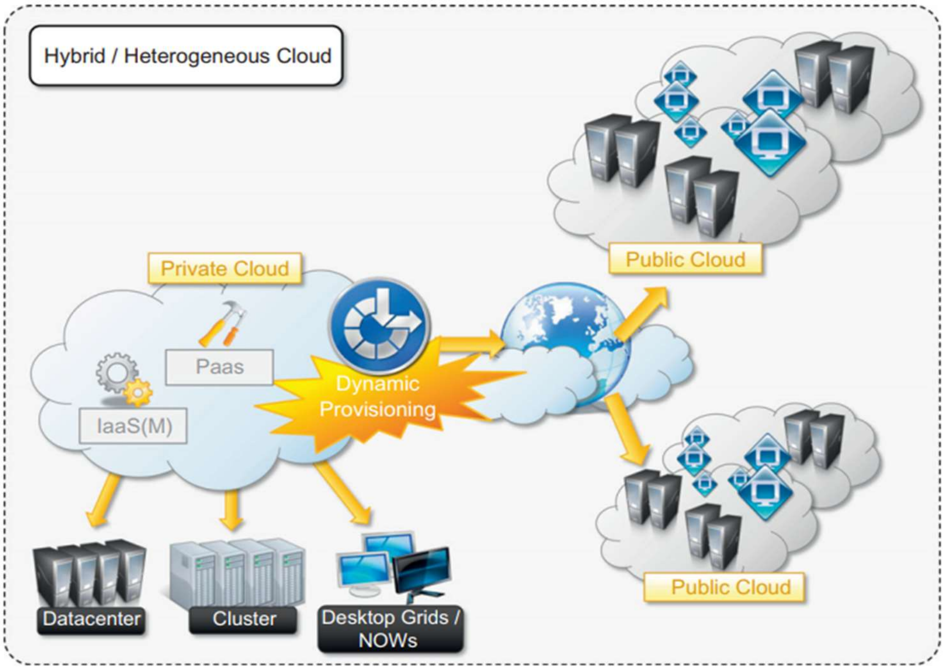
Need of private cloud

Public clouds offer a feasible option to minimize IT costs and reduce capital expenses, but they are not useful in all scenarios. As an example, the loss of control is a very general critique to the use of cloud computing in its canonical implementation. The provider is in control of the infrastructure and eventually of the customer's core logic and sensitive data in case of public cloud. Although there could be regulatory procedures in place that ensure a fair management and the respect of the customer's privacy, this situation can still be considered as a threat or as an unacceptable risk that some enterprises are not required. Public clouds will not consider as an option for processing or storing sensitive data of institutions such as government and military agencies. The risk of a breach in the security infrastructure of the provider could expose such information to others which is considered unacceptable. In other cases, the loss control of where your virtual IT infrastructure resides create other problems. Generally, the geographical location of datacenter determines the regulation that are applied to digital information management. Consequently, depending on the particular data location, some sensitive information can be accessed by government agencies or even assumed out of the law if processed with some cryptography techniques. At last, existing organization having large computing infrastructure or huge installed bases of software do not want to switch to public clouds, but utilize the existing IT resources and optimizing their revenue. All these qualities do not make the use of a public computing infrastructure always possible. However, a general idea assisted by the cloud computing vision can still be attractive. More precisely, having an infrastructure able to provide IT services on demand can still be a winning solution, even in the case when implemented within the private premises of an institution This resulted in the widespread use of private clouds, but its resource provisioning model is restricted within an enterprise boundary.

Hybrid clouds with schematic diagram

Hybrid cloud solution can take the benefits of both public and private clouds. Hybrid clouds permit maintaining sensitive information within the premises, exploiting existing IT infrastructures, and naturally growing and shrinking by provisioning external resources and releasing them on demand. Now, security concerns are only restricted to the public portion of the cloud, that can be used to carry out operations with less stringent constraints but that' are still part the system workload. A heterogeneous distributed system resulting from a private cloud is hybrid cloud. Private cloud combines extra services or resources from one or more public clouds. That's why, they are also known as heterogeneous clouds. In this scenario, dynamic provisioning is a fundamental component. Hybrid clouds deal with scalability issues by using external resources for exceeding capacity demand. For the needed amount of time, these resources or services are temporarily leased and thereafter released. This practice is also referred to as cloud-bursting. Here, cloud-burst refers to the dynamic provisioning of resources from public clouds.

The concept of hybrid cloud is general, but in most cases it applies to IT infrastructure. Within an IaaS scenario, dynamic provisioning means the ability to obtain on demand virtual machines to enhance the capability of the resulting distributed system and releasing them. Specifically, in case of private clouds, dynamic provisioning provides more complex scheduling algorithms and policies whose aim is also to optimize the budget spent to rent public resources. The building blocks for deploying and managing hybrid clouds are infrastructure management software and PaaS solutions. A schematic diagram of hybrid clouds is shown in fig.



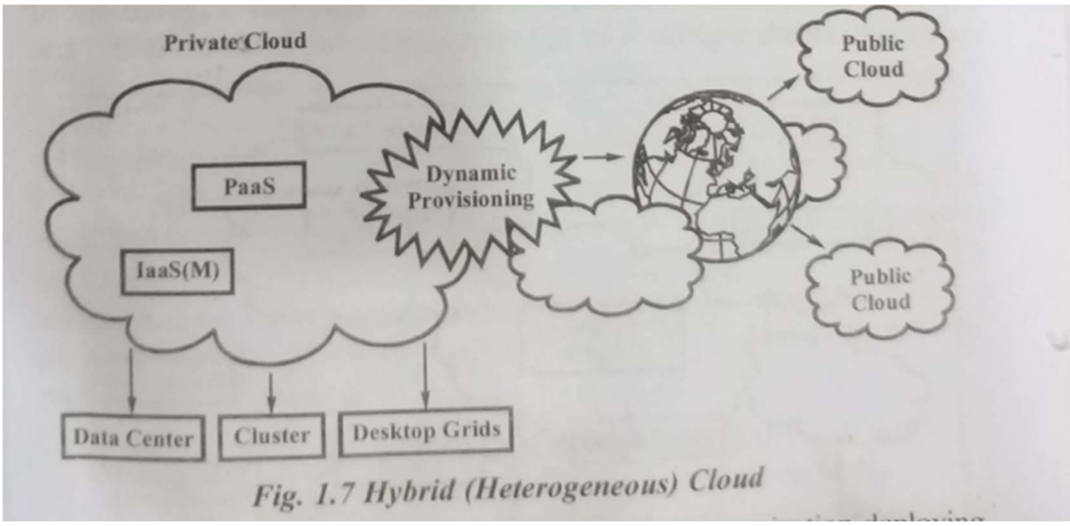
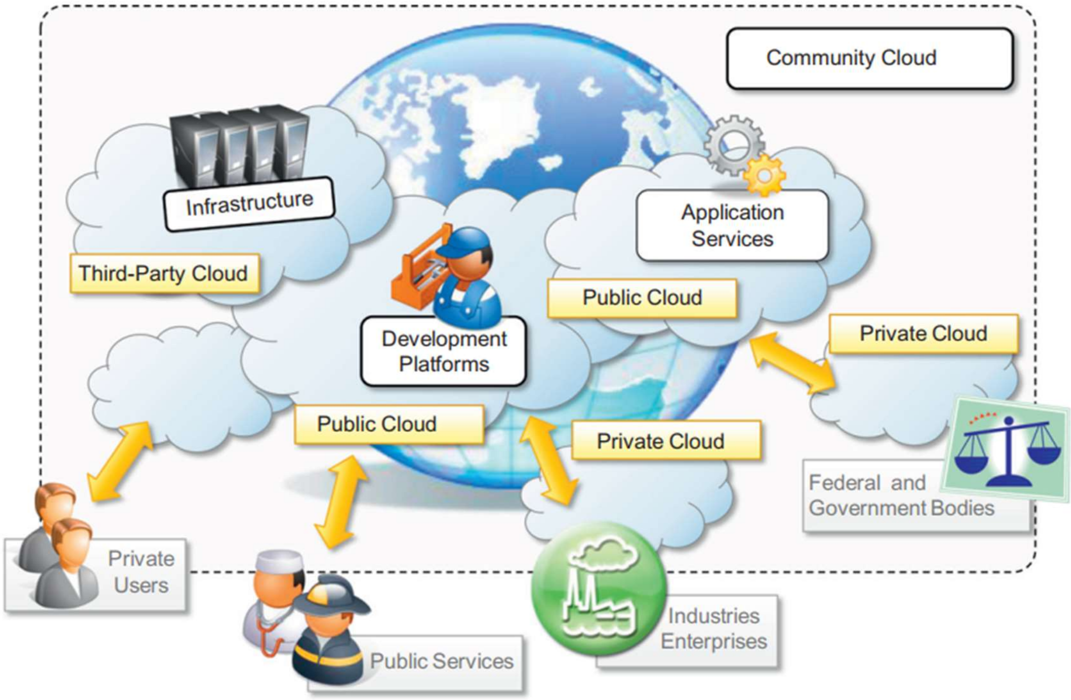


Fig. 1.7 Hybrid (Heterogeneous) Cloud

An example of hybrid cloud may consist of an organization deploying non-critical software applications in the public cloud, while keeping critical or sensitive apps in a private cloud, on the premises.

Community clouds

A community cloud is a distributed system made up by integrating the services of various clouds. This is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. Community clouds deal with the specific requirements of an industry, a business sector, or a community. The members of the community share access to the data and applications in the cloud. A general view of the usage scenario of community clouds together with reference architecture is shown in fig.



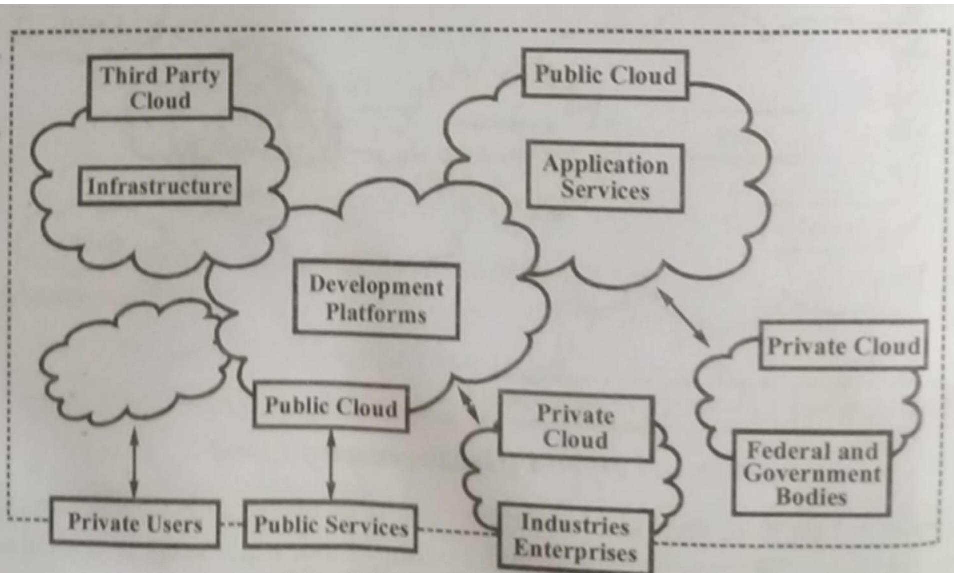


Fig. 1.8 Community Cloud

The member of a specific community are fall into a well-identified community, sharing the same concerns or requirements. They can be industries, government bodies or even simple users but all of them concentrate on the similar issues for their interaction with the cloud. This scenario serves a multitude of users with various requirements. A community cloud is possibly implemented over multiple administrative domains from an architectural perspective. It means that organizations like private businesses, research organization, government bodies and even public virtual infrastructure providers, contribute with their resources to construct the cloud infrastructure.

Following are the candidate sectors for community clouds -

(i) Public Sector - In the public sector, the adoption of public cloud offerings can be limited by legal and political restrictions. Besides, governmental processes incorporates various institutions and agencies, and are aimed to offer strategic solutions at local, national and international administrative level. They entail business-to-business, business-to-administration and citizen-to-administration processes.

(ii) Healthcare Industry - There are various scenarios within the healthcare industry where community clouds could be of use. Particularly, they can offer a global platform where information and knowledge can be shared without disclosing important data maintained within the private infrastructure.

(iii) Media Industry - To enhance the efficiency of content production, companies are looking for low-cost, agile, and simple solutions in the media industry. An extended ecosystem of partners is involved by most of the media productions. The production of digital content is the result of a collaborative process including movement of huge amount of data, complex workflow executions, and massive compute-intensive rendering tasks.

(iv) Scientific Research - An interesting example of community clouds is science clouds. Here, scientific computing is the common interest driving different organizations sharing a large distributed infrastructure.

(v) Energy and Other Core Industries - Community clouds in these sectors can bundle together the complete set of solutions that together vertically deal with deployment, management and orchestration of services and operations. A community cloud can offer the proper infrastructure to make an open and fair market as these industries entail different vendors

providers and organizations.

Advantage of community clouds

Following are the advantages of community clouds -

Openness - Community clouds are open systems where a fair competition between different solutions can occur by alleviating the dependency on cloud vendors.

(ii) **Graceful Failures** - There is no single point of failure because^ there is no single provider or vendor in control of the infrastructure

(iii) **Community** - Since the system can grow simply by expanding its user base, the infrastructure turns out to be more scalable, being based on a collectivity providing resources and services.

(iv) **Environmental Sustainability** - The community clouds are assumed to have a smaller carbon foot print because they harness underutilized resources. In addition, they tend to be more organic by growing and shrinking in a symbiotic relationship to assist the demand of the community, which in turns maintain it.

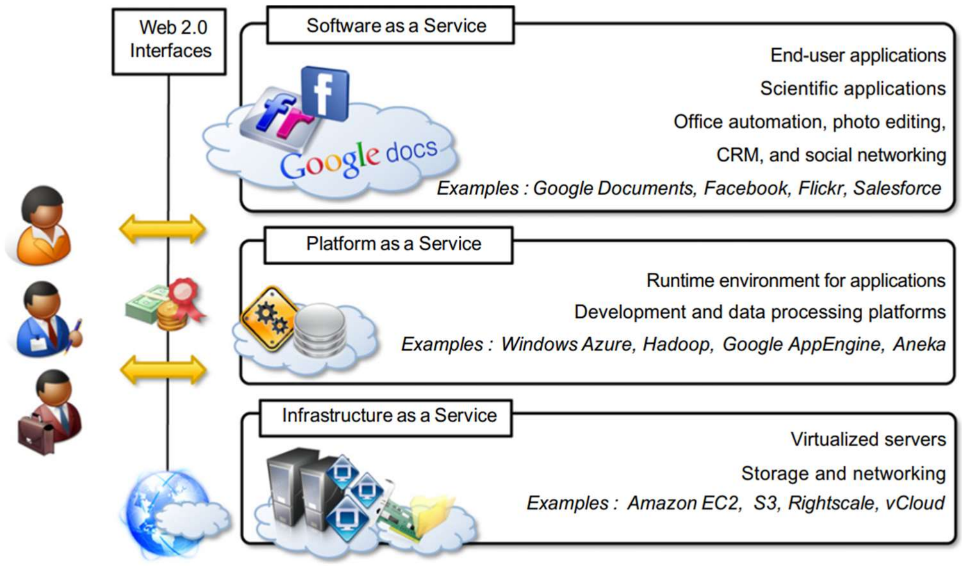
(v) **Convenience and Control**- Since the cloud is shared and owned by the community which operates all the decisions via a collective democratic process, there is no conflict between the convenience and control.

Cloud reference models

Cloud computing reference model

The capability to deliver on demand a range of IT services is a basic characteristic of cloud computing. This range of IT services provides a distinct perception of what cloud computing is among users.

Cloud computing services can be classified into three categories - Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). figure shows the relationship among these categories and provides an organic vie* of cloud computing. This diagram is referred to as cloud computing reference model This model shows a layered view of range of cloud computing services. This view walks the computing stack from bottom to top.



Infrastructure-as-a-Service solutions provide infrastructure on demand in the form of virtual hardware, storage, and networking at the base of the stack. Virtual hardware is used to offer compute on demand in the form of virtual machines instances. On user's request on the provider's infrastructure, these instances are created. Users are provided tools and interfaces to configure the software stack installed in the virtual machine. In terms of dollars per hours, the pricing model is defined, where the characteristics of the virtual hardware affect the hourly cost. Virtual storage is provided in raw disk space or object store form. The former complements a virtual hardware offering that needs persistent storage. The latter is a high-level abstraction to store entities instead of files. The collection of services is identified by virtual networking. These services manage the networking among virtual instances and their connectivity towards the Internet or private networks.

The next step in the stack is Platform-as-a Service solutions. These solutions provide scalable and elastic runtime environments on demand that host the execution of applications. These services are backed by a core middleware platform. The core middleware platform creates the abstract environment for deploying and executing applications. The service provider is responsible for offering scalability and managing fault-tolerance, while users are requested to concentrate on the logic of the application developed by leveraging the provider's API's and libraries.

Software-as-a-Service solutions are at the top of stack. They give applications and services on demand. The SaaS layer is the area of social networking Websites. These Websites use cloud-based infrastructures to bear the load produced by their popularity.

laaS solutions are sought by users to use cloud computing from building dynamically scalable computing systems needing a particular software stack. Hence, IaaS services are utilized to build scalable Websites or for background processing.

SaaS solutions

The concept of SaaS is precedent to cloud computing and started to circulate at the end of 90s. SaaS is a software delivery model which offers access to applications using the Internet. It gives a way to free users from complex hardware and software management by leaving such tasks to third parties, who create applications accessible to multiple users by a Web browser. Here, customers do not install anything on their premises. Also, the> do not pay considerable upfront costs to purchase the software and the required licenses. The) simply access the application Website, enter their credentials and billing details, and can instantly use the application that can be further customized for their requirements. The infrastructure maintains the specific details and characteristics of each customer's application and makes available when required on the provider side.

The SaaS model is useful for applications that can be adjusted to specific needs with little further customization and serving a variety of users. This requirement characterizes SaaS as a one-to-many software delivery model. In a one-to-many software delivery model, an application is shared across several users. This is the case of Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) applications that form general requirements for almost all the businesses. There will be similar requirements for the basic characteristics related to CRM and ERP in ever) enterprise, different requirements can be met with further customization, I his scenario makes easy the development of software platforms offering a set of characteristics and supporting specialization and ease of integrations of new components. It constitutes the perfect candidate for hosted solutions, because the applications provided to the user are the same, and the application itself give means to the users to shape itself on the basis of their requirements. Consequently, SaaS application are naturally multi-tenant, which is a characteristics of SaaS. This characteristics enables providers to centralize and sustain the effort of managing large hardware infrastructure, optimizing resources by sharing the costs among the large user base, and maintaining and upgrading applications transparently to the users. Such costs constitute a minimal fraction of the usage fee paid for the software on the customer side.

The SaaS approach resides on top of the cloud computing stack. It fits into the cloud computing vision denoted by the acronym XaaS- everything as a service. Application are provide as a service with SaaS. In the beginning the SaaS model was useful only for lead users and early adopter. After cloud computing , there has been an increasing acceptance of SaaS as a feasible software delivery model. This results in the development of SaaS 2.0, which does not give a new technology but changes the manner in which SaaS is used

Characteristics of SaaS solution

Like other forms of cloud computing, it is important to ensure that

solutions sold as SaaS in fact comply with generally accepted definitions of cloud computing. Some defining characteristics of SaaS include -

(i) Web access to commercial software.

(ii) Software is managed from a central location.

(iii) Software delivered in a "one to many" model

(iv) User not required to handle software upgrades and patches.

(v) Application Programming Interfaces (APIs) allow for integration between different pieces of software.

Application of SaaS solution

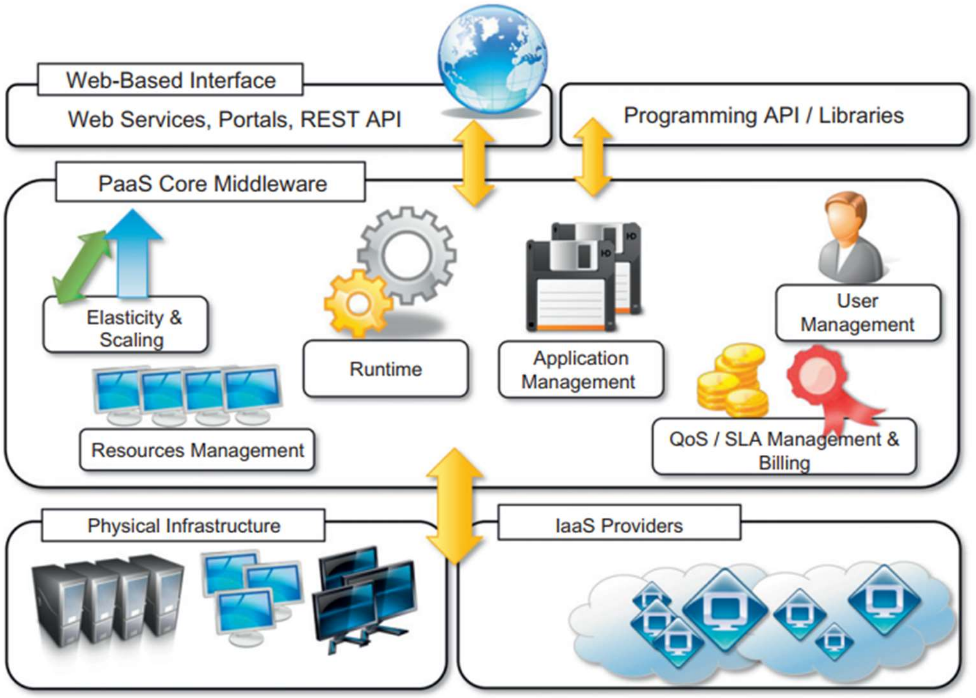
The most popular SaaS application are CRM, ERP and social networking. The most successful and popular example of CRM service is SalesForce.com, which builds on top of the Force.com platform SalesForce.com provides either a programming language or a visual environment to organize component together for creating application. It offers a variety of services for applications such as customer relationship and human resource management, enterprise resources planning, and several other feature. Apart from the basic features, the integration with third-party application improves the value of SalesForce.com. Customers can search, publish, and integrate new services and features into their existing application, particularly, through AppExchange. AppExchange makes

SalesForce.com absolutely extensible and customizable. Similar solutions are provided by RightNow and NetSuite.

Social networking applications like Orkut, Facebook and professional networking such as Linkedin constitute an another important class of SasS applications. Besides, the basic features of networking, SaaS applications enable incorporating and extending their capabilities by integrating third-party applications. For the hosting platform, SaaS applications can be developed as plug-ins and presented to the users to choose which applications they like to add in their profile. Consequently, the integrated applications get full access to the network of contacts and the user profile data.

PaaS solution

In the cloud, PaaS solutions offer a development and deployment platform for executing applications. PasS solutions form the middleware on top of which applications are made. The main functionality of the middleware is application management. PaaS implementations automate the process of deploying applications to the infrastructure, provisioning and configuring supporting technologies, configuring applications components, and managing system change on the basis of policies defined by the user. They do not expose any service for managing the underlying infrastructure and offer applications with a runtime environment. Developer's system is designed by them in terms of applications and are not related with operating systems, hardware, and other low-level services. According to the commitments done with the users, the core middleware is responsible for managing the resources and scaling applications automatically or on request. The core middleware exposes interfaces that permit programming and deploying applications on the cloud from a user perspective. These can be in the form of programming APIs and libraries or in the form of a Web-based interface. Fig. provides an overall view of the PaaS approach.



The interface exposed to the user is determined by the certain development model decided for applications. Certain implementations offer a fully web based interface hosted in the cloud offering various services. It is possible to discover integrated developed environment on the basis of 4GL and visual programming concepts, or rapid prototyping environment in which application are made by assembling mash up and user defined components, and successively customeized. Other implementation of the PaaS model offers a programming language based approach and offers a complete object model for representing an application This approach gives more opportunities and flexibility however, generates longer development cycles. Generally, developers have the full power of programming languages with some limitations to offer better scalability and security. In this situation, the conventional development environments are used to design and develop applications which are then deployed on the cloud by employing the APIs exposed by the PaaS provider For better utilizing the services given by the PaaS environment, specific components can be provided together with the development libraries.

PaaS implementation

PaaS solutions simply provide users with the software that is installed on the user's premises, or can provide a middleware for developing applications together with the infrastructure. In the former case, the middleware forms the core value of the offering. In the latter case, the PaaS provider also has large da la centers where applications are run. It is also possible to have vendors that provide both middleware and infrastructure and provide also only the middleware for private installations. Pass solutions are classified into three main categories - Pass-I, Pass-II, and Pass-Ill.

Pass-I category recognizes PasS implementations that entirely follow the cloud computing style for application development and deployment. The prov ide an integrated development environment hosted within the Web browser in which applications are designed, composed, developed and deployed. For example, Longjump and Force.com. Both of them provide the combination of middleware and infrastructure as a platform. In Pass-II category, all solutions that emphasize on offering a scalable infrastructure for Web applications are listed. Here, the providers APIs are used bv the developers to develop applications. In pass-ll category, the most popular product is Google App Engine. This product offers a expandabel runtime on the basis of java and python programming language that have been improved with additional APIs and components to support scalability and modified for offering a secure runtime environment. An open source implementation of Google AppEngine is AppScale. Appscale offers an interface compatible middleware that has to be installed on a physical infrastructure. A similar approach to Google AppEngine is provided by Joyent Smart Platform. Engine Yard and Heroku take different approach that offer scalability support for ruby. Pass-Ill category comprises all solutions that render a cloud programming platform for any sort of applications. Microsoft WindowsAzure is the most popular solution among these. It offers a framework on top of the .NET technology for building service-oriented cloud applications. In this category, other solutions are Manjrasoft Aneka, DataSynapse, Apprenda SaaSGrid, GigaSpaces DataGrid and Appistry Cloud IQ platform. All these solutions offer only a middleware with different services. Table shows a platform-as-a-service offering classification.

Characteristics of PaaS

Some essential characteristics of a PaaS solution are as follows

(i) **Automation** - PaaS environment automates the process of deploying applications to the infrastructure, and scaling them when required by provisioning extra resources. This process is carried out automatically and according to the SLA created between the customers and the provider. This characteristic offers ways to provision more resources.

(ii) **Abstraction** - The higher level of abstraction differentiates the PaaS solutions In PaaS, the concentration is on the applications the cloud must assist. It means PaaS solutions provide an approach to deploy and manage applications on the cloud instead of a bunch of virtual machines

(iii) **Cloud Service**- To help architects and developers to simplify the creation and delivery of elastic and highly available cloud applications, PaaS offerings provide them with APIs and services. Among competing PaaS solutions, these services are the main differentiator and generally entail certain components for developing applications, management, reporting, and advanced services for application monitoring. The ability to integrate third-party cloud services for application monitoring from other vendors by using service-oriented architecture is another important component for a PaaS based approach. This opportunity makes the applications development able to evolve as required by the customers and users, and able to move quickly and easily.

(iv) **Runtime Framework** - In PaaS solutions, this is the most intuitive characteristics and represents the software stack ol the PaaS model. The end user code is executed by the runtime framework on the basis of the policies defined by the user and the provider.

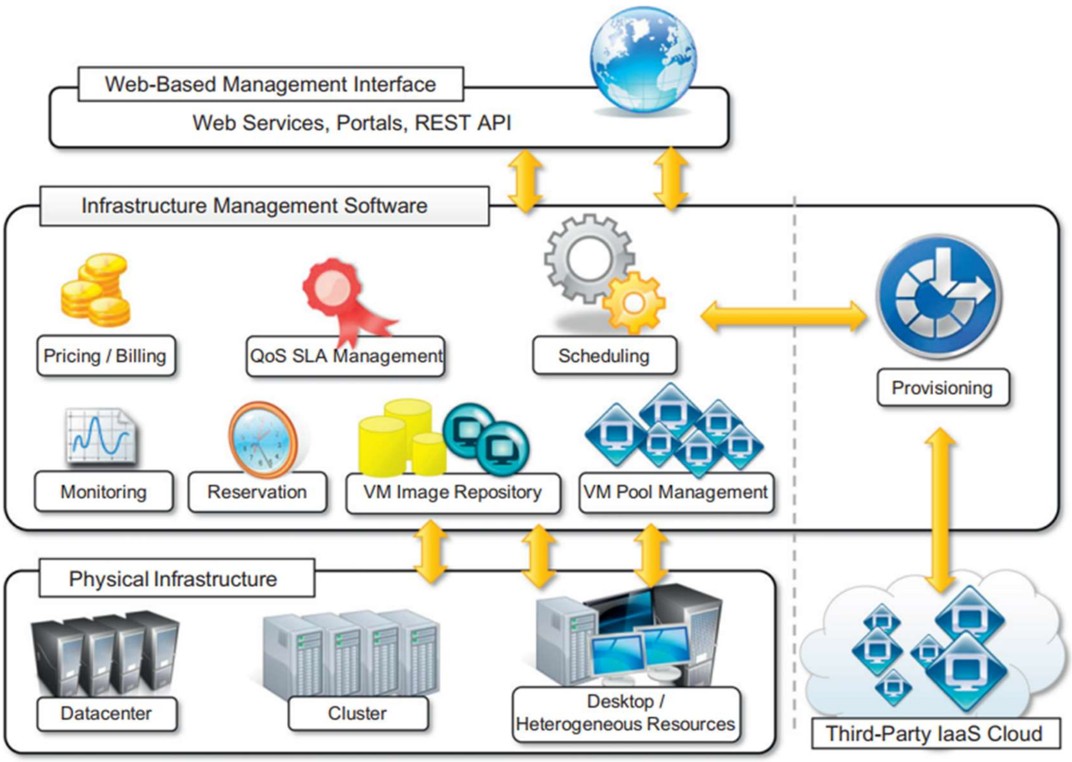
IaaS solution

Infrastructure/Hardware as a service solutions are the most popular. They provide customizable infrastructure on demand and build market segment of cloud computing. The available alternatives within the IaaS-offering umbrella are database, Web servers, load balancers and network devices from single servers to entire infrastructures. Hardware virtualization is the main technology used to provide and implement these solutions. In hardware virtualization, one or more virtual machines are suitably configured and interconnected that define the distributed system on top of which applications are installed and deployed. Virtual machines also form the atomic components. These components are deployed and priced depending on the memory, disk storage and number of processors. The advantages of hardware virtualization are sandboxing, hardware tuning, workload partitioning and application isolation. All these advantages of hardware virtualization are provided by IaaS/HaaS solutions. IaaS/HaaS solutions decreases the administration and maintenance cost, and the capital costs from the view point of the customer. It also enables better exploitation of the IT infrastructure and offers a more secure environment for executing third-party applications from the view point of the service provider. Simultaneously, users can take benefit of the full customization provided by virtualization to deploy their infrastructure in the cloud. Virtual machines mostly come with the selected

OS installed and the system can be configured with all the needed packages and applications. Apart from the basic virtual machine management capabilities, some other services can be offered. These services are workload management, SLA resource-based allocation, ability to integrate third party laaS solutions, and support fer infrastructure design through advanced Web interfaces.

Component of IaaS-based solution

The basic components of an IaaS-based solution are shown in fig. 2.2. Here, the physical infrastructure, the infrastructure management software and the Web based management interface or user interface are the three principal layers



The bottom layer is set up by the physical infrastructure. The management layer works on top of the physical infrastructure. The infrastructure can be of various types and the use of particular infrastructure relies on the specific use of the cloud. A service provider will probably use a large data center that has several number of nodes. A cloud infrastructure will depend on a cluster whether it is developed in house, in a small or medium organization or within a large department. It is also possible at the bottom of the scale to consider a heterogeneous environment where various types of resources such as PCs, clusters and workstations can be aggregated. The physical layer also incorporates the virtual resources that are rented from external IaaS providers from an architectural point of view.

In the infrastructure management software layer, the main features of an IaaS solution are implemented. The most prominent function carried out by this layer is the management of the virtual machines. The scheduler plays a central role, who is responsible for allocating the execution of virtual machine instance The scheduler interacts with the other components to carry out several other

tasks. A QoS/SLA management component will maintain a repository of all the Service Level Agreements (SLAs) done with the users and together with the monitoring component is used to make sure that a given virtual machine instance is executed with the required Quality of Service (QoS). The pricing/billing component takes care of the cost of executing each virtual machine instance and stores data that will be used to charge the user. The monitoring component records the execution of each virtual machine instance and stores data needed for analyzing and reporting the system performance of the system. The reservation component records the detail of all the virtual machine instances that have been executed or that will be executed in the future. The VM repository component offers a catalog of virtual machine images that are used by the users to produce virtual instances. A VM pool manager component maintains track of all the live instances. A provisioning component interacts with the scheduler in order to offer a virtual machine instance that is external to the local physical infrastructure, if the system supports the integration of additional resources related to a third-party IaaS provider.

At the top layer, the user interface offers access to the services exposed by the management layer. Generally, this type of interface depends on Web 2.0 technologies, which enable either applications or final users to access the services exposed by the underlying infrastructure. Web 2.0 applications permit developing full-featured management consoles fully hosted in a Web page or a browser. Without the human intervention, RESTful APIs and Web services enable program to interact with the service. Hence, offering complete integration within a software system.

Application level security in SaaS, PaaS, IaaS

Application or software security should be a critical element of a t security program. Most enterprises with information security programs have yet to institute an application security program to address this realm. Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reevaluate current practices and standards. The application security spectrum ranges from standalone single- user applications to sophisticated multiuser e-commerce applications used by many users. The level is responsible for managing -

(i) SaaS application security i

(ii) PaaS application security

(iii) IaaS application security

(iv) Application-level security threats

(v) End user security

(vi) Customer-deployed application security

(vi.) Public cloud security limitations.

Application Security in a SaaS - SaaS vendors provide the infrastructure and applications to users on the pay-per-use model. The cost per month paid to the SaaS provider is based on the modules selected, number of user accounts, and amount of utilization of the application.

Application Security in PaaS - PaaS vendors provide the infrastructure, application building blocks, compilers, and a runtime environment to develop and host applications. These blocks could be similar to those used internally within an enterprise; however, one needs* to code certain security in applications in order to cover multi-tenancy and thousands of users who have potential access to the platform. Application security has been a problem long before the arrival of PaaS. Some of the ways to protect data in a PaaS environment are as follows

(a) *Testing for Vulnerabilities* - Several tools have been developed to identify application vulnerabilities. Some good ones are described at the Open Web Application Security Project (OWASP) site (http:/ www.owasp.org). It lists several, battle tested tools, to protect the Web based applications from security threats. These can be effectively used to harden the cloud applications. OWASP is a non-profit organization, dedicated to improving application security by providing tools and best practices to discover design and implementation defects and to protect against the flaws.

(b) *Tools* - The cloud provider should be able to provide tools to identify security issues and scan Web pages. You must continuously scan Web pages for common security issues such as XSS and SQL injections.

(c) *Logs* - All activity and security events must be logged and the data must be protected through encryption. The log must be regularly scanned for indications of security threats.

(d) *Application Keys* - All API calls to the platform or services within must require an application key. The cloud application must have provisions to maintain and secure the key along with the other credentials.

(e) *Secure Protocols* - For Simple Object Access Protocol (SOAP) based messages, secure protocols such as Web services security must be used. It provides a foundation for implementing security functions such as confidentiality and integrity for Web based application. It is maintained by OASIS (Organization for the Advancement of Structured Information Standards), an international, non-profit consortium, which is focused on open standards adoption for applications. Cloud applications must use Secure Socket Layer (SSL), whenever possible.

(iii) *Application Security in an IaaS* - For application within an enterprise, several internal controls exist to protect the data. In a cloud, the corresponding security controls must be coded within the application. This section describes the security aspects for application developed in IaaS environment. In this service providers create virtual machines (VM'S) with internal or external storage devices. To meet the various types of security requirements, and mitigate incessant threats, IaaS providers offer special security tools to help application developers improve security and meet compliance requirements. These tools can be used to identify and block several threats. These include the following-

(a) *dWAF*- It allows a set of rules to be applied to Web-h j, communication to accept or drop packets based on port number, sour ' destination IP addresses, and other parameters.

(b) *Host-based Intrusion Detection Systems (HIDS)* monitors and reports if any user or application has circumvented the IaaS host security policy.

(c) *Host-based Intrusion Prevention Systems (HIPS!* - monitors each IaaS host for suspicious activities by analyzing the even- within the host and takes steps to stop such activity. It blocks the malicious activity by dropping the bad packets, resetting the connection, or entirely blocking traffic from the offending IP address or network to and from the IaaS host.

Advantage & Disadvantage of the service in clouds

The advantages and disadvantages of the services on the cloud as follows -

Advantages of IaaS -

(i) Quick addition of capacity - elastic to grow and shrink as capacity requirements change.

(ii) Most hardware, network and data center infrastructure costs are eliminated.

(iii) Lower labor costs are network infrastructure costs, data center costs are ongoing facility maintenance costs are omitted.

(iv) High availability Internet connections from hosting provider.

(v) Allows existing applications to be moved into the cloud with a minimum of modification.

Disadvantages of IaaS -

(i) Perceived loss of control of assets and physical security.

(ii) Network outages (local connection to Internet or the Internet itself) means complete service loss.

(iii) More Internet bandwidth required from facilities.

(iv) Possible loss of logical security, concerns of information leakage from one customer to another.

(v) Compliance auditing (i.e. SBOX) may become more complex as there is no direct control of assets located within cloud.

Advantages of PaaS -

(i) Quick addition of capacity - elastic to grow and shrink as capacity requirements change.

(ii) Hardware, network and data center infrastructure costs are eliminated.

(iii) Some software costs (OS and support software) are eliminated.

(iv) Initial pre-configuration of core-OS and some support software is eliminated.

(v) High availability Internet connections from hosting provider.

Disadvantages of PaaS -

(i) Less application flexibility as applications must conform to predefined platform template.

(ii) Only certain types of applications are suited for this model, depending on specifies of platform.

(iii) Less portability of existing applications as constrained to a single pre-defined platform configuration.

(iv) Same security/auditing/network bandwidth and dependency concerns as with IaaS.

(v) Provider "lock-in", portability of applications between providers may prove difficult.

Advantages of SaaS - .

(i) Easy and quick setup, often by non-technical people on demand

(ii) Easy and quick tear down, on demand when need for the for the application subsides

(iii) No long-term contracts means can be used for short-term in bursting.

(iv) Low per-user cost.

(v) Low client requirements.

Disadvantages of SaaS -

(i) May run slower when Internet in heavily loaded.

(ii) Often "one size fits all" customization/flexibility are limited.

(iii) Provider "lock in" is very likely, difficult or impossible to switch vendors.

(iv) Security is a concern, data leakage for example.

(v) Ability to audit and traceability are concerns.

Use of SaaS, PaaS, IaaS

(i) **Infrastructure as a Service (IaaS)** - The infrastructure as a service layer was based on virtualization technology and provides the basic computing infrastructure of servers, processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications and possibly limited control of select networking components.

The main purpose of IaaS is to avoid purchasing, housing and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface (which reduces hardware costs).

Customers arc allocated computing resources in order to run virtual machines consisting of operating systems and applications.

(ii) **Platform as a Service (PaaS)** - Platform as a service adds a higher level to the cloud infrastructure by providing a platform upon which applications can be written or deployed. These servicc providers offer, in this layer, application programming interfaces (APIs) that enable developers to exploit functionality over the Internet rather than delivering complete applications. It delivers development environments to programmers, analysts and software engineers as a service. PaaS gives end users control over application design, but does not give them control over the physical infrastructure. In these services, customers may interact with the software to enter and receive data, perform actions, get results and to the degree that the vendor allows it customize the platform involved.

The main purpose of PaaS is to reduce the cost and complexity of buying, housing and managing the underlying hardware and software components of the platform, including any needed program and database development tools. PaaS gives end users control over application design, but does not give them control over the physical infrastructure.

(iii) **Software as a Service (SaaS)** - Software as a servicc provides the consumer with typical software applications that run over the cloud computing infrastructure. SaaS delivers applications through a web browser to thousands of customers rather than installed on their computer. The end user does not exercise any control over the design of the application, servers, networking, and storage infrastructure.

The main purpose of SaaS is to reduce the total cost of hardware and software development, maintenance and operations. All these services offer scalability and multitenancy. In addition, they arc self-provisioning and can be deployed through public cloud deployment modules.

Examples of these three modes of cloud computing are given in table.

Examples - Amazon's elastic compute cloud (EC2) is a prominent example for an IaaS offer. It offers the user a virtual server, with the CPU, memory, storage, operating system and hypervisor or system monitoring software included.

(a) Google App Engine - Is an example for a Web platform as a service (PaaS) which enables to deploy and dynamically scale Python and Java based Web applications.

(b) Google Apps - Provides Web-based office tools such as e- mail, calendar, and document management.

(c) Rackspace Cloud - Is a cloud IaaS. It provides users with access to dynamically scalable computing and storage resources, as well as third-party cloud applications and tools.

(d) Salcsforce.com - Is a cloud SaaS. It provides a full customer relationship management (CRM) application.

(e) Zoho.com - Is a cloud SaaS. It provides a large suite of Web-based applications and it is used often by organizations.

Attributes	*SaaS*	*PaaS*	*IaaS*
Service providers	Google apps, Office live, G-mail, Facebook	Azure, Netsuite, Amazon web services	IBM, Amazon EC2, Xen SalesForce.com
Runtime management	By the customers	By the vendor	By the vendor
Data management	By the customers	By the developer	By the vendor
Application management	By the customers	By the developer	By the vendor
Used by	Business users	Developers and deployers	System manager
Visibility	End users	Application developers	Network architects
Type of services	Dynamic infra-structure service	Integration as a service	Dynamic application services
No of providers	Large numbers of application in the cloud	Few cloud platforms	Elite group of providers
Server management	By the vendor	By the vendor	Small

Architecture of Virtual desktop infrastructure

End-user virtualization solutions are provided by virtual desktop infrastructure. VDI is designed to convert distributed IT architectures into virtualized, open-standards-based frameworks leveraging centralized IT services. The software, hardware and services are combined by VDI to connect your clients authorized users to platform independent, centrally managed applications and full desktop images running like virtual machines that run on servers in the data center. An idea behind the VDI is to run applications and desktop operating systems inside virtual machines that keep on servers in the data center. This is known as virtual desktops. From a desktop PC client or thin client, users access virtual desktops and applications with the help of a remote display protocol. The desktop users get all local desktop features as if the applications were installed on their local systems, but the applications are centrally managed and hosted.

VDI solution is made up of thin client, optional portal interface, and PC with client components or Web browsers with client messaging and security technologies, provided via a single, consistent framework This solution offers authorized users with single-point, consistent access from a variety of choices of client devices and provides a general, standards-based, resilient H infrastructure that is security-rich and expandable

Key component of Virtual desktop infrastructure (VDI)

The three key components of virtual desktop infrastructure are host, connection broker and end points.

Advantage & disadvantages of Virtual desktop infrastructure (VDI)

Advantages of VDI - VDl makes a framework that provides several benefits to the enterprise, which are as follows -

(i) **Reduction in Cost**-The utilization can be increased by making use of resources in an efficient way.

(ii) **Security** - The data is still in the data center with access control.

(iii) Efficiency - When IT processes are optimized for a centralized environment, service delivery is more efficient.

(iv) **Availability** - In the case of a hardware failure, virtual machines are quickly moved to different physical server, therefore availability is higher.

(v) **Flexibility** - A number of end users are supported by common physical infrastructure. Without a hardware procurement cycle, new desktop images can be produced dynamically. The virtual machines can allow the execution of different types of guest operating systems. Hence the physical hardware can assist a large range of end users with economically integration or reconfiguring the systems between user accesses.

Disadvantages of VDI - There are three disadvantages of VDI

(i) Administrators should know about limitations and capabilities

of VDI software.

(ii) Virtual desktop infrastructure huge investment in server

hardware, network and storage infrastructure.

(iii) Many users can use same server or same image, any server-side problems can affect these users. So it is required to maintain redundant servers.

Access virtual desktop

The remote desktop client devices of users are used to connect to their virtual desktops. VMware Virtual Desktop Manager (VDM) offers this service. It is an enterprise-class connection broker product and is a component of VMware virtual desktop infrastructure. Remote clients are connected to the centralized virtual desktops by VMware View. This process is usually referred to as connection brokering. VMware View manages the logic controlling

which virtual desktop a client should connect. This makes the process of connecting to VMware View simple Tor the end user and tightly controlled lor the IT administrator. An existing PC runn.ng MS Windows is used by the end users where the user initiates a remote session to a View resource using a remote desktop client application, or a Web browser. You might have oca' desktop icons configured to access published applications or published desktops with some third-party products.

Pool management for VDI

Virtual Desktop Manager (VDM) authenticates the users and determines the pool they relate to. VDM using predetermined policies provision a desktop for that end user, competes with that user's specifications and privileges - and deploys it. These pools can be of two types non-persistent and persistent. Non-persistent pools have multiple hosted virtual desktops that are initially identical and cloned from the similar template. From the non- persistent pool, the VDM connection server allocates entitled users to a virtual desktop as needed. However, when the user logs off, this allocation is not retained and the virtual desktop is kept back into the non-persistent pool for reallocation to other entitled users. The user is connected by the VDM connection server to any virtual desktop in the non-persistent pool when the user connects to the non-persistent pool on subsequent occasions. In contrast to the non-persistent pool, the persistent pool has multiple hosted virtual desktops that are initially identical since they are cloned from the similar template Typically, it is a many-to-many relationship. Every user in the group is entitled to any of the virtual desktops in the pool when a group of users are entitled to the persistent pool. Users are allocated by the VDM connection server to a virtual desktop as needed. For subsequent connections, this allocation is retained.

A static, one-on-one relationship between a user and a specific virtual desktop is known as individual desktop assignment. This configuration can entail data access, resource allocations and particular applications. This configuration is suitable for power users where the desktop is specifically configured for a specific user. A high degree of customization is provided to users by individual desktops. The security-rich, 'anytime, anywhere' access to applications, information, and resources is achieved with the help of a virtualized IT environment. Virtual Desktop Infrastructure (VDI) is a unique end-user virtualization solution which assists businesses convert their distributed IT architectures into virilized, open-standards-based frameworks leveraging centralized II services. The software, hardware and services are combined by VDI to connect authorized users to platform-independent, centrally managed applications and lull client images running in virtual machines.

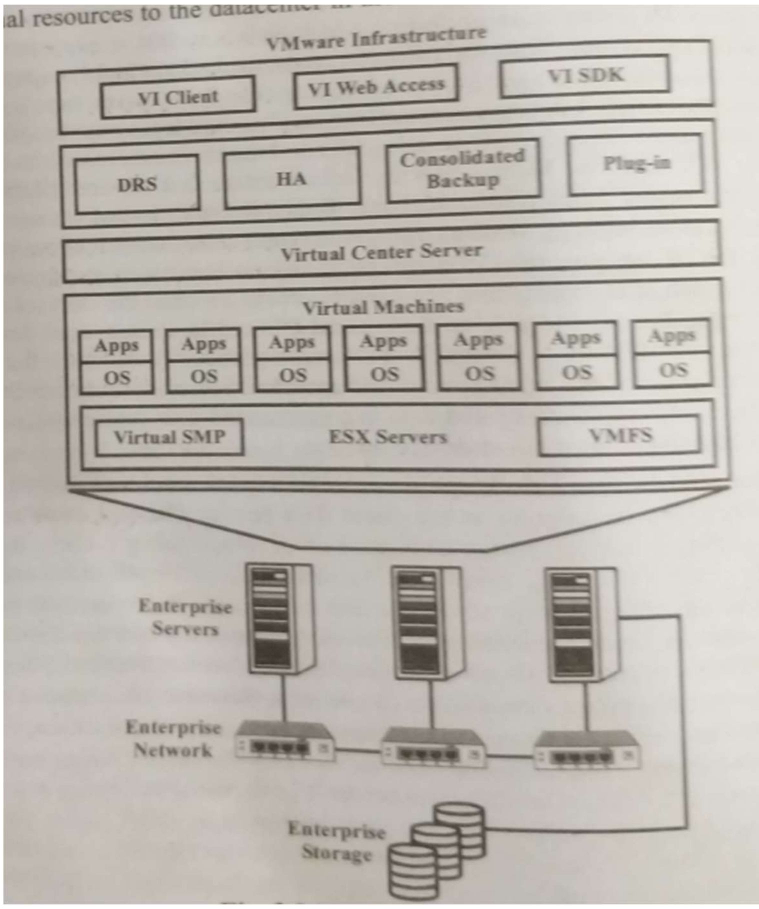
The total cost of ownership can be considerably decreased by desktop clou, project-based service with the help of reduced effort needed for desktop PC deployment and management, software distribution desk-side support and help-desk needed to support and maintain desktops. VDI also provides managed services for businesses that want to derive advantages of virtual infrastructure access but scares the necessary skills and expertise needed for the ongoing management of the virtual infrastructure.

VMware infrastructure in details

VMware infrastructure is a full infrastructure virtualization suit that provides comprehensive virtualization. Management, resources optimization, application availability, and operational automation capabilities is an integrated offering. VMware infrastructure virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the datacenter in the virtual environment

In addition, VMware infrastructure brings about a set of distributed services that enables fine-grain, policy-driven resource allocation, high availability, and consolidated backup of the entire virtual datacenter These distributed services enable an IT organization to establish and meet their production service level agreements with their customers in a cost-effective manner.

The relationships among the various components of the VMware infrastructure are shown in fig.



VMware infrastructure includes the following components shown in fig.

(i) **VMware ESX Server**- A robust, production-proven virtualization layer run on physical servers that abstracts processor, memory, storage, and networking resources into multiple virtual machines. There are different versions of ESX Server. ESX Server 3 is installable software that is purchased separately from physical hardware. ESX Server 3i is embedded by the original equipment manufacturer (OEM) in the physical hardware.

(ii) **Virtual Center Server** - The central point for configuring, provisioning, and managing virtualized IT environments.

(iii) **VMware Infrastructure Client (VI Client)** - An interface that allows users to connect remotely to the virtual center server or individual ESX servers from any windows PC.

(iv) **VMware Infrastructure Web Access (VI Web Access)** - A Web interface that allows virtual machine management and access to remote consoles.

(v) **VMware Virtual Machine File System (VMFS)** - A high- performance cluster file system for ESX Server virtual machines,

(vi) **VMware Virtual Symmetric Multi-processing (SMP)** - Feature- that enables a single virtual machine to use multiple physical processors simultaneously.

(vii) **VMware VMotion and VMware Storage VMotion-** VMware VMotion enables the live migration of running virtual machines from one physical server to another with zero down time, continuous service availability, and complete transaction integrity. VMware Storage VMotion enables the migration of virtual machine files from one datastore to another without service interruption.

(viii) **VMware High Availability (HA)** - Feature that provides easy-to-use, cost-effective high availability for applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other production servers that have spare capacity

(ix) **VMware Distributed Resource Scheduler (DRS)** - Feature that allocates and balancing computing capacity dynamically across collections of hardware resources for virtual machines. This feature include distributed power management (DPM) capabilities that enable a datacenter to significantly reduce its power consumption

(x) **VMware Consolidated Backup (Consolidated Backup)** - Feature that provides an easy-to-use, centralized facility for agent-free backup of virtual machines. It simplifies backup administrate and reduces the load on ESX servers.

(xi) **VMware Infrastructure SDK** - Feature that provides a standard interface for VMware and third-party solutions to access the VMware infrastructure.

Scalability and Fault Tolerance

The ability to scale on demand constitutes one of the most attractive features of cloud computing. Clouds allow scaling beyond the limits of the existing in-house IT resources, whether they are infrastructure (compute and storage) or applications services. To implement such a capability, the cloud middleware has to be designed with the principle of scalability along different dimensions in mind—for example, performance, size, and load. The cloud middleware manages a huge number of resource and users, which rely on the cloud to obtain the horsepower that they cannot obtain within the premises without bearing considerable administrative and maintenance costs. These costs are a reality for whomever develops, manages, and maintains the cloud middleware and offers the service to customers. In this scenario, the ability to tolerate failure becomes fundamental, sometimes even more important than providing an extremely efficient and optimized system. Hence, the challenge in this case is designing highly scalable and fault-tolerant systems that are easy to manage and at the same time provide competitive performance.

IaaS = Infrastructure as a service

PaaS = Platform as a service

SaaS = Software as a service

AaaS = Analytics as a service

BaaS = Backend as a service

FaaS = Function as a service

DaaS = Data as a service

STaaS = Storage as a service

CaaS = Container as a service

NaaS = Network as a service

DBaaS = Database as a service

AaaS =Authentication as a service

aPaaS = Application platform as a service

iPaas = Integration platform as a service

apimPaas = API management PaaS API

IoT PaaS = Internet of Things PaaS

mPaaS = Mobile PaaS

dbPaaS = Global Database PaaS

UIPaaS = User Interface PaaS

XaaS = Everything as a service

1. Infrastructure as a service (IaaS)

- It includes CPU processor, memory, storage, network, and other computing resources that users can rent through virtualization technology
- Users can deploy and run any software including operating systems and application software.
- But users do not have the right to manage and access the underlying infrastructure such as servers, switches, memory, etc
- Users can control the choice of operating systems, storage space, application software, and network components.
- DigitalOcean, Linode, Rackspace, Amazon Web Service (AWS), Cisco Metacloud, Microsoft Azure, Google Compute Engine (GCE)

2. Platform as a service (PaaS)

- It provides users with the ability to use development tools, libraries, and services supported by service providers to create and develop applications. For example, it can provide complete desktop and mobile software development kits (SDKs), rich development environments, fully managed database service, configurable applications, program construction, and support for multi-language development.
- Users can deploy applications they developed or acquired
- Users do not manage the underlying infrastructure (networks, servers, operating systems, storage, etc)
- Users can control the deployed application and the configurable parameters of the environment in which the application is hosted.
- It includes database services, web applications, and container services
- AWS Elastic Beanstalk, Windows Azure, Heroku, Salesforce.com, Google App Engine, OpenShift

3. Software as a service (SaaS)

- Users can access it through a client interface such as a browser, on various devices
- Any application on a remote server can be run through the network, which is SaaS.
- Users do not need to manage the underlying cloud infrastructure, including networking, servers, operating systems, storage space, and even individual application functions,
- However, users can have an application with limited user-specific configuration settings.
- Google workspace, Dropbox, Salesforce, Cisco WebEx, SAP Concur, GoToMeeting, etc

4. Analytics as a service (AaaS)

- Turning data into insights to drive business decisions with big data and AL/ML technology
- It is one of the fully customized data analytics software to process and analyze a large amount of information
- Outlier

5. Backend as a service (BaaS)

- It provides mobile application developers that integrate cloud backends
- It provides storage and hosting environments as well as some common back-end technical capabilities such as push.
- Users no longer manage all server-side components
- Supabase

6. Function as a service (FaaS)

- Users can develop, run, and manage application functionality without the complexities of building and maintaining the infrastructure.
- It is a serverless architecture for building microservice applications
- It is an event-driven approach that integrates various synchronous and asynchronous event sources
- Google Cloud Functions, AWS Lambda

7. Data as a service (DaaS)

- It provides a centralized management service for data resources and scenario-based data
- Data is either scattered in various teams or departments and could not be used to improve business operation efficiency.
- Users can purchase data they need from other companies or industries to improve their competitiveness
- Snowflake, Oracle

8. Storage as a service (STaaS)

- It provides users to offload their data to a reliable storage system
- HPE GreenLake for storage

9. Container as a service (CaaS)

- The software code is packaged in a container so that it can be read and run anywhere
- Libraries, code, and dependencies are packaged in a container
- Portainer

10. Network as a service (NaaS)

- It provides integrated hardware, software, licensing, and support services in a flexible network delivery service
- Users only pay for network services as needed
- Virtual private network, bandwidth-on-demand, and delivery optimization
- Perimeter81

11. Database as a service (DBaaS)

- It provides the snapshot technology to provide short-term backup services ranging from 0 to 30 days
- It simplifies and automates database management and operations
- The parsing engines and storage are separated
- Nutanix Era, Oracle Autonomous Database, IBM Cloudant

12. Authentication as a service (AaaS)

- It provides users access control solution
- It converts user registration, login, user management, authentication, and authorization modules into SaaS services
- It control who can use the product across devices and networks
- Thales

Everything platform as a service (xPaaS)

1. Application platform as a service (aPaaS)

- It supports the development, deployment, testing, and operation of - applications in the cloud
- It provides development tools to users, including data objects, rights management, user interface, etc
- It is low-code or zero-code so that non-programming background personnel can complete application development

2. Integration platform as a service (iPaaS)

- It facilitates the development, execution, and integration of flow governance with any on-premises and cloud-based processes, services, applications, and data integration.
- It is a set of automated tools that integrate software applications that are deployed in different environments.

3. API management Platform as a service (apimPaaS)

- It provides a solution for API authority so that developers can utilize a robust portal to create products, and enforce policies

4. Internet of Things Platform as a service (IoT PaaS)

- It turns data collected from IoT to trigger IoT devices to be intelligent with big data and AL/ML technology

5. Mobile Platform as a service (mPaaS)

- It provides solutions for Application development, testing, operation, and maintenance.
- It reduces R&D costs and improves development efficiency

6. Database Platform as a service (dbPaaS)

- It is any database management system (DBMS) or data storage, designed as a scalable, elastic, multi-tenant subscription service, with certain self-management capabilities, and by cloud service providers (CSP)
- It provides an option for those companies that are unable or unprepared to migrate to public cloud offerings

7. User Interface PaaS (UIPaaS)

- It provides many kinds of components so that users can configure the main frame, page layout, and menu of the mobile terminal interface in a zero or low-code method

Question BANK UNIT 3

1. Define virtualization. Also the benefits of virtualization

Or

What is the need of virtualization? Explain in brief

2. Discuss the architecture of a compute system before and after virtualization

3. Write down the comparison between virtualization and cloud computing

4. Discuss the architecture of Hyper-V and discuss its use in cloud computing

5. What do you mean by hypervisor virtual machine(HVM)

Or

Explain what do you understand by hypervisor management software and their requirements

Or

Explain virtualization hypervisor management software

Or

Write a detail note on hypervisor management software

6. Describe different types of hypervisor with example and block diagram.

7. Write the difference between block and file level storage virtualization

Or

Differentiate between block level storage and file level storage

Or

Write in brief about block and file level storage virtualization

Or

Write a note on block level storage virtualization and file level storage virtualization in detail

Or

Discuss the various levels of virtualization implementation

8. Discuss VLAN and VSAN

Or

Differentiate between VLAN and VSAN

Or

Explain virtual LAN and virtual SAN in cloud computing

9. Short note on

Map reducer

Cloud Governance

Unit 3: Cloud Management & Virtualization Technology

Resiliency
Provisioning
Asset management
Concepts of Map reduce
Cloud Governance
High Availability and Disaster Recovery.

Virtualization: Fundamental concepts of compute, storage, networking, desktop and application virtualization
Virtualization benefits
server virtualization
Block and file level storage
virtualization Hypervisor management software
Infrastructure Requirements
Virtual LAN(VLAN) and Virtual SAN(VSAN) and their benefits

High Availability (HA)

High Availability refers to removing single failure points. "High availability refers to a system or component that for a long period is continuously operational." This could mean anything as simple as configuring several discs as a RAID for storage, or it could mean multiple redundant storage systems and servers, designed to provide reliable and continuous uptime for storage.

It must be capable of enduring failures at various levels of the solution for a solution to truly be deemed highly available. This involves internal hardware, software, and networking, but is not constrained.

Disaster Recovery (DR)

If a system fails, recovering from the incident quickly is always essential for an organization, and this is where the idea of disaster recovery comes into play.

Disaster recovery is a strategy that "allows an organization to maintain or quickly resume mission-critical functions after a disaster." IT organizations need features that enable data backup or automate the reconstruction of infrastructure, thus incurring minimal downtime, to be able to recover from a catastrophic event. This enables companies to sustain the productivity levels expected.

The Need for High Availability (HA) and Disaster Recovery (DR)

To guarantee business continuity, it is necessary to use both high availability AND disaster recovery technologies. High availability, as defined, protects us from day-to-day events that can affect device availability, such as hardware failure, network failure, load-induced failure, or other failures of the application. Having processes and technologies of high availability in place to ensure that these types of failures result in either limited or no effects, results in a highly accessible system. Disaster recovery comes into play when, as a consequence of natural disasters, user-induced data loss, security breaches, or site-wide failures, a significant outage is encountered.

We have resilient backups available to recover data in a disaster situation, resulting in data loss, by obtaining backups of business-critical systems and holding offsite DR copies. In a system-wide catastrophe where an entire site could be offline, replication ensures we are safe. In the event of the main production site going down, resources can be diverted to the DR site by replicating virtual machines to a DR facility. In business-continuity planning, both high availability and catastrophe recovery are extremely significant. In the event of a major catastrophe, each plays a vital role in ensuring both day-to-day uptime and data recoverability.

Key Elements of High Availability and Disaster Recovery

Distributed Approach

This approach suggests that the business control room and the enterprise customers on different computers, in addition to clustering automation everywhere and relevant data centre components.

The enterprise control room is fairly versatile to accommodate a large number of requests. Deploy multiple enterprise control room or enterprise client instances on multiple physical or virtual servers, as necessary.

Load Balancing

This is the method of spreading application or network traffic across multiple servers to protect service operations conducted by a load balancer and enables workloads to be spread across multiple servers. It ensures that all operations continue on clustered servers.

Databases

To protect the data, databases use their built-in failover. This allows data recovery from databases.

Set up synchronous replication between the main (active) and secondary (passive/standby) clustered MS SQL servers in the data centre between the HA clusters. In the event of a database node failure, this ensures consistency.

Configure the database between the DR sites to provide asynchronous replication from the primary DR site (production) to the secondary DR site (recovery) that is at a geographically separated location from the primary DR site.

Cloud Governance

Cloud governance is a set of policies and rules used by companies who build or work in the cloud. This framework is designed to ensure data security, system integration and the deployment of cloud computing are properly managed. Since cloud systems are dynamic, involving third-party vendors or different teams within your business, cloud governance solutions must be adaptable.

A cloud governance framework done right will manage risks, enhance data security and enable cloud systems operations for your business. This method of cloud computing governance for IT balances resource and risk with a focus on accountability. Without cloud governance you run the risk of poor integration of cloud systems and a lack of alignment with business goals and face new security issues associated with deploying cloud systems.

Cloud Governance Benefits

A good cloud governance framework can provide your business with the following benefits:

- Improves management of resources so there is no overlap for different teams working separately in the cloud.
- Improves cloud security issues by having comprehensive rules and protections in place designed to thwart cybercriminals.
- Helps curb shadow IT — the use of applications, software and services without approval from the IT department.
- Reduces administrative overhead and labor when cloud computing follows the same rules across your entire business.
- Whether your business uses the public cloud or private cloud, cloud security provided by cloud computing governance is vital. Ensuring that your business aligns with the principles of cloud governance is a step toward smooth cloud operations.

Setting Up a Cloud Governance Framework

There are three steps involved in setting up a cloud governance framework for your business.

Define Controls: Define your controls, both financial and operational. This can involve following regulatory rules such as HIPAA, limiting the number of cloud instances you use and deciding who has clearance to make changes to your cloud computing environment.

Implement Controls: Once you have a policy document defining the rules to fit your business needs, implement those controls. Communicate with teams and employees and optionally use third-party tools to help you implement controls.

Audit Controls: Continuously monitor controls to make sure you are doing all the right things the right way and monitoring them the right way.

6 Principles of Cloud Governance

Controls can be designed to prevent an issue, detect an issue after it occurs, or correct an issue that has already taken place.

When considering controls, you should take into account 6 principles of cloud governance:

1. Financial Management: This principle revolves around creating and implementing a strategy for governance structure to address cloud inefficiencies and higher cloud costs. Which third-party vendor you use and whether you work in the public or private cloud can have an impact. Investing time into financial management helps you understand the costs of the cloud.

2. Cost Optimization: Alongside financial management, measuring, monitoring and optimizing cloud costs is an important principle of the cloud governance framework. The procedures and tools involved in cost optimization can enable your business to manage cloud spend while maximizing cloud investment.

3. Operational Governance: For cloud computing, operational governance is designed to enhance data security, enable smooth cloud operations and manage risks. This helps your business state policies as business processes and enforces these policies throughout your business.

4. Performance Management: This is used to find out how well your cloud system is functioning and identify places for improvement. Performance management cares about the actual performance of hardware and virtual systems and checks workload and memory usage.

5. Asset and Configuration Management: Asset management involves the assets your business uses to deliver IT and cloud services. Configuration management involves tracking the relationship between IT or cloud service components. Together this principle monitors cloud services and deliverables to ensure consistency and quality.

6. Security and Incident Management: Ensuring your cloud operations are secure and having a plan to react should a breach occur are vital for working in the cloud. Cloud security posture management (CSPM), which identifies and remediates risk using threat –detection, uninterrupted monitoring and automating visibility, is a good framework to

use. Searching for misconfigurations in cloud environments can help bolster public, private and hybrid cloud security.

Map reducer

The concept of MapReduce is introduced by Google. MapReduce is a programming platform to process huge amount of data. Here, map and reduce are the two simple functions used to represent the computation logic of an application. The distributed storage infrastructure completely handles the data transfer and management. Distributed storage infrastructure is in-charge of providing access to data, replicating files and finally moving them where required. Hence, these issues are not handled anymore by developers and are offered with an interface which offers data at a higher level like a collection of key-value pairs. Then, the MapReduce applications computation is arranged in a workflow of map and reduce operations. These operations are fully managed by the runtime system, and developers have only to mention how these operations work on the key-value pairs. The MapReduce programming model is represented in the form of the two functions – map and reduce. These functions are written as -

map (kl, vl) list (k2, v2)
reduce (k2, list (v2)) -> list (v2)

A list of different key-value pairs is generated by the map function after reading the given key-value pairs. Then, a pair composed by a key and a list of values is read by the reduce function that generates a list of values of the same type. Here, the output of map function is aggregated together by combining the values on the basis of their corresponding keys and forms the input for reduce function. In reduce function, the list of attached values is reduced to a single value for each of the keys found. Thus, the MapReduce computation input is represented as a collection of key-value pairs and the output is represented by a list values.

Virtualization

Or

Need of virtualization

The technique of masking and abstracting physical resources is known as virtualization. Virtualization makes easy the infrastructure and accommodates the increasing growth of business and technological changes. It improves the capability and utilizations of IT resources, like networks, servers, or storage devices, beyond their physical limits. Virtualization facilitates resource management by storing and pooling resources for high utilization. It makes them seem as logical resources with increased capabilities.

In case of infrastructure-based services, virtualization technology is considered as one of the fundamental components of cloud computing. Virtualization enables creation of secure, customizable, and isolated execution environment for running applications, without influencing other user's applications. In addition, virtualization technologies not only give a virtual environment for executing applications, but also for memory, storage, and networking. Virtualization offers a great opportunity to construct elastically scalable systems that are capable of provisioning additional capability with minimum costs. Thus, it is largely used to provide customizable computing environment on demand.

The three main components in a virtualized environment are guest, virtualization layer and host. The system component that interacts with the virtualization layer is represented by the guest. The virtualization layer is responsible for recreating the same or a different environment where the guest will operate. The original environment where the guest is supposed to managed is represented by the host

Importance of Virtualization

Cloud computing environment a very popular concept is used known a, virtualization. Cloud systems use virtualization concepts as a tool to enable, better functionality and more advanced features within and across latest technology.

Virtualization is critical to cloud computing because it simple ties the delivery of services by providing a platform for optimizing complex IT resources in a scalable manner, which is what makes cloud computing so cost effective.

Virtualization has three characteristics that make it ideal for cloud computing -

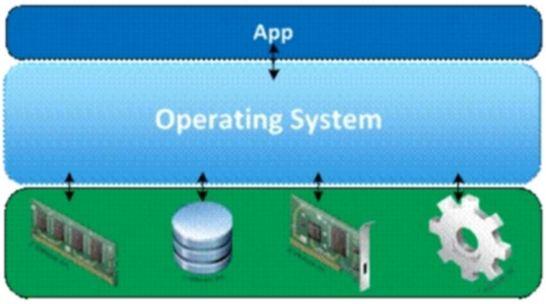
(i) **Partitioning** - In virtualization, we can use partitioning to support many applications and OS in a single physical system.

(ii) **Isolation** - Because each virtual machine is isolated, each machine is protected from crashes and viruses in the other machines.

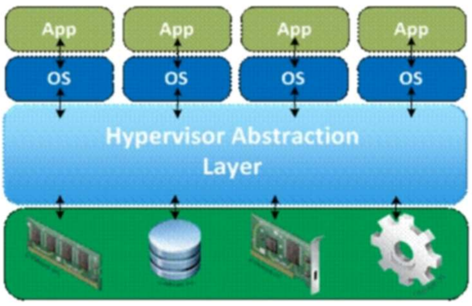
(iii) **Encapsulation** - This can protect each application so that it does not interfere with other applications. Using encapsulation, a virtual machine can be represented as a single file, making it easy to identify and present to other applications.

Architecture of a computer system before & after virtualization

A traditional computer system runs with hardware, host operating system. Operating system is designed according to hardware architecture. After virtualization, operating systems can run on same hardware and manage different applications and independent from host operating system. This is possible through additional virtualization layer software. This virtualization layer is also called hypervisor or virtual machine monitor. The virtual machine are appearing in the external boxes where applications run with their own guest operating system over the virtualized hardware resources like CPU, memory and input output resources. For virtualization the main function software layer is to virtualize the host machine physical hardware into virtu resources to be used by the VMs exclusively. This requires more steps for implementation, the virtualization software makes the virtual machine abstract through interposing a virtualization layer at many steps of a computer system General virtualization layers include the instruction set architecture level, application level, hardware level, operating system level, library support level.



Before Virtualization



After Virtualization

Objectives of virtualization

objectives of virtualization are -

(i) Improvement of scalability

(ii) Improvement of availability

(iii) Improvement of maintainability

(iv) Improvement of performance.

Benefits of Virtualization

Following are the benefits of virtualization -

(i) **Optimization of Workloads** - Virtualization can increase the use of existing resources by enabling dynamic sharing of resource pools. It enables you to respond dynamically to the application need of its users.

(iii) **Consolidation to Reduce Hardware Cost**- Virtualization enables

you to have a single server function as multiple virtual servers. It enables you to efficiently access and manage resources to reduce operations and systems management cost while maintaining needed capacity.

(iii) **Business Continuity and Disaster Recovery** - Virtualization allow easier software migration, including system backup and recovery which makes it extremely valuable as a disaster recovery or business continuity planning solution. Virtualization can duplicate critical servers so IT does not need to maintain expensive physical duplicates of every piece of hardware for disaster recovery purposes

(iv) **Business Agility** - Virtualization can greatly increase business agility and flexibility It improves agility by enabling IT to respond to rapid changes in demand by decoupling business processing from physical hardware Vernalization also enables enterprises to be faster to deploy new products and services, more able to incorporate offsite. contract and offshore labor, and more easily expand into new markets.

(v) **Reduce Downtime** - It is another key driver for virtualization. Virtual images are easier to restore after a failure.

(vi) **Reduced Administration Costs** - Administration becomes a lot easier, faster and cost effective with virtualization. Any failure in the environment can be rectified quickly and easily. Virtualization can significantly reduce management and maintenance costs, especially for large user communities, and wide geographic networks.

(vii) **High Performance and Scalability** - By using caching performance of physical storage can be improved in some implementations. Process of mapping between logical storage and physical storage require some processing and lookup tables and this results some latency in the mapping.

Characteristics of virtualized environment

The characteristics of virtualized environments are as follows -

(i) **Portability** - On the basis of specific type of virtualization, the concept of portability is used in different ways. In programming level virtualization, the binary code representing application components can be executed without any recompilation on any implementation of the corresponding virtual machine. This makes the application deployment very simple and application development cycle more flexible. In hardware virtualization solution, the guest is packaged into a virtual image that, in almost all the cases, can be safely removed and run on top of distinct virtual machines. This occurs with the same simplicity with which a picture image can be displayed in different computers except for the file size. In general, virtual images are proprietary formats. These formats need a certain virtual machine manager to be executed. At last, portability permits having your own system always with you and ready to use, given that the needed virtual machine manager is present. Generally, this need is less stringent compared to all other applications and services.

(a) *Sharing* - The creation of a separate computing environment within the similar host is allowed by virtualization. Hence, it is possible to fully make use of capabilities of a powerful guest, which would be underutilized otherwise.

(b) *Aggregation* - Virtualization enables the aggregation, which is opposite to sharing. In aggregation, a group of separate hosts are bound together and provided to guests like a single virtual host. This function 15 generally implemented in middleware for distributed computing.

(c) *Isolation* - Guests are provided with a complete separate environment to run them using virtualization. The guests may be applications operating systems and other entities. They carry out their activity by interacting with an abstraction layer, that gives access to the underlying resources Then are several benefits due to isolation. First, it offers a separation between the host and the guest. Second, it enables multiple guests to execute on the same host without interfering each other.

(d) *Emulation* - The execution of guests are performed within an environment that is handled by the virtualization layer, which is a program This permits for tuning and handling the environment that is exposed to guests For example, a complete different environment with respect to the host can be emulated, thus enabling the execution of guests requiring specific feature that are not available in the physical host. For testing purpose, this feature becomes very helpful. Again, hardware virtualization solutions are able to offer virtual hardware and emulate a specific type of device like SCSI (small compute system interface) device, without the hosting machine having such hardware installed. Old and legacy software that does not satisfy the needs of current systems can be run on emulated hardware without any need of changing the node. This is possible either within a particular operating system sandbox by emulating the needed hardware architecture.

(e) *Performance Tuning* - Performance tuning provides the considerable advances in hardware and software supporting virtualization. It facilitates the controlling of the performance of the guest by finely tuning the properties of the resources exposed via the virtual environment. This offers ways to effectively implement a QoS infrastructure that satisfies the service level agreement created for the guest.

(iii) **Improved Security** - For delivering a secure, controlled execution environment , the ability to handle the execution of a guest in a complete transparent way gives new possibilities. The virtual machine expresses an emulated environment where the guests are run. Generally, all the operations of the guest are carried out against the virtual machine. Thereafter, the virtual machine translates and applies the operations to the host. This level of indirection enables the virtual machine manager to handle and filter the activity of the guest, thus not allowing some harmful operations from being carried out. Then, resources exposed by the host can be protected from the guest

Different between or comparison in virtualization & cloud computing

1. Part of the ordered substructure	Brings resources of computing as a utility to client across the network
2. A self-service layer itself is not provided to the client and without that layer user cannot handover compute as utility	Cloud deals computing as a service instead of a particular technology
3. One probable utility that can be delivered.	An access for the bringing of utilities to an clients
4. Can exist without the cloud	Can exist only with virtualization.
5. Virtualization allows itself an arrangement to serve and efficiently use its **IT** resources	Using cloud computing it is possible to use those resources on other level by giving access to elements when required

Different type of virtualization

Following are the various types of virtualizations -

(i) **Execution Virtualization** - Execution virtualization incorporates all those techniques whose objective is to emulate an execution environment that is separate from the one hosting the virtualization layer. All these techniques focus their interest on giving support for the program's execution. The programs may be an application, the operating system, or a binary specification of a program compiled against an abstract machine model. Thus, the implementation of execution virtualization can be done directly on top of the hardware, by an application, the operating system, or libraries statically or dynamically linked against an application image. Execution virtualization techniques are divided into two major categories depending on the type of host they need. The implementation of process level techniques are done on top of an existing operating system, which has full control of the hardware. The implementation of system level techniques are done directly on hardware and do not need an existing operating system.

(ii) **Storage Virtualization** - A system administration practice that| enables decoupling the physical organization of the hardware from its logical representation is called storage virtualization. Users do not have to be thought about the particular location of their data by employing this technique. The particular location of data is recognized through a logical path. Storage virtualization enables harnessing a variety of storage facilities and representing them under a single logical file system. We can divide the storage virtualization into different techniques Among them, the most popular is network-based virtualization ty means of Storage Area Networks (SANs). A network accessible device is used by storage area networks using a large bandwidth connection to offer storage facilities.

(iii) **Network Virtualization** - For the creation and management of a, virtual network, network virtualization combines hardware appliances and specific software. Different physical networks can be aggregated into a single logical network (external network virtualization) by network virtualization lo an operating system partition (internal network virtualization), network virtualization, offer network like functionality. Generally, the outcome of external network virtualization is Virtual LAN (VLAN). An aggregation of hosts that communicate with each other if they were located under the same broadcasting domain is a VLAN. Internal network virtualization is applied together with the hardware and operating system level virtualization where the guests achieve a virtual network interface to communicate with. The implementation of internal network virtualization are done in several ways - the guest can contains a private network only with the guest; the guest can share the same network interface of the host and use NAT to access the network; or the virtual machine manager can emulate, and install on the host, an additional network device together with the driver.

(iv) **Desktop Virtualization** - The desktop environment available on a personal computer is abstracted by desktop virtualization in order to give access to it by employing a client-server approach. Desktop virtualization makes accessible a different system, but this system is remotely stored on a different host and accessed using a network connection. Apart from this, desktop virtualization deals with the situation of making the same desktop environment accessible from everywhere. However, the term desktop virtualization means the ability to remotely access a desktop environment. In general, the desktop environment is stored in a data center or a remote server that offers a high availability infrastructure, and guarantees the accessibility and the persistence of the data. There are several benefits of desktop virtualization accessibility, persistence, high availability and ease of management.

(v) **Application-server Virtualization** - A collection of application servers is abstracted by application-server virtualization. These application servers offer the similar services like a single virtual application server by employing load balancing strategies and offering a high availability infrastructure for the services hosted in the application server. This is a specific type of virtualization and serves the same purpose of storage virtualization.

(Execution)CPU virtualization

CPU virtualization is one of the cloud-computing technology that requires a single CPU to work which acts as multiple machines working together. Virtualization got its existence since the 1960s that became popular with hardware virtualization or CPU virtualization. CPU virtualization was invented to mange things easily by running every OS in one single machine. The virtualization mainly focusses on efficiency and performance-related operations by saving time. The hardware resources are used when needed and the underlying layer process instructions to make virtual machines work.

Application of virtualization

Application virtualization is a method that describes software technologies that separate them from the underlying operating system on which they are executed. This applies to applications at all tiers, from servers to desktops. Generally, this is achieved using encapsulation. Encapsulating and isolating the application from the OS changes the way applications can install and interact with the OS. This makes it possible for the application to be moved from one system to another, patched, and updated without interactions with other applications. Application virtualization also allows applications to be copied or backed up as a single file. A fully virtualized application is not installed in the traditional sense, although it still executes as though it were. The application is tricked at run time to believe that it is directly interfacing with the original OS and the resources it manages.

(storage)Memory virtualization Importance

There are several importance of memory virtualization -

(i) Memory virtualization helps in memory utilization through sharing of resources which are scarce and consolidating more virtual machines on a physical host and sharing of contents.

(ii) Memory virtualization lowers latency.

(iii) Memory virtualization gives faster access as compare to SSD, SAN

(iv) Memory virtualization helps in sharing large amount of data between applications of many server without redundancy and reduce memory requirement.

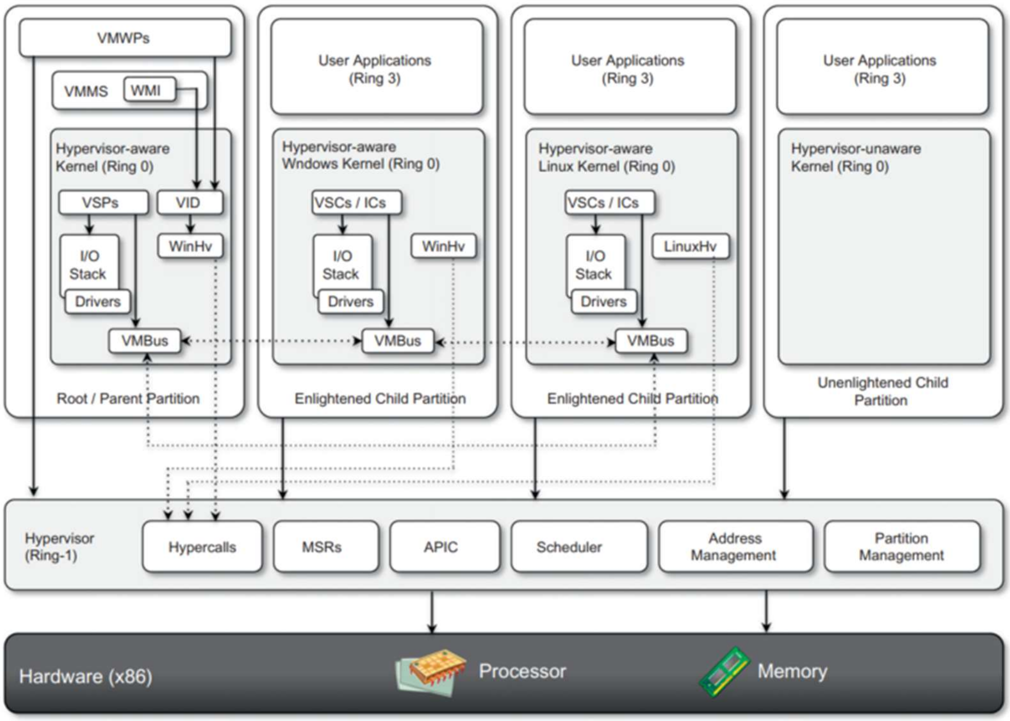
(v) Memory virtualization helps to access more memory as compared to capacity of physical memory.

(vi) Memory virtualization helps in reducing run time of input output bound applications which consume more data, thus increases efficiency.

(vii) Memory virtualization helps in keeping some memory space free before halting services as long as memory frees up.

Architecture of Hyper-V and use in cloud computing

Hyper-V is an infrastructure virilization solution for server virtualization. It is developed by Microsoft. Hyper-V supports multiple and concurrent execution of the guest operating system using partitions. A partition is an isolated environment in which an operating system is installed and run. An overview of Microsoft Hyper-V architecture is shown in fig.



In spite of its straightforward installation as a component of the host operating system, Hyper-V takes control of the hardware, and the host operating system becomes a virtual machine instance with special privileges, called parent partition or root partition. Only the parent partition has direct access to the hardware, it runs the virtualization stack, creates child partitions through the hypervisor, and host all the drivers required to configure guest operating systems. Child partitions are used to host guest operating systems, and do not have access to the underlying hardware, but their interaction with it is controlled by either the parent partition or the hypervisor itself.

Hypervisor - It is the component that directly manages the underlying hardware and defined by the following components

(i) **Hypercalls Interface** - For all the partitions this is the entry for the execution of sensible instructions. This interface is used by drivers in the partitioned operating system to contact the hypervisor by using the standard Windows calling conventions. This interface is also used by parent partition to create children partition.

(ii) **Memory Service Routines** - These are the set of functionalities that control the memory, and its access from partitions. By leveraging hardware- assisted virtualization, the hypervisor uses the input output memory management unit to fast track the access to devices from partitions, by translating virtual memory addresses.

(iii) **Advanced Programmable Interrupt Controller** – This component represents the interrupt controller, which manages the signals coming from the underlying hardware when some event occurs.

(iv) **Scheduler** - The virtual processors are scheduled by this component to run on available physical processors. Policies that are set by parent partition control the scheduling.

(v) **Address Manager** - Manages the virtual network addresses that are allocated to each guest operating system.

(vi) **Partition Manager** - This component performs partition creation, destruction, configurations, enumeration and finalization.

Enlightened I/O and Synthetic Devices - Enlightened I/O offers an optimized way to perform I/O operations allowing guest operating systems to leverage an inter-partition communication channel. This option is only available to guest operating systems that are hypervisor aware. As shown in fig. there are three components of Enlightened I/O - VMBus, Virtual Service Providers and virtual service clients. VMBus defines the protocol for communication between partitions and implements the channel. VSPs are kernel-level drivers that are deployed in the parent partition and provide access to the corresponding hardwares devices. These interact with VSCs which represent the virtual device drivers seen by the guest operating systems in the children partitions.

Parent Partition- The host operating system is executed by the parent partition. The parent partition implements the virtualization stack that complements the activity of the hypervisor in running guest operating systems. This partition a way hosts an instance of the Windows Sewer 2008 R2 which manages the virtualization stack made available to the children partitions. This partition is the one that directlv accesses device drivers and mediates the access to them by children partitions by hosting the VSPs.. The creation, execution and destruction of children partitions. It does so by means of Virtualization Infrastructure Driver(VID), which control the access to the hypervisor and also allows the management of virtual processors and memory. A Virtual Machine Worker Process (VMWP) is instantiated in the parent partition, which manages the children partition by interacting with the hypervisor through the VDl for each children partition created.

Common pitfall comes with virtualization

Some of the pitfalls of virtualization are as follows -

(i) **Inefficiency and Degraded User Experience** - Sometimes, there is an inefficient use of host in virtualization. Some of the features of the host cannot be exposed by the abstraction layer and they become inaccessible. In case of hardware virtualization, this could happen when for device drivers, the virtual machine can sometimes just provide a default graphic card which maps only a subset of the features available in the host. Some of the features of the underlying operating systems may become inaccessible unless specific libraries are used in case of programming level virtual machines.

(ii) **Security Holes and New Threats** - New and unexpected form of phishing has introduced due to virtualization. The capability of emulating a host in a complete transparent manner, has led the way to malicious programs which are designed to extract sensitive information from the guest. Malicious programs can preload themselves before the operating system, and act as a thin virtual machine manager towards it in case of hardware virtualization. Then, the operating system is controlled, and can be manipulated in order to extract sensitive information of interest for third parties. BluePill and SubVirt are the examples of these kind of malware. The diffusion of such kind of malware is facilitated by the fact that originally, hardware and CPU were not manufactured by keeping the virtualization in mind. The same considerations can be made for programming level virtual machines modified versions of the runtime environment can access sensitive information, or monitor the memory locations utilized by guest applications while these are executed In order to make this possible, the original version of the runtime environment needs to be replaced by the modified one, and this can generally happen if the malware is run within an administrative context, or a security hole of the host operating system is exploited.

(iii) **Performance Degradation** - Increased latencies and delays can be experienced by the guest because virtualization interposes an abstraction layer between the guest and the host. For instance, in case of hardware virtualization, where the intermediate emulates a bare machine on top of which an entire system can be installed, the causes of performance degradation can be traced back by the overhead. Also, when hardware virtualization is realized through a program that is installed or executed on top of the host operating systems, a major source of performance degradation is represented by the fact that the virtual machine manager is executed and scheduled together with other applications, thus sharing with them the resources of the host.

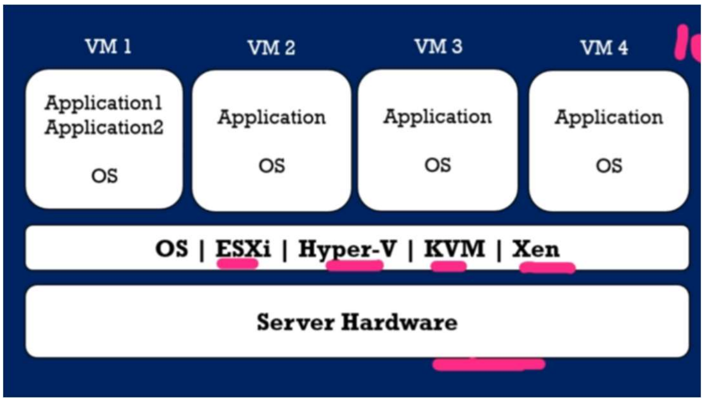
Similar consideration can be made in case of virtualization technologies at higher levels, such as in the case of programming language virtual machines. The execution of managed applications is slow down due to binary translation and interpretation. Moreover, being their execution filtered by the runtime environment, access to memory and other physical resources can represent sources of performance degradation.

Hypervisor virtual machine (HVM)

Or

Hypervisor management software

There is a companion layer of hypervisor management software for each hypervisor. This layer offers various functions such as create virtual machine, move virtual machine, delete virtual machine, etc. for Power Systems, Systems Director or the Power HMC as the hypervisor management function controlling the PowerVM hypervisor. For each 'Hypervisor/Hypervisor Management Software' pair, a unique set of APIs and GUIs is available that is used by the client IT staff and by ISVs to create management services or other applications. There is a freedom to make one's own hypervisor management software with open-source hypervisors like KVM and Xen.

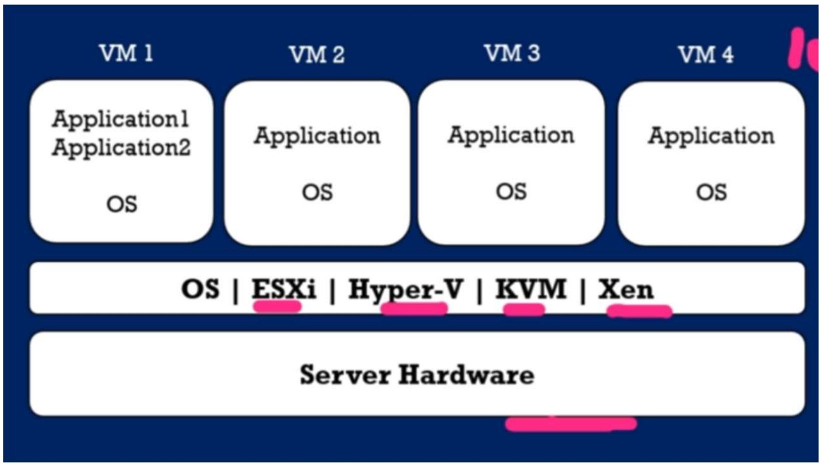


The foundation for virtualization on server is hypervisor. It enables hardware to be partitioned into multiple logical portion and make sure isolation among them Ethernet transport mechanism and Ethernet switch that arc required for virtual LAN capability are supported by hypervisor. To provide support tor virtual storage, hypervisor supports virtual SCSI. A global firmware image situated outside the partition memory in the first physical memory block at physical address zero is hypervisor. As soon as system is switched on, hypervisor takes control and collect information about CPU, memory, I/O and other resources. All the specified resources and other resources that are GLOBAL to the system are contolled and owned by hypervisor. Hypervisor allows the setup of logical partitioning and corresponding partition boundaries. Hypervisor tracks resource assigned to partition and offers isolation between partitions. Hypervisor is used to carry out virtual memory management employing a global partition page table. The physical memory is divided into physical memory blocks and logical memory is divided into logical memory blocks. The mapping of physical memory blocks. The hypervisor has access to whole memory space and manages memory allocation to partitions using a global partition page table. This guarantees the isolation for memory usage.

Type of hypervisor with diagram

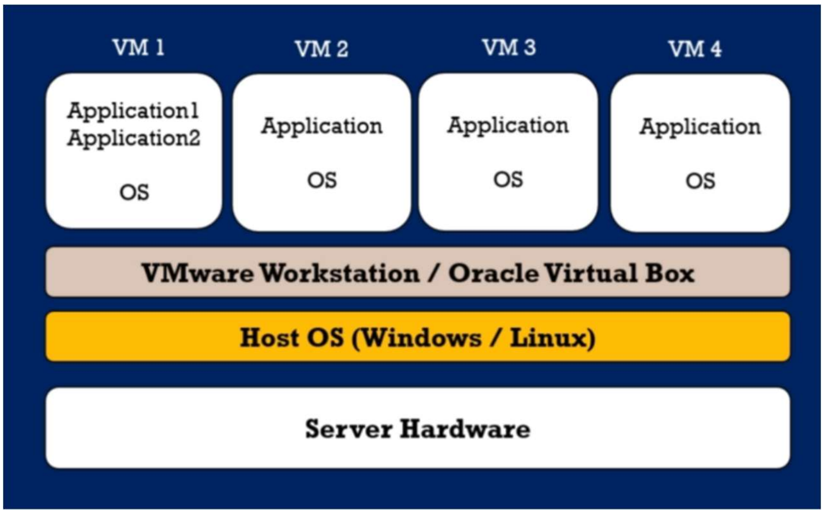
Hypervisors are classified into two types -

(i) **Type I (Bare Metal/Native Hypervisor)** - Software systems that run directly on the host's software as a hardware control and guest operating system monitor. A guest operating system thus runs on another level above the hypervisor. This is the classic implementation of virtual machine architectures. A type-1 hypervisor is a type of client hypervisor that interacts directly with hardware that is being virtualized. It is completely independent from the operating system and boots before the operating system. Type-1 hypervisor has no host operating system because they are installed on a hare system. Examples of type-1 hypervisors are LynxSecure, Oracle VM, VirtualLogic VLX, Sun xVM Server, RTS Hypervisor, etc. Type-1 hypervisor is shown in fig.



(ii) **Type 2 (Embedded/Host Hypervisor)**

Software application that run within a conventional operating system environment. Considering the hypervisor layer being a distinct software layer, guest operating systems thus run at the third level above the hardware. A type-2 hypervisor is a type of client hypervisor that sits on top of an operating system. A type-2 hypervisor relies heavily on the operating system. It cannot boot until the operating systems is already up and running and, if for any reason the operating system. It cannot boot until the operating system is already up and running system crashes, all end-users are affected. Example of type-2 hypervisor are Microsoft Hyper V, Wind RiverSimics, Containers, VMWare fusion, KVM, Xen Windows Virtual PC, Parallels Desktop for Mac, etc. Type-2 hypervisor ins show in fig



Advantages - Following are the advantages of hypervisor technology

(i) The hypervisor is used as a layer of abstraction to isolate the virtual environment from the hardware underneath.

(ii) Hypervisor is implemented below the guest OS in the cloud computing hierarchy, which means that if an attack passes the security systems in the guest OS, the hypervisor can detect it.

(iii) The hypervisor level of virtualization controls all the access between the guests' operating systems and the shared hardware underside. Therefore, hypervisor is able to simplify the transaction monitoring process in the cloud environment.

(iv) Hypervisor controls the hardware and it is only way to access it. This capability allows hypervisor based virtualization to have a secure infrastructure. Hypervisor can act as a firewall and will be able to prevent malicious users to from compromising the hardware infrastructure

Storage virtualization

Storage virtualization needed for -

(i) Inefficient storage utilization

(ii) Fast and reliable storage

(iii) Provides flexibility.

There are three ways in which storage virtualization structured -

(i) **Host-based Virtualization** - It is very simple way to provide storage virtualization. The responsibility of controlling physical storage space is depended on existing device drivers. A virtualization program on top (these drivers intercept the input output request and gives the meta-data lookup and input output mapping.

(ii) **Storage Device-based Virtualization** - It is the other way c virilization. In this way virtualization is performed on hardware level, leverages the capability of RAID controllers. It manages meta-data b creating a logical storage space through the use of large number of physical device drivers resources. Advanced RAID controllers permit further storage devices to be attached as-well-as features like cloning and remote replication.

(iii) **Network-based Virtualization** - It is performed on network device like server. Network device resides between the host and storage gives the features of input output redirection, vitalizing input output requests and mapping between physical and logical space. Many storage device look like physical!) connected to the operating system. Storage and virtualization device and this network of hosts are known as storage area network.

Block & file level storage virtualization

Or

Block level storage & file level storage

Block Level Storage Virtualization - Block level storage virtualization is illustrated in fig. It offers a translation layer between the hosts and the storage arrays in the storage area network (SAN) Here, the hosts are directed to the virtualized logical unit numbers (LUNs) on the virtualization device. The translation between the virtual LUNs and the physical LUNs on the individual arrays is carried out by the virtualization device. This makes easy the use of arrays from several vendors at a time, without any interoperability issues. All the arrays seem as a single target device and LUNs can be partitioned or distributed across multiple arrays for a host. Block level storage virtualization combines heterogeneous storage arrays, increases storage volume online, allows transparent volume access, and resolves application growth requirements.

LUN migration from one array to some other array was an offline event in traditional SAN environments since the hosts required to be updated to reflect the new array configuration. In other cases, host CPU cycles were needed to migrate data from one array to the other, particularly in a multi-vendor environment. In case of block level virtualization solution, the virtualization engine manages the back-end migration of data that allows LUNs 'o remain online and accessible during data migration. Since the host still Points to the same virtual targets on the virtualization device, no physical changes are needed. Although, there should be a change in the mappings on the virtualization device. These changes are transparent to the end user and be executed dynamically. In a virtualized environment. Deploying heterogeneous arrays makes easy an information lifecycle management (ILF strategy, enabling considerable cost and resource optimization.

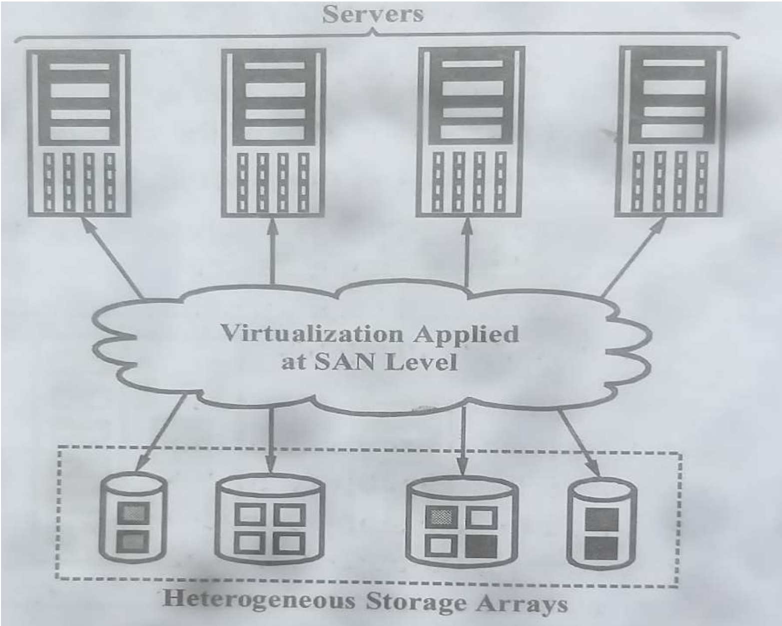
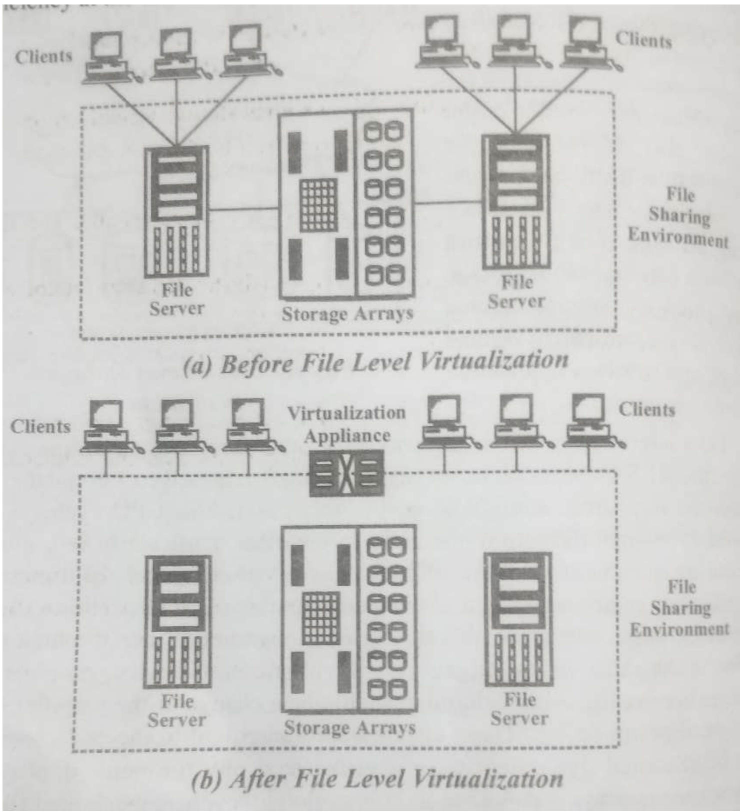


Fig. 3.7 Block Level Storage Virtualization

File Level Storage Virtualization - A network attached storage (NAS) environment before and after the implementation of file level virtualization is shown in fig. File level virtualization offers opportunities to perform nondisruptive file migrations, and server consolidation and to optimize utilization. It meets the NAS challenges by alleviating the dependencies between the location where the files are physically stored and the data accessed at the file level. Each NAS device or file server is logically and physically independent before virtualization. Each host knows exactly the location of its file level resources. Underutilized storage resources and capacity problems result due to boundation of files to a certain file server. Due to performance reasons or when the file server fills up, it is necessary to migrate the files from one server to another It is not easy to move file across the environment and this needs downtime for the file servers. In addition, hosts and applications have to be reconfigured with the new path, making it complex for storage administrators to enhance storage efficiency at the time of maintaining the required service level.

The mobility of file is facilitated by file level virtualization. It offers users or application independence from the stored file location. File level virtualization generates a logical pool of storage. which allows users to use a logical path to access files The movement of file systems across the online file servers is simplified by file level virtualization. It refers that when files are being moved, clients can access their files without causing problems. The files of clients can be read from the old location and written them back to the different location without realizing the change of physical location. Online movement of files can be performed by multiple clients attached to multiple servers to optimize utilization of their resources. The mapping of logical path of a file to the physical path names can be done using a global namespace.



Benefits of block level storage virtualization

Following are the benefits of block level storage virtualization -

(i) In each block or storage volume can be formatted with the file system required by the application.

(ii) The block level storage systems are more reliable and their transport systems are very efficient.

(iii) In each block or storage volume can be treated as an independent disk drive and are controlled by external server OS.

(iv) The block level storage systems are popular with the storage area network (SAN).

(v) The block level storage system offers a better performance.

(vi) They can support external boot-up of the systems connected to

them.

Virtual local area network(VLAN)

A switched network that is logically segmented by functions, applications, or project teams, independent of the user's physical location is known as virtual LAN (VLAN). A VLAN is same as a physical LAN except that it allows the grouping of end stations even in the situation when they are not physically located on the same network segment. This is a layer 2 (data link layer) construct. For reducing the overall cost of deploying a network infrastructure and allowing better utilization of port density, a network switch can be divided among multiple VLANs. The overall broadcast traffic is controlled by VLAN The transmission of broadcast traffic on one VLAN is not carried out outside that VLAN, that considerably decreases the networks vulnerability to broadcast storms, makes bandwidth available for applications, and reduces broadcast overhead.

VLANs are employed to limit individual user access, flag network intrusions, provide security firewalls, and control the size and composition of the broadcast domain. It is an example of network virilization that offers an simple, flexible and less expensive way to control networks. VLANs are used to make large networks more manageable by allow.ng a centralized configuration of devices located in physically diverse locations.

Storage area network

Storage area network provides high speed storage system with block-level storage. However, client can install file system on the top of SAN to provide file-level access. SAN is normally connected with fibre channel to improve the performance and speed. File sharing in SAN depends on the operating system. In SAN, data is accessed by block which is replicated to multiple locations to increase the availability. SAN uses many protocols like SCSI over TCP/IP, AoE, FcoE and many more. fig shows the architecture of SAN.

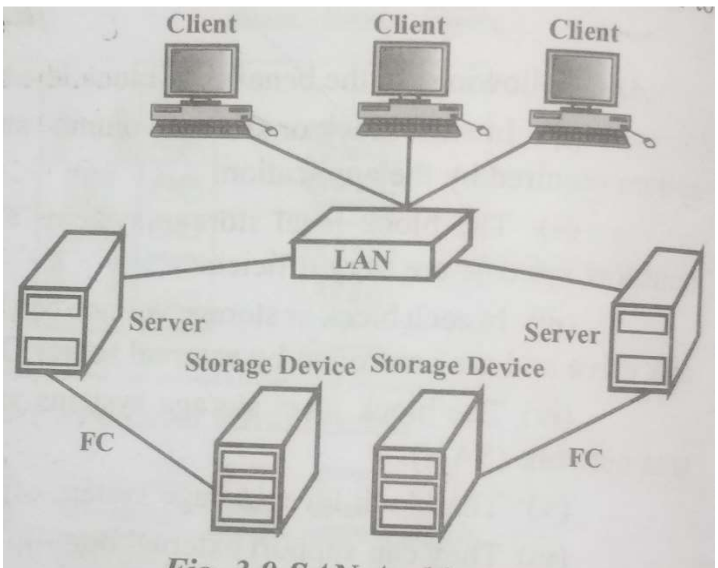


Fig. 3.9 SAN Architecture

SAN need because a single server can manage and provide the hard drives storages to multiple machines, and as the device computation increases the more storage require a single server can provide that. SAN help the each standard user it moves the storage resources to the freeway by the high speed network SAN allows each system to access directly as a shared storage devices do.

When the host wants to access device on SAN, it sends the request to the storage appliance. That access as the block-based access request. The storage area network is designed using the three components- Cabling, Host bus adapter (HBA), Switches. Each of the storage systems interconnected in the SAN and the physical interconnections can provides the higher bandwidth levels that can handle the data storage activities, e.g. there is a large business system mas have several of terabytes of data, that needs to be accessible by multiple devices on a local area network (LAN). Another efficient way to increase network storage, only one hard drive needs to be added to the computer system by installing SAN setup in the server.

Component of storage area network (SAN)

A SAN is typically assembled using three principle components

(i) Cabling

(ii) Host bus adapter (HBA)

(iii) Switch.

(i) **Cabling** - Cabling is the physical medium which is used for establishing a link between every SAN device by using transmission mediums like copper or optical fibre based on distance requirement of the organization.

(ii) **Host Bus Adapter (HBA)-** Host bus adapter is an expansion card that fits into expansion slot in a server. HBA naturally offloads data storage and retrieval overhead from the local processor which results m improving server performance.

(iii) **Switch** - Switch is used to handle and direct traffic between different network devices. It accepts traffic and then transmits the traffic to the desired endpoint device. In a SAN. each storage server and storage device is linked through a switch which includes SAN features like storage visualization, quality of service, security and remote sensing, etc.

Characteristics of Storage area network (SAN)

The characteristics SAN are as follows

(i) Shared storage facility across high-speed network

(ii) Improved client-server storage access.

(iii) Detaches storage tasks from specific servers.

(iv) Separate network handling storage needs.

(v) Hard disks, tape libraries, CD arrays.

(vi) Centralized management.

(vii) Scalability and shared data.

(viii) Direct storage-to-storage communication for backup.

(ix) High availability and disaster recovery.

(x) Storage consolidation and high bandwidth.

Limitation of Storage area network (SAN)

Following are the limitations of SAN

(i) Fabre channel is not a routable protocol.

(ii) These networks have high cost and weak security.

(iii) Management of SAN are difficult.

(iv) It has poor interoperability.

(v) Scalability is a concern in complex deployments.

Application of Storage area network (SAN)

The applications of SAN are as follows -

(i) It is a high-speed storage sharing system.

(ii) It's separated from the regular network system, and has an ability to expand the storage capacity.

(iii) SAN reduces the cost of the storage management since it simplifies the system fabric and devices management.

(iv) It increases the network bandwidth and reliability of data I/O

Working of Storage area network (SAN), and its features

A recent development of SAN is a virtual SAN or virtual fabric and conceptually, works in the similar way as a VLAN. A group of hosts or storage ports in a VSAN communicate with other employing a virtual topology defined on the physical SAN. One or more virtual SANs on a physical topology containing switches and ISLs are built by VSAN technology. This technology increases storage area network availability, scalability and security. These advantages are derived from the separation of fibre channel services in each VSAN and isolation of traffic between VSANs.

Following are the features of VSAN-

(i) Fabric-related configurations in one VSAN do not disrupt the traffic in another VSAN.

(ii) Every instance of a VSAN executes all needed protocols like FSPF, zoning and domain manager.

(iii) Events leading to traffic disruptions in one VSAN are kept within that VSAN. These are not propagated to other VSANs.

(iv) In a VSAN, a host fibre channel ID is allocated to a host in another VSAN thus improves SAN scalability.

VSAN, benefits

Benefits of Virtual SAN - The major benefits of virtual SANs are as follows

(i) Virtual SAN provides secure and reliable isolation of different storage islands.

(ii) Virtual SAN shares common infrastructure and resources like tape libraries to further reduce storage and network expenditures.

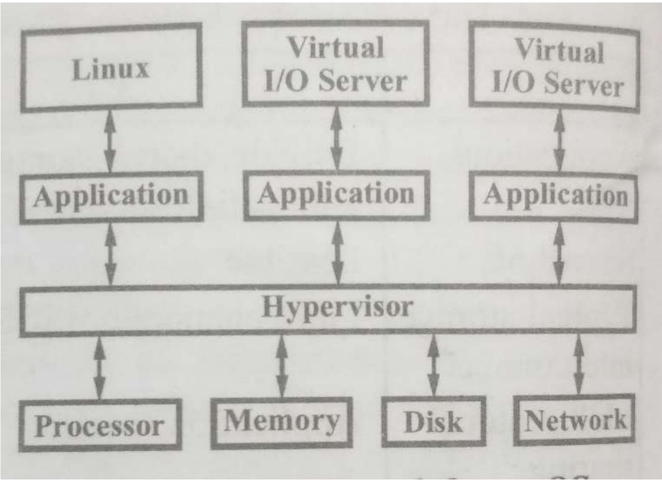
(iii) Virtual SAN can be used to consolidate separate physical SAN fabrics into one large fabric for ease of management and reduced total cost of ownership.

Server virtualization

Or

Kind of server virtualization

Server virtualization covers various kinds of virtualization like client, storage and network virtualization. The masking of server resources, including the number and identity of individual physical servers, operating system and processors from server users is server virtualization. A software application is used by the server administrator to partition one physical server into different isolated virtual environments that offer an abstraction of a complete, independent server to the server users. Virtual machine is often termed as virtualization environment, virtualized environment, partition, or container. It is a server environment that does not present physically but is created within some other server. Here, a virtual machine is a guest whereas the environment it runs within is a host. Usually, multiple virtual machines are run in a single host environment at a time. The host environment is often able to dynamically assign physical resources among virtual machines since virtual machines are separated from those resources they use. A user making contact with a virtual machine can consider it as a physical machine where the user would see access to an operating system and machine resources such as network, hard disk, memory and CPU.



In server virtualization, there are two main types of technology are used –

(i) hardware virtualization, and
(ii) operating system virtualization. Hardware

virtualization virtualizes the server hardware. It is also called Type 1 virtualization, Hypervisor-based virtualization. Bare-metal Hypervisor, or simply Hypervisor. Hardware Virtualization technology contains a virtualization layer running immediately on the hardware, that partitions the server machine into different virtual machines or partitions with a guest operating system running ln each of the machines. This virtualization technology gives binary transparency since the virtualization environment products themselves offer transparency to the application operating system and middleware that operate above it. Novell SUSE Xen, Red Hat Xen and KVM, Open Source KVM, VMware ESX server, Citrix XenServer and Microsoft Hyper-V are the example of hardware virtualization technology.

Operating system virtualization virtualizes the application environment. It is also called Type 2 virtualization, OS-based virtualization and OS-level virtualization Operating system virtualization generates virtual environment within a single operating system instance

Benefits of server virtualization

Following are the benefits of server virtualization -

(i) Server virtualization reduces cost because less hardware is required so that alone saves business money.

(ii) It lets each virtual server run its own operating system and each virtual server can also be independently rebooted of one another.

(iii) Server virtualization also utilizes resources to the fullest so ii can also save operational costs.