MCA (Semester – III)
Course Code - MCS-227
Course Title - Cloud Computing and IoT
Credits - 4

BLOCK 1: CLOUD COMPUTING FUNDAMENTALS AND VIRTUALIZATION

Unit 1: Cloud Computing: An Introduction

Unit 2: Cloud Deployment Models, Service Models and Cloud Architecture

Unit 3: Resource Virtualization

BLOCK 2: RESOURCE PROVISIONING, LOAD BALANCING AND SECURITY

Unit 4: Resource Pooling, Sharing and Provisioning

Unit 5: Scaling

Unit 6: Load Balancing

Unit 7: Security Issues in Cloud Computing

BLOCK 3: IoT FUNDAMENTALS AND CONNECTIVITY TECHNOLOGIES

Unit 8: Internet of Things: An Introduction

Unit 9: IoT Networking and Connectivity Technologies

BLOCK 4: Application Development, Fog Computing and Case Studies

Unit 10: IoT Application Development

Unit 11: Fog Computing and Edge Computing

Unit 12: IoT Case Studies

Unit 1: Cloud Computing: An Introduction

1.1. Traditional Computing Approaches

Previously, the power of computing was considered to be costly and scarce. Today, with the emergence of cloud computing, it is plentiful and inexpensive, causing a profound paradigm shift — a transition from scarcity computing to abundance computing. This computing revolution accelerates the commoditization of products, services and business models and disrupts current information and communications technology (ICT) Industry .It supplied the services in the same way to water, electricity, gas, telephony and other appliances. Cloud Computing offers on-demand computing, storage, software and other IT services with usage-based metered payment. Cloud Computing helps re-invent and transform technological partnerships to improve marketing, simplify and increase security and increasing stakeholder interest and consumer experience while reducing costs. With cloud computing, you don't have to over-provision resources to manage potential peak levels of business operation. Then, you have the resources you really required. You can scale these resources to expand and shrink capability instantly as the business needs evolve. This computing paradigm gave rise to many forms of distributed computing such as grid computing and cloud computing.

These vast applications required high-performance computing systems for their execution wherein the concept of cluster computing, grid and cloud computing came into existence. Some of the examples are:

- Numerous Scientific and engineering applications
- Modeling, simulation and analysis of complex systems like climate, galaxies, molecular structures, nuclear explosions, etc.
- Business and Internet applications such as e-commerce and web-servers, file servers, databases, etc.

For running these applications, the traditional approach to computing in the form of parallel computing was used. But, then, the dedicated parallel computers were very expensive and were not easily extensible. Hence, as per the users' demand, the computer scientists or engineers designed the cost-effective approaches in the form of cluster, grid and cloud computing.

1.2. Evolution of Cloud Computing

Today's PCs have remarkably high computing power. In the last few years, networking capabilities have also improved phenomenally. It is now possible to connect clusters of workstations with latencies and bandwidths comparable to tightly coupled machines. The concept of "Clusters" started to take off in the 90's. The term "grid computing" also originated in the early 1990s as a metaphor for making the computer power as easy to access as an electric power grid. The grids were considered as an innovative extension to the distributed computing technology. However, the development of Cloud Computing through various phases, including Grid Computing, Utility Computing, Application Service Provision and Software as a Service, etc., has taken place in a remarkable way. But the overall (whole) concept of the provision of computing resources via a global network began in the 1960s. But the history of cloud computing is how we got there and where all that started. Cloud computing has a history that is not that old, the first business and consumer cloud computing website was launched in 1999 (Salesforce.com and Google). Cloud computing is directly connected to Internet development and the development of corporate technology as cloud computing is the answer to the problem of how the Internet can improve corporate technology. Business technology has a rich and interesting background, almost as long as businesses themselves, but the development

that has influenced Cloud computing most directly begins with the emergence of computers as suppliers of real business solutions. History of Cloud Computing Cloud computing is one of today's most breakthrough technologies.

- Early Phases of 1960s

Computer scientist John McCarthy had the concept of time-sharing that allowed the organization to use an expensive mainframe at the same time. This machine is described as a major contribution to Internet development, and as a leader in cloud computing.

- 1969

  J.C.R. Licklider, responsible for the creation of the Advanced Research Projects Agency (ARPANET), proposed the idea of an "Intergalactic Computer Network" or "Galactic Network" (a computer networking term similar to today's Internet). His vision was to connect everyone around the world and access programs and data from anywhere.
- 1970s
- Usage of tools such as VMware for virtualization. More than one operating system can be run in a separate environment simultaneously. In a different operating system it was possible to Cloud Computing: Unedited Version pg. 15 operate a completely different computer (virtual machine). IN 1997 Prof Ramnath Chellappa in Dallas in 1997 seems to be the first known definition of "cloud computing," "a paradigm in which computing boundaries are defined solely on economic rather than technical limits alone." IN 1999 Salesforce.com was launched in 1999 as the pioneer of delivering client applications through its simple website. The services firm has been able to provide applications via the Internet for both the specialist and mainstream software companies. IN 2003 This first public release of Xen ,is a software system that enables multiple virtual guest operating systems to be run simultaneous on a single machine, which also known as the Virtual Machine Monitor (VMM) as a hypervisor. IN 2006 The Amazon cloud service was launched in 2006. First, its Elastic Compute Cloud (EC2) allowed people to use their own cloud applications and to access computers. Simple Storage Service (S3) was then released. This incorporated the user-as-you-go model and has become the standard procedure for both users and the industry as a whole.

1.3. Comparison between Cluster, Grid and Cloud Computing

FEATURES	*CLUSTER COMPUTING*	*GRID COMPUTING*	*CLOUD COMPUTING*
Characteristics	Tightly coupled systems, Single system image, Centralized Job management & scheduling system	Loosely coupled (Decentralization) Diversity and Dynamism Distributed Job Management & scheduling	Dynamic computing infrastructure, IT service-centric approach, Self-service based usage model, Minimally or self-managed platform, Consumption-based billing
Physical Structure	In cluster computing, a bunch of similar/identical computers are hooked	In grid computing, the computers do not have to be in the same physical location and	In cloud computing, the computers need not to be in the

	up locally (in the same physical location, directly connected with very high speed connections) to operate as a single computer	can be operated independently. As far as other computers are concerned each computer on the grid is a distinct computer	same physical location.
Hardware	The cluster computers all have the same hardware and OS	The computers that are part of a grid can run different operating systems and have different hardware	The memory, storage device and network communication are managed by the operating system of the basic physical cloud units. Open source Software such as LINUX can support the basic physical unit management and virtualization computing.
Resources	The whole system (all nodes) behaves like a single system view and resources are managed by centralized resource manager.	Every node is autonomous i.e. it has its own resource manager and behaves like an independent entity	Every node acts as an independent entity
Applications	1. Educational resources 2.Commercial sectors for industrial promotion 3.Medical research	1.Predictive Modeling and Simulations 2.Engineering Design and Automation 3.Energy Resources Exploration 4.Medical, Military and Basic Research 5.Visualization	1.Banking 2.Insurance 3.Weather Forecasting 4.Space Exploration 5.Software as a service 6.PaaS 7.Infrastructure-as -a-Service
Networking	Dedicated, high-end with low latency and high bandwidth Interconnection Network	Mostly Internet with high latency and low Bandwidth Interconnection Network	Dedicated, high-end with low latency and high Bandwidth Interconnection Network
Scalability	Size or scalability is 100s	Size or scalability is 1000s	Size or scalability is 100s to 1000s

1.4. Utility Computing

Utility computing basically refers to the utility computing technologies and the business models that are offered by a service provider to the IT customers. The client is charged as per their consumption. Examples of these IT services are storage, computing power, and applications.

The term utility is basically the utility services like water, telephone, electricity, and gas that are provided by any utility company. In a similar manner, the customer when receives utility computing, its computing power on the shared computer network bills is decided on the basis of the consumption which is measured.

Utility computing is similar to virtualization and the total web storage space amount with the computing power that is made available to the user is higher as compared to a single time-sharing computer. The web service is possible through a number of backend web servers. The web servers could be dedicated and used as a cluster form which is created and then gets leased to the end-user. Distributed computing is the method where a single such calculation is done on multiple web servers.

In utility computing, there is a provider who will own the storage or power resources. The customer is charged based on how much they make use of the services. The customer is not charged each month and the services are not sold outright. Depending on the resources that are offered utility computing could also be called Infrastructure as a Service or IaaS and Hardware as a Service or HaaS.

Their function is similar to the other basic utilities. It is like you or any major company uses electricity. Both of you do not pay a flat monthly rate but pay the amount as per the electricity that you consume.

There are companies that offer a different kind of utility computing where the user will rent a cloud computer and use it in order to run the applications or an algorithm or anything that may need a lot of computing power. You pay per second or per hour and do not pay a flat fee to use the service.

Utility computing is beneficial because of its flexibility. Since you do not own the resource and are not leasing them for long it is easy to change the amount of power that you buy. You are free to grow or to shrink the service amount within a few seconds based on your business requirements.

1.5. Characteristics of Cloud Computing

- *On-demand Self Service:* A consumer can request and receive access to a service offering, without an administrator or some sort of support staff having to fulfil the request manually.
- *Broad network Access:* The servers can be accessed from any location using any type of device – anywhere access and anytime.
- *Resource Pooling*: Resource can be storage, memory, network bandwidth, virtual machines, etc. which can be consumed by the cloud users. Resource Pooling means that multiple customers are serviced from the same physical resources.
- *Measured Services:* Pay according to the services you use.
- *Rapid Elasticity and Stability*: One of the great things about cloud computing is the ability to quickly provision resources in the cloud as organizations need them and then to remove them when they don't need them.
- *Easy maintenance:* Maintenance of the cloud is easier.
- *Security:* Copy of our data on various servers i.e., if 1 fails, data is safe on the other.

1.6. Benefits of Cloud Computing

- Resources accessible anywhere, anytime
- On-demand self-service
- Reduced IT cost(We need not purchase hardware, no maintenance, etc.)
- Scalability- If traffic on website is more, we can scale up anytime and similarly scale down also.

- Online development and deployment tools
- Collaboration – People sitting in different countries can do a project through collaborating and getting their data stored on the cloud
- Offers security as data stored is stored at multiple locations.
- Location and device independence
- Saves our time – we need not update the softwares, or maintain the hardware.

1.7. Applications of Cloud Computing

1. *Online Data Storage :*

   Cloud computing allows storing data like files, images, audios, and videos, etc on the cloud storage. The organization need not set physical storage systems to store a huge volume of business data which costs so high nowadays. As they are growing technologically, data generation is also growing with respect to time, and storing that becoming problem. In that situation, Cloud storage is providing this service to store and access data any time as per requirement.
2.
3. *Backup and Recovery:*

   Cloud vendors provide security from their side by storing safe to the data as well as providing a backup facility to the data. They offer various recovery application for retrieving the lost data. In the traditional way backup of data is a very complex problem and also it is very difficult sometimes impossible to recover the lost data. But cloud computing has made backup and recovery applications very easy where there is no fear of running out of backup media or loss of data.
4.
5. *Big data Analysis:*

   We know the volume of big data is so high where storing that in traditional data management system for an organization is impossible. But cloud computing has resolved that problem by allowing the organizations to store their large volume of data in cloud storage without worrying about physical storage. Next comes analyzing the raw data and finding out insights or useful information from it is a big challenge as it requires high-quality tools for data analytics. Cloud computing provides the biggest facility to organizations in terms of storing and analyzing big data.

6. *E-commerce Application:*
   Cloud-based e-commerce allows responding quickly to the opportunities which are emerging. Users respond quickly to the market opportunities as well as the traditional e-commerce responds to the challenges quickly. Cloud-based e-commerce gives a new approach to doing business with the minimum amount as well as minimum time possible. Customer data, product data, and other operational systems are managed in cloud environments.

7. *Cloud computing in education :*

Cloud computing in the education sector brings an unbelievable change in learning by providing e-learning, online distance learning platforms, and student information portals to the students. It is a new trend in education that provides an attractive environment for learning, teaching, experimenting, etc to students, faculty members, and researchers. Everyone associated with the field can connect to the cloud of their organization and access data and information from there.

6.*E-Governance Application :*

Cloud computing can provide its services to multiple activities conducted by the government. It can

support the government to move from the traditional ways of management and service providers to an advanced way of everything by expanding the availability of the environment, making the environment more scalable and customized. It can help the government to reduce the unnecessary cost in managing, installing, and upgrading applications and doing all these with help of could computing and utilizing that money public service.

7. *Cloud Computing in Medical Fields :*

In the medical field also nowadays cloud computing is used for storing and accessing the data as it allows to store data and access it through the internet without worrying about any physical setup. It facilitates easier access and distribution of information among the various medical professional and the individual patients. Similarly, with help of cloud computing offsite buildings and treatment facilities like labs, doctors making emergency house calls and ambulances information, etc can be easily accessed and updated remotely instead of having to wait until they can access a hospital computer.

8. *Entertainment Applications:*

Many people get entertainment from the internet, in that case, cloud computing is the perfect place for reaching to a varied consumer base. Therefore different types of entertainment industries reach near the target audience by adopting a multi-cloud strategy. Cloud-based entertainment provides various entertainment applications such as online music/video, online games and video conferencing, streaming services, etc and it can reach any device be it TV, mobile, set-top box, or any other form. It is a new form of entertainment called On-Demand Entertainment (ODE).

1.8. Challenges of Cloud Computing

- *Availability of Services*
- *Data Lock-In:* Shifting of large volume of data from one platform to another.
- *Data Seggregation:* Isolation of data of each user.
- *Scaling Resources:* Sudden demand of increased resources may arise.
- *Location of Data:* Geographically stored(Each country has its own rule)
- *Deletion of Data:* User demands complete removal of data
- *Recovery and Backup:* How frequently and how fast a cloud system recovers from failure.

UNIT 2 CLOUD DEPLOYMENT MODELS, SERVICE MODELS AND CLOUD ARCHITECTURE

Structure

2.0 INTRODUCTION

The purpose of this chapter is to provide a broad range of cloud deployment methods, which are one of the most essential topics in cloud computing. The various methods in which the cloud computing environment may be set up or the various ways in which the cloud can be deployed are referred to as deployment models. It is critical to have a basic understanding of deployment models since setting up a cloud is the most basic requirement before moving on to any other aspects of cloud computing. This chapter discusses the basic three core cloud computing service models, namely IaaS, PaaS, and SaaS. The end user's and service provider roles may differ depending on the services given and subscribed to. In addition, the end user and service provider responsibility of IaaS, PaaS, and SaaS are discussed in this chapter. This chapter also covers appropriateness, and benefits and drawbacks of various cloud service models. This chapter consists of a brief overview of various other service models such as NaaS, STaaS, DBaaS, SECaaS, and IDaaS. The cloud architecture is initially described in this chapter. Cloud architecture is made up of a series of components arranged in a hierarchical order that collectively define how the cloud functions. The cloud anatomy is explained in the next section, followed by an overview of cloud network connection.

2.1 OBJECTIVES

After completion of this unit, you will be able to:

• Be familiar with the different deployment models.

• Contrast and compare different service delivery models

• Give a high-level overview of the cloud architecture.

• Provide information about the cloud's layers and anatomy.

• Describe how network connection plays a part in cloud computing.

2.2 CLOUD DEPLOYMENT MODELS

Now a days, the majority of businesses use cloud infrastructure to save capital investment and control operational costs since it provides several advantages such as lower infrastructure expenses, more mobility, scalability, and improved collaboration. These advantages should be categorized according to the organization needs based on the deployment model. The infrastructure accessibility and ownership are the factors to be considered into cloud deployment models. The deployment model defines the ways for deploying or making cloud services available to clients based on ownership, capacity, access and purpose. The kinds of deployments vary according to the management of the infrastructure and the location of that infrastructure.
There are four main categories of the deployment models are:

- Public
- Private
- Community
- Hybrid

2.2.1 Public Cloud: The most popular and common deployment is the public cloud. The public cloud is accessible from anywhere in the globe and is ease to use for the general public. Any organization or enterprise or academic or a combination of them, may own and manage it. The entire infrastructure is located on the cloud provider's premises. It's a pay-per-use model and provides the services on demand according to service-level agreements. An end user can actually buy these resources on an hourly basis and utilize them as needed. In public cloud, users no need to maintain any infrastructure instead everything will be owned and operated by cloud public provider. The following Fig. 2.2.1 represents the public cloud.

Fig.2.2.1 Public Cloud

The Public cloud model has the following benefits:

- **Minimal Investment:** This model eliminates the need for extra hardware expenditures.
- **No startup costs:** Users can rent the computing resources on pay-per-use, there is no need of establishing infrastructure from user side in turn reduces the startup costs.
- **Infrastructure Management is not required:** There is no need of any hardware to be set up from user side but everything is operated and controlled by service provider.

- **Zero maintenance:** The service provider is responsible for all maintenance work from infrastructure to software applications.
- **Dynamic Scalability:** On-demand resources are provisioned dynamically as per customer requirements.

2.2.2 Private Cloud: It is a cloud environment created specifically for a single enterprise. It is also known as on-premise cloud. It allows access to infrastructure and services inside the boundaries of an organization or company. Private cloud is more secure when compared to similar models. Because the private cloud is usually owned, deployed and managed by the organization itself, the chance of data leakage is very less. Because all users are members of the same organization, there is no risk from anybody else. In private clouds, only authorized users have access, allowing organizations to better manage their data and security. The following Fig. 2.2.2 represents the private cloud.

Fig. 2.2.2 Private Cloud

The Private cloud model has the following benefits:

- **Better Control:** Private cloud is managed by their own organization staff.
- **Data Privacy:** Data is accessed and managed by inside the boundaries of an organization.
- **Security:** Provides security for the data because only authorized users may access it.
- **Customization:** In contrast to a public cloud deployment, private cloud allows a customization of resources to meet its specific needs.

2.2.3. Community Cloud: The community cloud is the extension of private cloud and this kind of model is sharing cloud infrastructure among multiple organizations in the same community or area. Organizations, businesses, financial institutions and banks etc. are examples of this category. The infrastructure is provided for exclusive usage by a group of users from companies with similar computing requirements in a community cloud environment. The following Fig. 2.2.3 represents the community cloud.

Fig. 2.2.3 Community Cloud

The Community cloud model has the following benefits:

- **Cost-effective:** Community cloud is cost-effective since its infrastructure cost is shared among number of enterprises or communities.
- **Security:** The community cloud is more secure compared to public cloud
- **Shared resources:** Infrastructure and other resources shared with multiple organizations.
- **Data sharing and collaboration:** It is excellent for both data sharing and collaboration.
- **Setup Benefits:** Customers may be able to work more efficiently as a consequence of these shared resources.
- **Smaller investment:** Investment on infrastructure is shared among organizations in the community.

2.2.4. Hybrid Cloud: It is a kind of integrated cloud computing, which means that it may be a combination of private, public, and community cloud, all of which are integrated into a single architecture but remain independent entities inside the overall system. This aims to combine the benefits of both private and public clouds. The most common way to use the hybrid cloud is to start with a private cloud and then use the public cloud for more resources. It is possible to utilize the public cloud for non-critical tasks like development and testing. On the other hand, critical tasks such as processing company data are carried out on a private cloud. The following Fig. 2.2.4 represents the hybrid cloud.

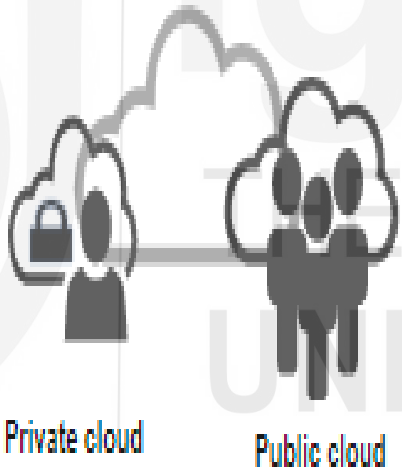

Fig. 2.2.4 Hybrid Cloud

The Hybrid cloud model has the following benefits:

- **Flexibility and control:** Companies with greater flexibility may create customized solutions to match their specific requirements.
- **Cost:** Cost is less compared to public cloud users paid only for additional resources used from public cloud.
- **Partial Security:** The hybrid cloud is generally a mix of public and private clouds. Although the private cloud is considered as secure and the hybrid cloud includes public cloud, poses a significant chance of security breach. As a result, it can only be described as partially secure.

2.3 CHOOSING APPROPRIATE DEPLOYMENT MODELS

The instances where this cloud model may be employed are referred to as selecting an acceptable deployment model. It also denotes the best circumstances and environment in which this cloud model may be implemented.

2.3.1 Suitability of Public Cloud:

The public cloud model is appropriate in the following circumstances:

- There is a high demand for resources, resulting in a large user base.
- There is a dynamic change of resources based on customer requirements.
- No physical infrastructure exists.
- A company's finances are limited.

The public cloud model is not appropriate in the following circumstances:

- It is critical to maintain a high level of security.
- Autonomy is expected by the organization.
- Reliability from a third party is not recommended.

2.3.2 Suitability of Private Cloud:

The term suitability in terms of cloud refers to the conditions under which this cloud model is appropriate. It also denotes the best circumstances and environment in which to use this cloud model, such as the following:

- Enterprises or businesses that demand their own cloud for personal or business purposes.
- Business organizations have appropriate financial resources, since operating and sustaining a cloud is an expensive effort.
- Business organizations consider the data security to be important.
- Enterprises want to get complete control and autonomy over cloud resources.
- Private cloud is suitable for organizations with less number of employees.
- Organizations that already have a pre-built infrastructure will choose private cloud for managing resources efficiently.

The private cloud model is not appropriate in the following circumstances:

- An organization consists of more number of users.
- Enterprises that have constraints on finance.
- Organizations that do not have a pre-existing infrastructure
- Organizations with insufficient operational staff to maintain and administer the cloud

2.3.3 Suitability of Community Cloud:

The Community cloud is suitable for the organizations with the following concerns:

- Wish to build a private cloud but lack of financial support.
- Don’t want to take complete control of maintenance responsibility of the cloud
- Desire to work in collaboration for effective outcome.
- provides more security when compared to public cloud

The community cloud model is not appropriate in the following circumstances:

- Organizations want to get complete control and autonomy over cloud resources.
- Doesn't really want to collaborate with other organizations

2.3.4 Suitability of Hybrid Cloud:

The hybrid cloud model is appropriate in the following circumstances:

- Organizations that desire a private cloud environment with public cloud scalability
- Businesses that demand greater protection compared to the public cloud.

The Hybrid cloud model is not appropriate in the following circumstances:

- Organizations that prefer security as a top priority
- Organizations that are unable to handle complex hybrid cloud infrastructures

2.3.5 Comparative analysis of cloud deployment models

Characteristics	Public	Private	Community	Hybrid
Demand for in-house infrastructure	Not required	Mandatory	Shared among organizations	Required for private cloud
Ease of use	Very easy to use	Requires an operational IT staff	Requires an operational IT staff from multiple organizations	Complex because involves more than one deployment model
Cost	Affordable and lower compare to other models	High compared to public cloud	Cost is distributed among organizations	Cheaper than private cloud and costlier than public cloud
Security	Less secure than other models	Provides more security than other models	Higher than public cloud and lower than private cloud	Higher than public cloud and lower than private and community cloud
Ownership	Cloud service Provider	Single Organization	Multiple organizations with similar concerns	Cloud service Provider for public cloud and organization for private cloud
Managed by	Cloud service Provider	Organization operational staff	operational staff among multiple organizations	Cloud service Provider for public cloud and operational staff for private cloud
Scalability	Very High	Limited	Limited	High

2.4 CLOUD SERVICE DELIVERY MODELS

Cloud computing model is used to deliver the services to end users from a pool of shared resources such as compute systems, network components, storage systems, database servers and software applications as a pay-as-you-go service rather of purchasing or owning them. The services are delivered and operated by the cloud provider, which reduces the end user's management effort. Cloud computing allows the delivery of a wide range of services categorized into three basic types of delivery models as follows:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

Different cloud services are aimed towards different type of users, as shown in Fig. 2.4.1. For instance, consider the IaaS model is aimed at infrastructure architects, whereas PaaS is aimed at software developers and SaaS is aimed at cloud users.

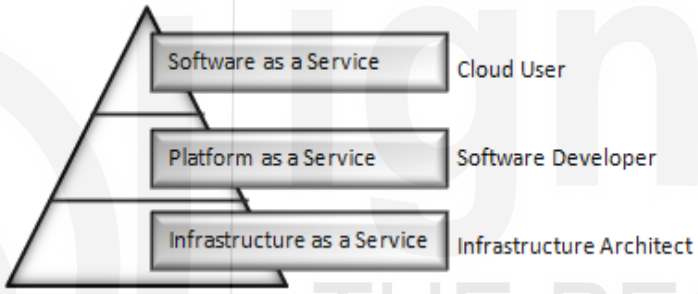

Fig. 2.4.1 Cloud Service delivery models

2.4.1 IaaS: on Demand Virtualized Infrastructure

The resources are provisioned to the users of IaaS, to run any kind of software, including operating systems and applications, by giving them access to fundamental computer resources like processing, storage, and networks. There is no control over the physical infrastructure, but the user has control over operating systems, storage and installed software, as well as specific networking components (for example host and firewalls). A service model known as IaaS refers to the usage of a third-party provider's virtual physical infrastructure in place of one's own (network, storage, and servers). Because IT resources are housed on external servers, they may be accessed by anybody with an internet connection.

The IT architect or infrastructure architect is the target audience for IaaS. The infrastructure architect may choose the virtual machine instance based on their requirements. The physical servers are managed by the service providers. As a result, the complexity of managing the physical infrastructure is removed or hidden from the IT architects. The following services might be provided by a regular IaaS provider.

- **Compute:** Virtual computing power and main memory are provided to end users as part of Computing as a Service.
- **Storage:** It provides back-end storage for storing files and VM images.
- **Network:** There are many number of networking components like bridges, routers and, switches are provided virtually.
- **Load balancers:** These are used to manage the sudden spikes in usage of infrastructure for balancing the load

Pros and Cons of IaaS

IaaS is a one of the most prominent cloud computing service delivery model. It provides more benefits to the IT architects.

The following are the advantages of IaaS:

1. Charging based on usage: The services of IaaS are provisioned on a pay-per-use basis to users. Customers are paid for only what they have used. This strategy reduces the needless expenditure of investment on hardware purchases.

2. Reduced cost: IaaS providers allow their customers to rent computing resources on a subscription basis instead of investing on physical infrastructure to run their operations. IaaS eliminates the need to purchase physical resources, lowering the total cost of investment.

3. Elastic resources: IaaS provides resources depending on user requirement. The resources can be scale up and scale down by using load balancers. Load balancers automate the process of dynamic scaling by sending additional requests are redirected the new resources.

4. Better resource utilization: The most important factor of IaaS provider is the resource utilization. To get return on investment by utilizing the infrastructure resources efficiently.

5. Supports green IT: Dedicated servers are utilized for many business requirements in conventional IT architecture. The power consumption will be more due to the large number of servers deployed. IaaS eliminates the need for dedicated servers since a single infrastructure is shared among several clients, decreasing the number of servers in turn decreases the power consumption resulting in Green IT.

• Despite the fact that IaaS saves investment cost for start-up companies, but it lacks security for data protection.

The following are some of the disadvantages of IaaS:

1. Security issues: IaaS is providing services through Virtualization technology through hypervisors.. There are several chances to attack the compromised hypervisors. If hypervisors are compromised, any virtual machines may be simply attacked. The majority of IaaS providers are unable to ensure complete security for virtual machines and the data stored on them.

2. Interoperability issues: IaaS service providers don't have any standard operating procedures. Any VM transfer from one IaaS provider to another is a difficult one. Customers may encounter the issue of vendor lock-in issue.

3. Performance issues: It is providing resources from distributed servers, those are connected through a network.. The network latency is a key factor in determining performance of the service. Due to latency concerns, the VM's performance might suffer from time to time.

The following are the popular examples of IaaS :

- Microsoft Azure
- Rackspace
- AWS
- Google Compute Engine

2.4.2 PaaS: Virtualized development environment

The PaaS user or developer can develop their applications on virtualized development platform provided by PaaS provider. The users doesn't have the control on the development platform and underlying infrastructure like servers, storage , network and operating system but the user has control on the deployed applications as well data related to that applications.

Developers can build their applications online using programming languages supported on provider platform and deploy their applications using testing tools supporting the same platform. Pass users utilizing the services offered by the providers through the internet. As a result, the cost of obtaining and maintaining a large number of tools for constructing an application is decreased. PaaS services include a wide range of programming languages supported on platforms, databases, and testing software tools. PaaS providers provide a wide range of software development and deployment capabilities including load balancers.

1. Programming languages: PaaS providers offer a scope for multiple programming languages in which users can develop their own applications. Some examples of languages are python, java, Scala, PHP and Go etc.

2. Application platforms: PaaS providers offer a variety of application platforms, those are used to develop applications. The popular examples of platforms are Joomla, Node.js, Drupal, WordPress, Django and Rails

3. Database: Applications need backend for storing data. Database is always associate with frontend application to access data. Databases are provided by PaaS providers as part of their PaaS platforms. Some of the prominent databases offered by PaaS vendors are Redis, MongoDB, ClearDB, Membase, PostgreSQL, and Cloudant.

4. Testing tools: Testing tools are provided by PaaS providers as part of their PaaS platforms. Testing tools are required to test application after development.

Pros and Cons of PaaS

The complexity of platform and underlying infrastructure maintenance is managed by PaaS provider. This allows developers to concentrate more on the application development.
In addition, PaaS provides the following advantages:

1. App development and deployment: PaaS provides all the necessary development and testing tools in one place, allowing you to build, test, and deploy software quickly. After the developer completes the development process, most PaaS services automate the testing and deployment process. This is faster than conventional development platforms in developing and deploying applications.

2. Reduces investment cost: The majority of conventional development platforms need high-end infrastructure leads to increase the investment cost for application development. Using PaaS services eliminates the requirement for developers to purchase licensed development and testing tools. On the other side, PaaS lets programmers rent everything they need to create, test and deploy their applications. The total investment cost for the application development is reduced because of expensive infrastructure is not required.

3. Team collaboration: Traditional development platforms do not offer much in the way of collaborative development. PaaS allows developers from multiple locations to collaborate on a single project. The online shared development platform supplied by PaaS providers makes this feasible.

4. Produces scalable applications: Applications need scale-up or scale-down the resources based on their load. In case of scale-up, companies must keep an additional server to handle the increased traffic. New start-up companies have a tough time expanding their server infrastructure in response to rising demand. PaaS services, on the other hand, provide built-in scalability to applications produced on the PaaS platform.

When compared to the traditional development environment, PaaS offers several advantages to developers.
On the other side, it has several disadvantages, which are listed below:

1. Vendor lock-in: Vendor lock-in is a key disadvantage of PaaS providers. Lack of standards is the primary cause of vendor lock-in. PaaS providers do not adhere to any common standards for providing services. The adoption of proprietary technology by PaaS providers is another factor for vendor lock-in. The majority of PaaS companies employ proprietary technologies that are incompatible with those offered by other PaaS providers. PaaS services have a vendor lock-in issue that prevents applications from being transferred one provider to another.

2. Security problems: Security is a big concern with PaaS services. Many developers are hesitant to use PaaS services since their data is stored on third-party servers off-site. Obviously, many PaaS providers have their own security mechanism to prevent user data from security breaches, but feeling safety of on-premise deployment is not same as off-premise deployment.. When choosing a PaaS provider, developers should compare the PaaS provider's regulatory, compliance, and security standards to their own security needs.

3. Less flexibility: PaaS limit developer's ability to create their own application stack. Most PaaS providers give access to a wide range of programming languages, database software's, and testing tools but user doesn't have control on platform. Developers can only customize or build new programming languages for PaaS platform from a few providers. The majority of PaaS vendors still do not give developers with enough flexibility.

4. Depends on Internet connection: Developers must have an internet connection in order to utilize PaaS services. The majority of PaaS providers do not provide offline access but very few can provide offline access. With a poor Internet connection, the PaaS platform's usability will not meet the developer expectations.

Examples of PaaS:

- Redhat Open Shift
- Google App Engine (GAE)
- Heroku
- Scalingo
- Python Anywhere
- Azure App Service
- AWS Elastic Beanstalk

2.4.3 SaaS: Cloud based application

The end user has the option of using the provider's cloud-based applications. It is possible to access the software from multiple client devices using a web browser or other client interface (such as web-based e-mail). The customer has no access or control over the cloud infrastructure, which includes networks, servers, operating systems, storage, software platforms, and configuration settings. An internet based, no-installation kind of software as a service has been provided on subscription and these services may be accessed from any location in the globe.

SaaS applications are provided on-demand through the internet, users can access these applications through web enabled interface without software installation on end-user machines. Users have complete control over when, how and how often they use SaaS services. SaaS services can be accessed through web browser on any device, including computers, tablets and smart devices. Some SaaS services can be accessed by a thin client, which does not have as much storage space as a standard desktop computer and cannot run many applications. Thin clients for accessing SaaS applications have a longer lifespan, lower power consumption and lower cost are all

advantages of using these devices. A SaaS provider might provide a variety of services, including business management services, social media services, document management software's and mail services.

1. Business services: In order to attract new customers, the majority of SaaS suppliers now provide a wide range of commercial services. SaaS include ERP, CRM, billing, sales and human resources.

2. Social media networks: Several social networking service providers have used SaaS as a method of assuring their long-term survival because of the widespread usage of social networking sites by the general public. Because the number of users on social networking sites is growing at a rapid rate, cloud computing is the ideal solution for varying load.

3. Document management: Because most businesses rely heavily on electronic documents, most SaaS companies have begun to provide services for creating, managing, and tracking them.

4. E-mail services: Many people utilize e-mail services these days. The potential growth in e-mail usage is unexpected. Most e-mail providers started offering their services as SaaS services to deal with the unexpected amount of users and demand on e-mail services.

Pros and Cons of SaaS

SaaS provides software applications that are used by a wide range of consumers and small organizations because of the cost benefits they provide.

SaaS services give the following advantages in addition to cost savings:

1. No client-side installation: Client-side software installation is not required for SaaS services. Without any installation, end users may receive services straight from the service provider's data centre. Consuming SaaS services does not need the use of high-end hardware. It may be accessible by thin clients or any mobile device.

2. Cost savings: Because SaaS services are billed on a utility-based or pay-as-you-go basis, end customers must pay only for what they have utilized. Most SaaS companies provide a variety of subscription options to suit the needs of various consumers. Sometimes free SaaS services are provided to end users.

3. Less maintenance: The service provider is responsible for automating application updates, monitoring, and doing other routine maintenance then the user is not responsible for maintain the software.

4. Ease of access: It is possible to access SaaS services from any device that has access to the Internet. The use of SaaS services is not limited to a certain set of devices. It features are making it adaptable to all devices.

5. Dynamic scaling: On-premise software makes dynamic scalability harder since it requires extra hardware. Because SaaS services make use of cloud elastic resources, they can manage any sudden spike in load without disrupting the application's usual operation.

6. Disaster recovery: Every SaaS service is maintained with suitable backup and recovery techniques. A large number of servers are used to store the replicas. The SaaS may be accessed from another server if the allocated one fails. This solves the problem of single point of failure. It also ensures high availability of application.

7. Multi-tenancy: Multi-tenancy refers to sharing same application among multiple users improves resource use for providers and decreases cost for users.

Data security is the biggest problem with SaaS services. Almost every organization is concerned about the safety of the data stored on the provider's datacenter.

Some of the problems with SaaS services include the following:

1. Security: When transitioning to a SaaS application, security is a big issue. Data leakage is possible because the SaaS application is shared by many end users. The data is kept in the datacenter of the service provider. We can't trust our company's sensitive and secret data on third-party service provider. To avoid data loss, the end user must be careful when choosing a SaaS provider.

2. Requirements for connectivity: In order to use SaaS applications, users must have internet connection. If the user's internet connection is low in some cases then the user is unable to use the services. In SaaS applications, the high-speed internet connection is the major problem.

3. Loss of control: The end user has no control over the data since it is kept in a third-party off-premise location.

Examples of SaaS

- Google GSuite (Apps)
- Dropbox, Salesforce
- Cisco WebEx and
- GoToMeeting

Figure 2.4.1 illustrates the three types of cloud computing services that are offered to clients. It's important to note that cloud service delivery is made up of three distinct components: infrastructure, platform, and software. The end user's responsibility in IaaS is development platform and the application that runs on top of it are properly maintained. The underlying hardware must be maintained by the IaaS service providers. In PaaS, end users are only responsible for developing and deploying the application and its data only. In SaaS, user do not have any control over infrastructure management, development platform and end-user application, all maintenance is handled by SaaS providers. The responsibility of the provider and user is indicated in Figure 2.4.2

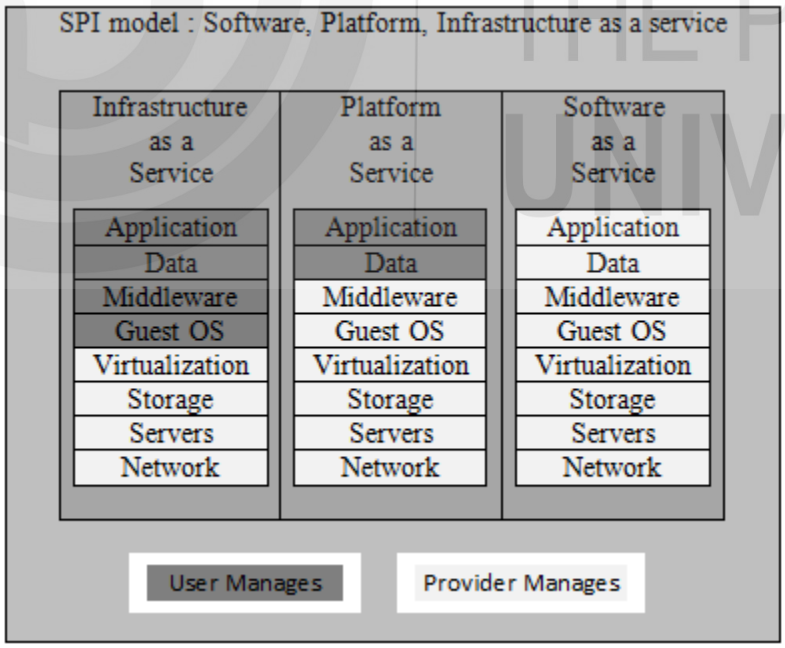

Fig. 2.4.2 Service provider and User management responsibilities of SPI model

2.4.4 Other services

1. Network as a Service (NaaS): It allows end users to make use of virtual network services provided by the service provider. It is a pay-per-use approach similar to other cloud service models, NaaS allows users to access virtual network services through the Internet. In on-premise organizations, they have spent expenditure on network equipment to run their own networks in their own datacenters. On the other hand, Naas are transformed into a utility to make virtual organizations, virtual organization interface cards, virtual switches, virtual switches and other systems administration components in the cloud environment. There are a number of popular services provided by NaaS, including VPNs, bandwidth-on-demand, and virtualized mobile networks.

2. DEaaS (Desktop as a Service): It allows end customers to enjoy desktop virtualization service without having to acquire and manage their own computing infrastructure. It is a pay-per-use model in which the provider handles data storage, backup, security and updates on the back end. DEaaS services are easy to set up, secure, and provide a better user experience across a wide range of devices.

3. STorage as a Service (STaaS): It provides end users with the opportunity to store data on the service provider's storage services. Users may access their files from anywhere and at any time with STaaS. Virtual storage emulates from physical storage is abstracted by the STaaS provider. STaaS is a utility-based cloud business model. Customers may rent storage space from the STaaS provider and they can access from any location. STaaS provides disaster recovery backup storage solution.

4. Database as a Service (DBaaS) : This service that allows end users to access databases without having to install or manage them. Installing and maintaining databases is the responsibility of the service provider. End consumers may utilize the services immediately and pay for them based on their use. Database administration is automated using DBaaS. The database services may be accessed by end users using the service provider's APIs or web interfaces. The database management procedure is made easier using DBaaS. DBaaS provides popular services such as ScaleDB , SimpleDB, DynamicDB, MongoDB and GAE data store.

5. Data as a Service (DaaS): An on demand service provided by a cloud vendor to users to access the data over the Internet. Data consists of text, photos, audio, and videos etc. all are part of the data. Other service models for example SaaS and STaaS are closely related to DaaS. For offering a composite service, DaaS may simply include in either SaaS or STaaS. Geographical data services and financial data services are two areas where DaaS is widely employed. Agility, cost efficiency, and data quality are some of the benefits of DaaS.

6. SECurity as a Service (SECaaS): It is a pay-per-use security service that allows the user to access the cloud provider's security service. The service provider combines its security services for the benefit of end customers in SECaaS. It provides a wide range of security-related functions, including authentication, virus and malware / spyware protection, intrusion detection, and security event management. Infrastructure and applications within a company or organization are often protected by SECaaS service providers. SECaaS services are provided by Cisco, McAfee or Panda etc.

7. Identity as a Service (IDaaS): It is possible to leverage a third-party service provider's authentication infrastructure on behalf of end customers, which is called Identity as a Service (IDaaS). A company or business is the most common end user of IDaaS. Any company may effortlessly maintain its workers' identities with IDaaS services without incurring any extra costs. Services such as directory services and single sign-on are all included within IDaaS in general, Integrated services, such as registration, authentication, risk and event monitoring, identification and profile management.

- **Check Your Progress 1**

1.List out the names of popular cloud computing service providers

……
……
……..

2. Distinguish between public and private clouds.

……
……

2.5 CLOUD ARCHITECTURE

The cloud architecture is divided into four major levels based on their functionality. Below Fig. 2.5.1 is a diagrammatic illustration of cloud computing architecture.

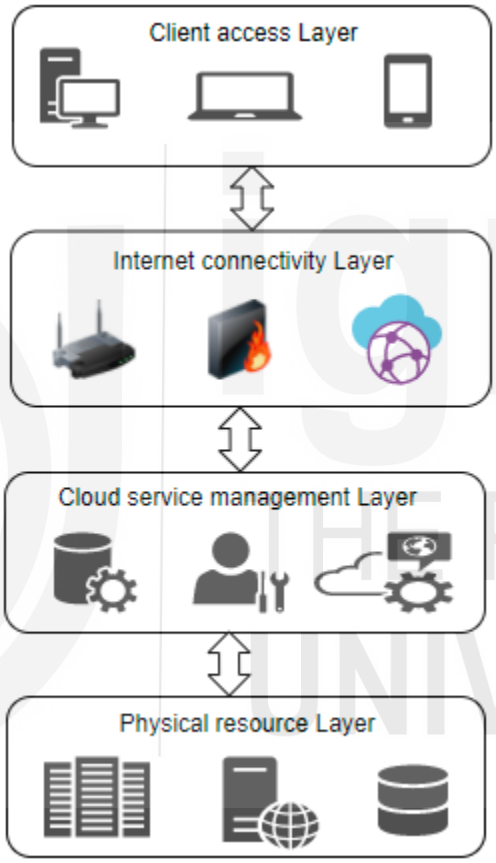

Fig. 2.5.1 Cloud Architecture

1. Client access Layer:

Client access layer is the top-most layer of cloud architecture. The clients of cloud are come into this layer. Clients begin their journey toward cloud computing here. The client may use any device that supports basic web application functionality, smart mobile or portable device such as thin or thick devices. Thick devices are general-purpose computers or smart devices with sufficient computing power but on the other hand, a thin device has a very limited processing capacity and depends on other systems. A cloud application is often accessible in the same manner as that of web application but the characteristics of cloud application is different from web application. Thus, client access layer is made up of different types of client smart devices.

2. Internet connectivity layer:

This internet network layer connects users to access the cloud. The entire structure of cloud is based on the internet network connection through which clients access the services. In case of public cloud, it entirely relies on the internet connection. The public cloud location is not known to the user but the public cloud may be accessed across the world through the internet. The private cloud exists within organization premises; a local area network may provide connection with in the organization. In both cases, the cloud is completely relies on the network connection but users require minimal bandwidth while using the public or private cloud. Service-level agreements (SLAs) doesn't include the internet connection between the user and the cloud while considering QoS(Quality of Service), so this layer will not be covered by the SLAs.

3. Cloud service management Layer

This layer is made up of technologies that are used to manage the cloud. Cloud management software that run on this layer are responsible for managing the service providers resources such as scheduling, provisioning, optimization (such as consolidating servers and storage workloads), and internal cloud governance. Activities in this layer affect the SLAs agreed between clients and cloud vendor since this layer is dependent upon SLAs. SLA violations occur when there is a lack of timely or consistent service. If a SLA is violated, the service provider is required to pay a penalty. Both private and public cloud services are relies on these service level agreements. some of the popular public cloud vendors are Microsoft Azure and AWS. Similarly some of the private cloud vendors are Eucalyptus and Openstack are used to create and management of private clouds.

4. Layer of physical resources

The bottom layer is the actual hardware resources layer and it is the base or foundation layer of any cloud architecture. The resources comprise compute, storage, database and network, which are the fundamental physical computing resources that make up a cloud infrastructure. These physical resources are actually pooled from different datacenters located at different locations to provide service to a large number of users. Service provider offers compute systems as a service to host the applications of the user and also provides the software to manage the application based on scalability of resources. Storage systems keep track of business information as well as data created or processed by applications running on the computing systems.

Computing systems and storage systems are linked together through networks. A network, such as a local area network (LAN) connects physical computing devices to one another, allowing applications running on the compute systems to communicate with one another. A network connects compute and storage systems to access the data on the storage systems. The cloud serves computing resources from several cloud datacenters, networks link the scattered datacenters and allowing the datacenters to function as a single giant datacenter. Networks also link various clouds to one another, allowing them to share cloud resources and services (as in the hybrid cloud model).

2.6 LAYERS AND ANATOMY OF THE CLOUD

The hierarchical structure of a cloud is called cloud anatomy. Cloud anatomy differs from architecture. It does not include the communication channel on which it deliver the services, whereas architecture completely describes the communication technology on which it operates. Cloud architecture is a hierarchical structure of technology on which it defines and operates. Anatomy might therefore be considered as subset of cloud architecture. Figure 2.6.1 represents the cloud anatomy structure, which serves as the foundation for the cloud.

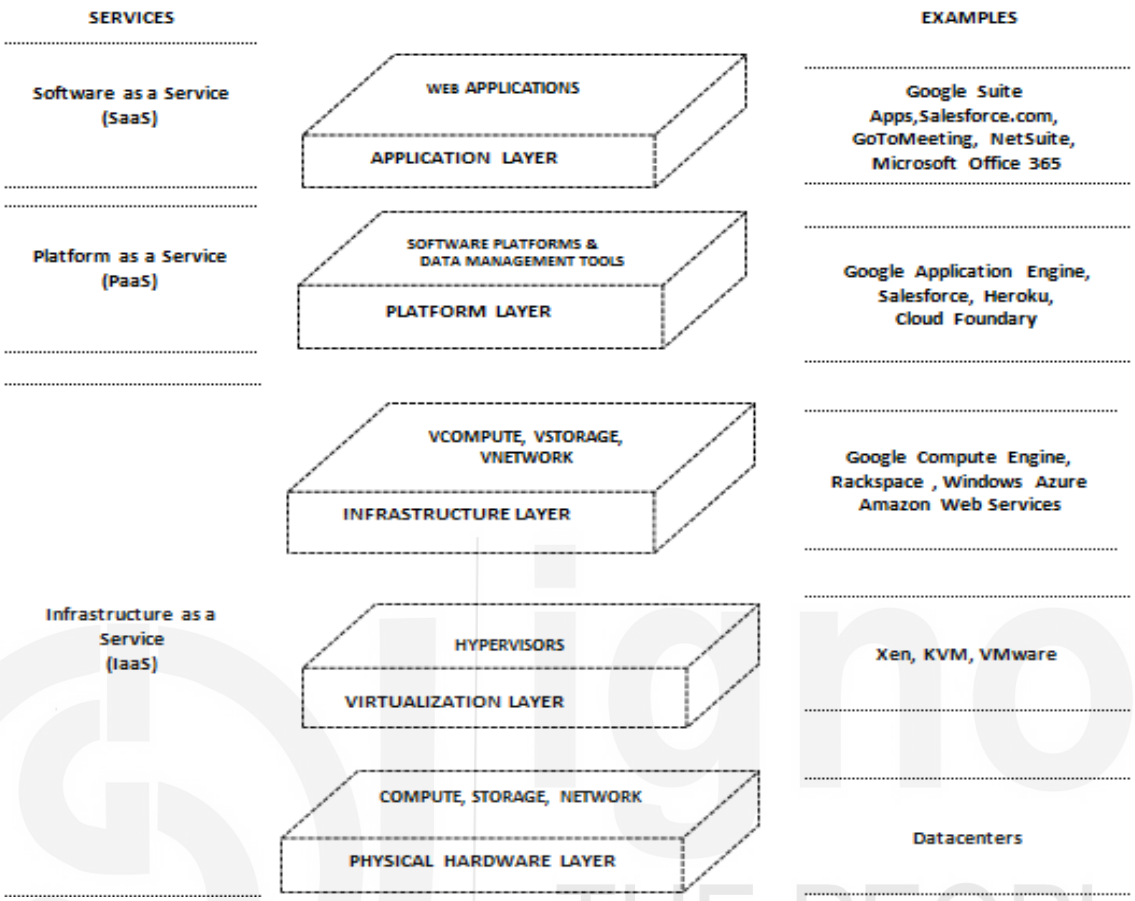

Fig.2.6.1 Layers of Cloud Anatomy

The cloud is made up of five main elements:

1. Application: Top most layer is the application layer. This layer may be used to execute any kind of software application.

2. Platform: This layer exists below the application layer. It consists of executable platforms those are provided for the execution developer applications.

3. Infrastructure: This layer lies below the platform layer. Infrastructure includes virtualized computational resources are provided to the users to connect with other system components. It allows the users to manage both applications and platforms. This allows the user to do computations based on their requirements.

4. Virtualization: It's a vital technology that allows cloud computing to function. It is the process of making abstraction of actual physical hard ware resources are provided in virtual manner. It changes the way of providing the same hardware resources are distributed to multiple tenants independently.

5. Physical hardware: The bottom most layer is the physical hardware layer. It consists of servers, network components, databases and storage units.

2.7 NETWORK CONNECTIVITY IN CLOUD COMPUTING

The cloud resources include servers, storage, network bandwidth, and other computer equipment are distributed over numerous locations and linked via networks. When an application is submitted for execution in the cloud, the necessary and appropriate resources are used to run the application that connects these resources through the internet. Network performance will be a major factor in the success of many cloud computing applications. Because cloud computing offers a variety of deployment choices, a network connection viewpoint will be used to examine cloud deployment models and their accessible components.

There following are the different types of network connectivity in cloud computing:

- **Public Inter cloud Networking**

Customers may be able to connect to public cloud over the internet, Some cloud providers can provide virtual private networks (VPNs). Public cloud services bring up security issues, which are in turn connected to performance. One possible strategy to provide security is to encourage connection through encrypted tunnels, allowing data to be transferred across secure internet pipelines. This process will add the extra connectivity overhead and employing it will almost probably increase latency and have an influence on performance.

If we want to minimize latency without sacrificing security, we must choose an appropriate routing strategy, decreases communication latency by decreasing the number of transit hops in the path from cloud provider to consumer, for instance. When a connection is made available via internet for peer to peer systems through a federation of connected providers (also known as Internet service providers (ISPs).

- **Private Inter Cloud Networking**

In private cloud, the cloud and network connectivity is within organization premises. The connectivity with in private cloud is provided through Internet VPN or VPN service. All services are accessed quickly through well-established pre-cloud infrastructure. Moving to private clouds does not affect the ability to access application performance

- **Public Intra cloud Networking**

Public intra cloud networking is the network connectivity included for public cloud model. The cloud resources that are geographically distributed over datacenters and providing those resources to end users via the internet only. The user cannot access public cloud intra networks since they are internal to the service provider. Quality of Service (QoS) is primary factor considered for linked resources throughout the world. The majority of these performance concerns and violations are addressed commercially in SLAs.

- **Private Intra cloud Networking**

Intra cloud networking is the most complex networking and connection challenge in cloud computing. The most challenging aspect of private cloud is the private intra cloud networking. The applications running in this environment are linked to intra cloud connection. Intra networking connects the provider datacenters owned by an organization. Intra cloud networking will be used by all cloud computing systems to link users to the resource to which their application has been assigned. Once the link is established to the resource, intra networking used to serve the application to multiple users based on service oriented architecture (SOA). If the SOA concept is followed, traffic may flow between application components and between the application and the user. The performance of such connections will therefore have an influence on the overall performance of cloud computing.

Modern approaches should be used to assess cloud computing networks and connections, Globalization and changing organization needs, particularly those related with expanded internet use, require more prominent adaptability in the present corporate organization.

➢ **Check Your Progress 2**

1. How the cloud architecture differ from cloud anatomy?

……
……
……..

2. Describe briefly about private cloud access networking?

……
……
……..

2.8 SUMMARY

We covered the three SPI cloud service types as well as the four cloud delivery models in this chapter. We also looked at how much influence a consumer had over the various arrangements. After that, we looked at cloud deployment and cloud service models from a variety of perspectives, leading to a discussion of how clouds arise and how clouds are utilized. To begin, the deployment models are the foundation and must be understood before moving on to other components of the cloud. The size, location, and complexity of these deployment models are all taken into account.

In this chapter, we'll look at four different deployment models. Each deployment model is described, along with its characteristics and applicability for various types of demands. Each deployment model is significant in its own right. These deployment patterns are crucial, and they frequently have a significant influence on enterprises that rely on the cloud. A wise deployment model decision always pays off in the long run, avoiding significant losses. As a result, deployment models are given a lot of weight. Before diving into the complexities of cloud computing, it's vital to understand a few key concepts, including one of the most significant: cloud architecture.

Before getting into the complexities of cloud computing, it's vital to understand a few key concepts, including one of the most significant: cloud architecture. It has a basic structure with component dependencies indicated. Anatomy is the same way as architecture; however it does not take into account any dependencies as architecture does. The cloud network connection, which is at the heart of the cloud concept, is also critical. The network is the foundation on which the cloud is built.

2.9 SOLUTIONS/ANSWERS

➢ **Check Your Progress 1**

1. List out the names of popular cloud computing service providers

- Microsoft Azure
- Rackspace Cloud
- Amazon Web Services (AWS)
- Alibaba Cloud
- IBM Cloud
- SAP
- Google Cloud
- VMWare
- Oracle
- Salesforce

2. Distinguish between public and private clouds.

Public Cloud	Private Cloud
It is managed by cloud service provider	It is managed by organization operational staff
On-demand scalability	Limited scalability
Multitenant architecture supports multiple users from different organizations	Dedicated architecture supports users from single organization
Services hosted on Shared servers	Services hosted on dedicated servers
Establishes connection to users through internet	Establishes connection to users through private network within the organization
Cost of using public cloud is cost-effective than private cloud	Cost of using private cloud is costly compared to public cloud
Suited for less confidential information	Suited for secured confidential information

➢ **Check Your Progress 2**

1. How the cloud architecture differ from cloud anatomy?

Cloud anatomy describes the layers of cloud computing paradigm at service provider side. Cloud anatomy and cloud architecture both are not same but anatomy is considered as part of cloud architecture. cloud architecture completely specifies and explains the technology under which it operates but in anatomy does not include technology on which it operates.

2. Describe briefly about private cloud access networking?

Virtual private network (VPN) establishes a secured private corporate network connection within private cloud to access the services. The technology and methodologies are local to the organization network structure in the private cloud. This cloud network might be an Internet-based VPN or a service supplied by the network operator.

2.10 FURTHER READINGS

1. Cloud Computing: Principles and Paradigms, Rajkumar Buyya, James Broberg and Andrzej M. Goscinski, Wiley, 2011.
2. Mastering Cloud Computing, Rajkumar Buyya, Christian Vecchiola, and Thamarai Selvi, Tata McGraw Hill, 2013.
3. Essentials of cloud Computing: K. Chandrasekhran, CRC press, 2014.

Unit 3: Resource Virtualization

Structure

3.1 INTRODUCTION

Cloud Computing has gained immense popularity due to the availability of scalable Infrastructure as a Services, Platform as a Service, and Software as a Services. This is a framework where different kinds of services related to networks, computing resources, storage, development platform, and application are provisioned through the internet. In this respect, the basic information of cloud computing is already discussed in the previous unit. In this unit, we will discuss the basics of virtualization, its advantages, and its underlying abstraction. It is to be noted that virtualization is the fundamental technology that helps to create an abstraction layer that hides the intricacy of the underlying hardware. The virtualization technique provides a secure and isolated environment for any user application such that one running application does not affect the execution of another application. Further, in this unit, we will learn about server-level virtualization and explore different hypervisor-based virtualization approaches. We will also discuss operating system-level virtualization, network virtualization, storage virtualization, and desktop virtualization. Finally, a brief comparison will be done on hypervisors like XenServer and VMware.

3.2 OBJECTIVE

After going through this unit you should be able to:

- ➔ describe virtualization and its advantage;
- ➔ understand the concept of machine or server-level virtualization;
- ➔ learn about the hypervisor-based virtualization approaches;
- ➔ understand the basics of the operating system, network, storage, and desktop virtualization;
- ➔ compare among XenServer and VMware;

3.3 Virtualization and Underlying Abstraction

Virtualization is a key technology that creates an abstraction to hide the complexity of computing infrastructure, storage, and networking. Though virtualization technology has been around for the last 50 years, its popularity has increased with the advancement of cloud computing. In a cloud environment virtualization allows maximum customization and control over hardware resources and enables the utilization of hardware resources to their maximum capacity.

Virtualization allows the creation of an abstract layer over the available System hardware elements like processor, storage, memory, and different customized computing environments. The computing environment which is created is termed virtual as it simulates an environment similar to a real computer with an operating system. The use of the virtual version of the infrastructure is smooth as the user finds almost no difference in the experience when compared to a real computing environment. One of the very good examples of virtualization is *hardware virtualization*. In this kind of virtualization, customized virtual machines that work similarly to the real computing systems are created. Software that runs on this virtual machine cannot directly access the underlying hardware resources. For example, consider a computer system that runs Linux operating system and simultaneously host a virtual machine that runs Windows operating system. Here, the Windows operating system will only have access to hardware that is allocated to virtual machines. Hardware virtualization plays an important role in provisioning the IaaS service of cloud computing. Some of the other virtualization technologies for which virtual environments are provided are networking, storage, and desktop. The overall environment of virtualization may be divided into three layers: host layer, virtualization layer, and guest layer. The host layer denotes a physical hardware device on which the guest is maintained. Virtualization layer act as the middleware which creates a virtual environment similar to the real computer environment to execute a guest virtual application. Here guests always communicate through the virtualization layer and it may denote a virtual machine or any other virtual application. A diagrammatic representation of the virtualization environment is shown in Figure 1.

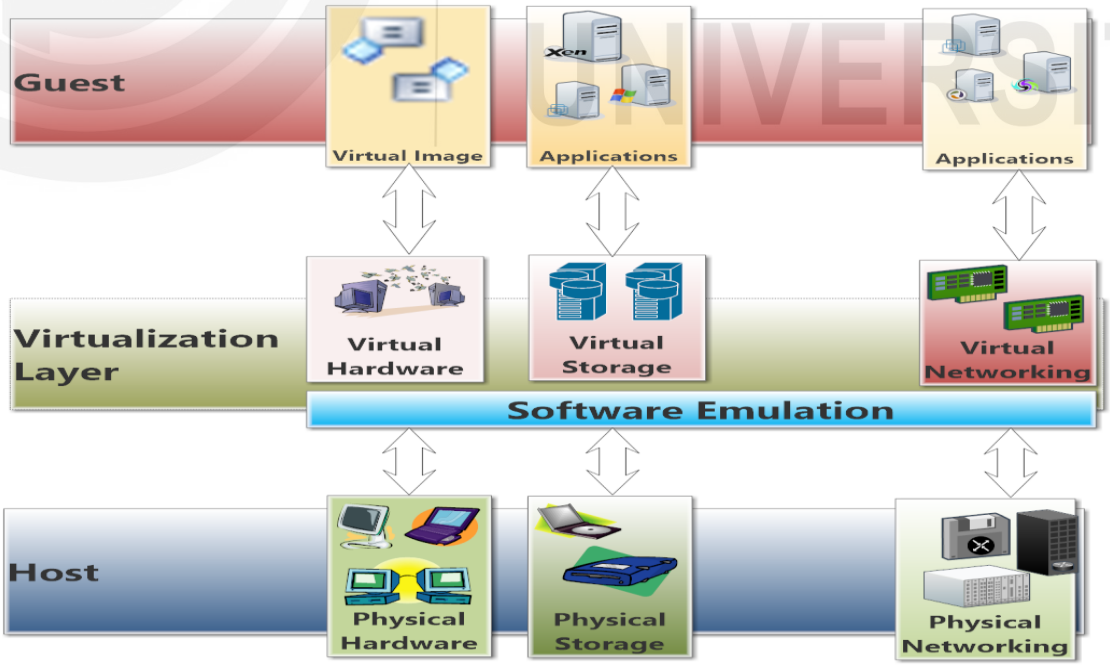

Figure 1: Diagram showing the virtualization environment.

From the above discussion, it should be noted that in reality, the virtualization environment is a software program, and hence virtualization technology has better control and flexibility over the underlying environment. The capability of software to imitate a real computing environment has facilitated the utilization of resources in an efficient way. In the last few years, virtualization technology has drastically evolved and the current version of technology allows us to make use of the maximum benefit that virtualization provides. In this respect some of the important characteristics of virtualization can be discussed as follows:

- ➔ Advancement in Security: In reality, more than one guest virtual machine runs on a single host machine, and on each virtual machine different virtual applications are executed. Further, it is very important to run each virtual machine in isolation such that no two applications running on different virtual machines interfere with each other. In this respect, virtual machine manager (VMM) plays an important role by managing virtual machines efficiently and providing enough security. The operations of the different virtual machines are observed by VMM and filtered accordingly such that no unfavorable activity is permitted. Sometimes it becomes important to hide some sensitive or important data of the host from other guest applications running on the same system. This kind of functionality is automatically provided by the virtualization environment.

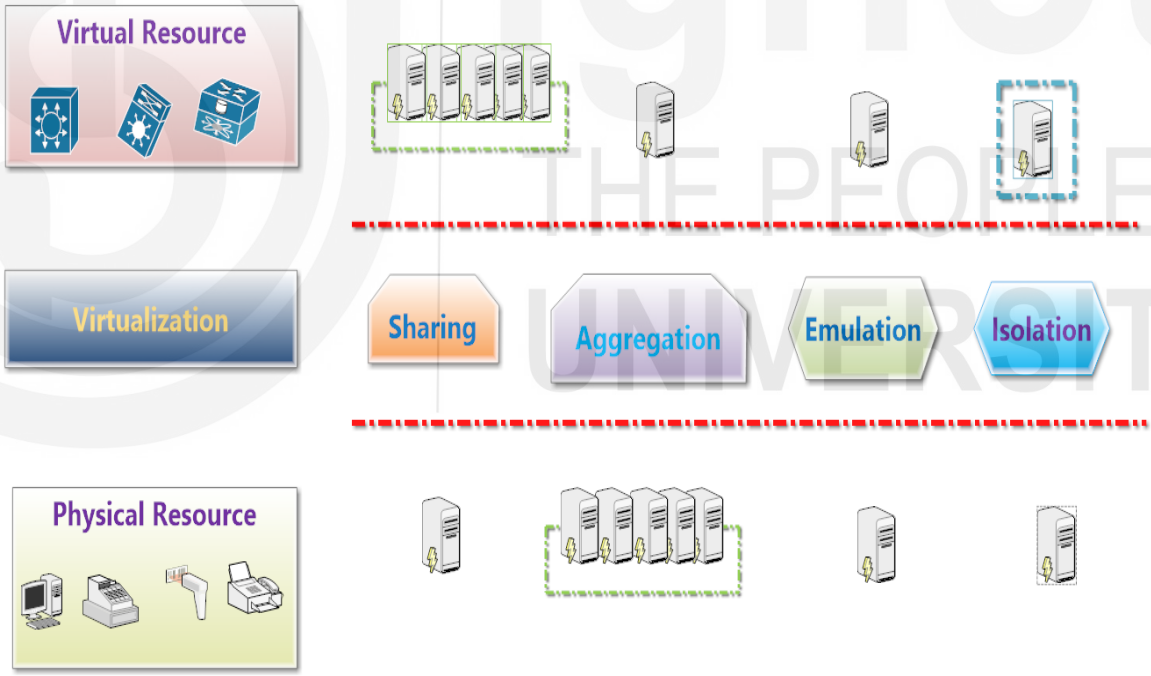

Figure 2: Features provided by virtualization environment

- ➔ Managing of Execution: In addition to the features like security, sharing, aggregation, emulation, and isolation are also considered to be important features of virtualization. The explanation of these features are as follows:

- Sharing: Virtualization technology allows the execution of more than one guest virtual machine over a single host physical machine. Here, the same hardware resources are being shared by all the guest virtual machines. Here sharing of existing hardware resources and using individual physical machines to their optimum capacity help to minimize the requirement of a number of servers and the power consumption.

- Aggregation: Virtualization technology allows to combine, the resources of different independent host machines and seems to guest as one virtual host. The cluster management software is one of the very good examples of distributed computing. Cloud computing environments also make use of these features.

- Emulation: Virtualization environment allows different guest applications to run on top of the host physical machine. Here the underlying virtualized environment is a software program and hence can be controlled more efficiently. Further, based on the requirement of guest application or program the underlying environment can be adjusted or modified for smooth execution.

- Isolation: Virtualization environment enables guest virtual machines to run in isolation such that no virtual machine running on the same host physical machine interferes with each other. The guest virtual application accesses the underlying resources through the abstraction layer. The virtual machine manager monitors the operation of each guest application and try to prevent vulnerable activity operation if any.

Virtualization technology is adopted by different areas of computing. Further, based on the requirements and uses different virtualization techniques were developed and each technique has its own unique characteristics. In this regard Figure 3. shows a detailed classification of virtualization techniques. We will be discussing some of the techniques in detail in the later sections.

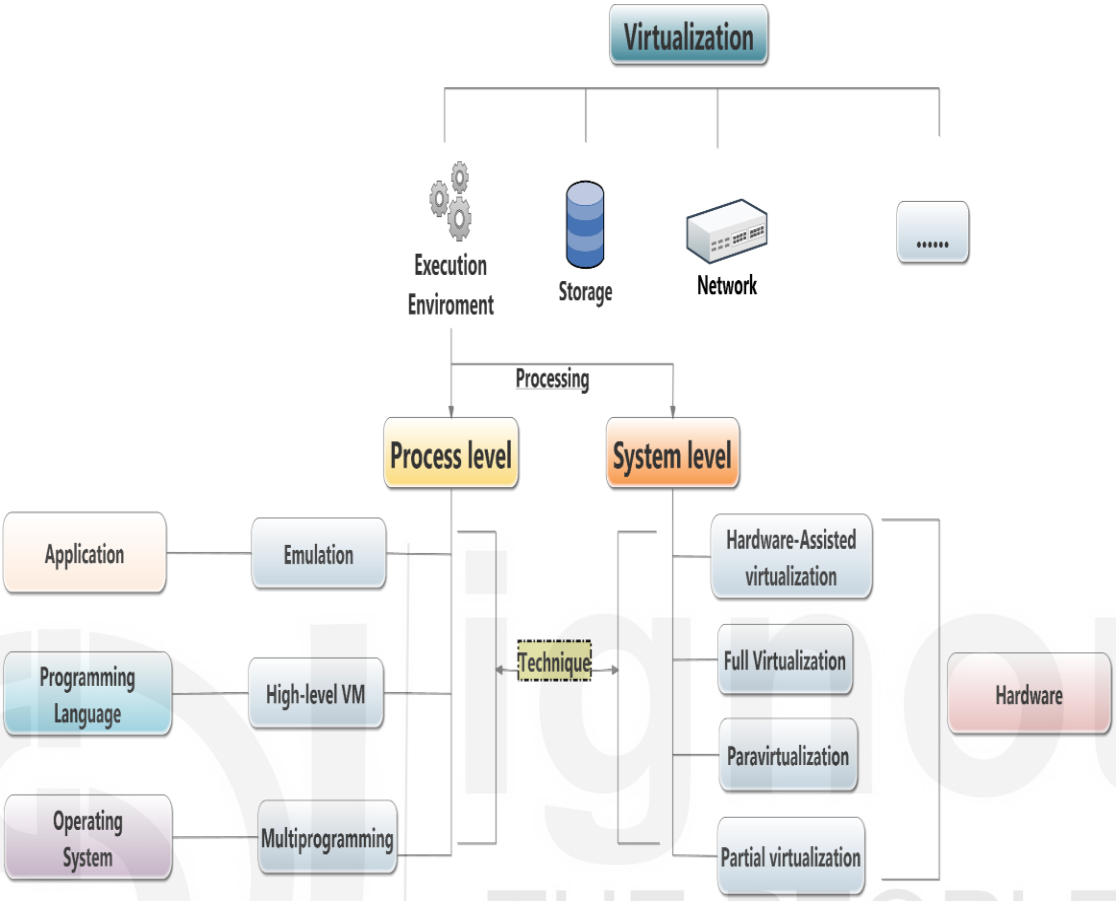

Figure 3: A classification of virtualization technique

Check your Progress 1

1) Explain the importance of virtualization in cloud computing?

……

……

……

2) How security is achieved through virtualization?

……

……

……

3) Emulation and isolation are important features of virtualization. Justify the statement.

……

……

.....
.....

.....
.....

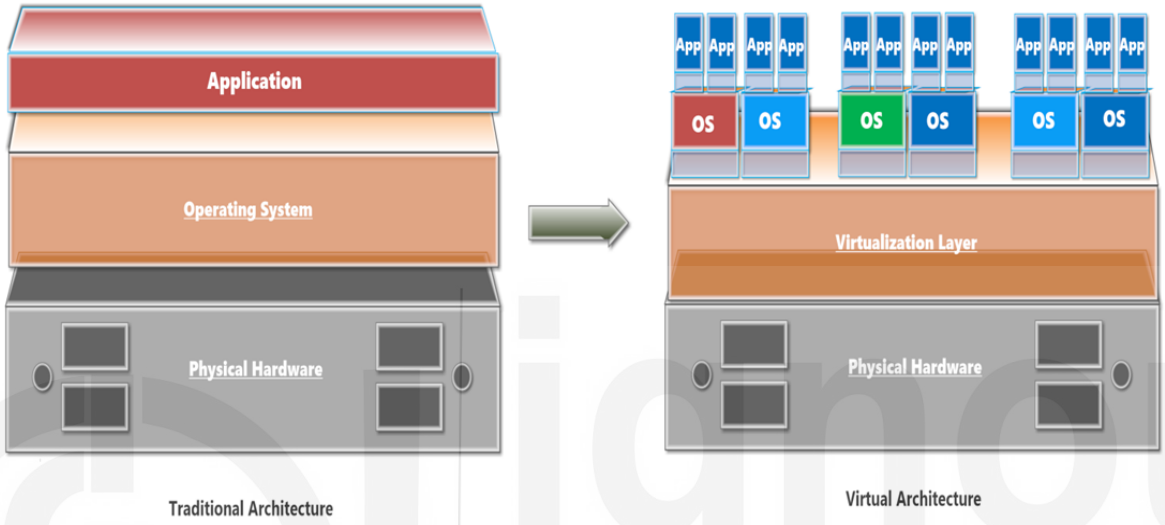

Figure 4: Diagram showing the traditional and virtual architecture

3.4 Advantages of Virtualization

As discussed earlier, virtualization creates an abstracted layer over the available hardware elements, such as a processor, storage, and memory allowing them to disperse over several Virtual Computers, also known as Virtual Machines (VMs). The importance of virtualization was realized when IT industries were facing difficulty to overcome the problem of x86 servers which enable running of only a single operating system and application. The virtualization technology paved the way for the existing IT industry by maximizing the utilization of individual servers and enabling them to operate at their maximum capacity. In this regard Figure 4. shows the difference in traditional and virtual architecture. Further when we compare the older virtualization technique with the current version then we will notice that the older virtualization technique used to support only a single CPU and it was slow. Further, the current version of virtualization techniques has improved a lot and it was found that virtual machines may execute server applications as well as bare metal computer systems.

In order to improve performance, and to maximize the availability and reliability of the service, virtualization allows virtual machines to move from one host machine to another and this is called a virtual machine migration. The migration of virtual machines is achievable as the underlying environment is virtual. The virtual machine migration can be achieved offline or live. In case of offline migration the guest virtual machine is temporarily stopped and after copying the image of the virtual machine's memory to the destination host machine virtual machine is restarted. Next in the case of live migration an active virtual machine is moved from one host machine to another. It should also be noted that virtualization technology prefers to migrate virtual machines from one host machine to another when some kind of load balancing is required. The type of virtual machine is chosen based on the requirement, that is if downtime is permissible then offline migration is preferred, or else live migration is preferred.

Virtualization allows for more efficient use of underlying resources, resulting in a higher return on a company's hardware investment. Some other advantages of virtualization may also be highlighted and it can be summarized as follows:

- **Reducing Power Need:** Virtualization helps to run more than one operating system and application on a single physical system. This allows to reduce the requirement of more servers and hence reducing the requirement of energy for running and cooling the physical machines.
- **Lower Cost:** Virtualization of hardware or software resources help to maximize the utilization of individual resources without compromising with the performance. Thus the extra investment on the servers is minimized by running more than one operating system and application on a single server. In addition to this, the requirements for extra space are also reduced. In this way virtualization technology is helping IT industries to achieve maximum benefit at a minimal cost.
- **Better Availability:** Virtualization technology allows to overcome the problem of sudden downtime due to hardware fault or human-induced fault. That is virtualization provides a fault-tolerant environment in which applications are run seamlessly. Virtualization allows better control and flexibility over the underlying environment when compared to the standalone system. Further, during the time of fault or system maintenance, virtualization technology may use live migration techniques to migrate virtual machines from one server to another. Any application or operating system crash results in downtime and lowers user productivity. As a result, administrators can use virtualization to run many redundant virtual computers that can readily handle this situation. However running numerous redundant Physical Servers, on the other hand, will be costly.
- **Resource Efficiency:** We may run numerous applications on a single server with virtualization, each with its own virtual machine, operating system, and without sacrificing the Quality of Services like reliability and availability. In this way, virtualization allows efficient use of the underlying physical hardware.
- **Easier Management:** In software-defined virtual machines, it is much easier to implement any new rule or policy, making it much easier to create or alter policies. This may be possible as virtualization technology provides better control over the virtual environment.
- **Faster Provisioning:** The process of setting up hardware for each application is time-consuming, requires more space, and costs more money. Further provisioning a virtual machine (VM) is faster, cheaper, and efficient and can be managed smoothly. Thus virtualization technology may help to create the required configured virtual machines in minimum time and may also be able to scale up or scale down the required demands in minimum time. Here it should be noted that the problem of scalability may also be handled efficiently by virtualization techniques.
- **Efficient resource management:** As discussed earlier, virtualization provides better control and flexibility when compared to traditional architecture. Virtualization allows IT administrators to create and allocate the virtual machine faster and live- migrate the virtual machine from one server to another when required to increase the availability and reliability of the services. In order to manage the virtualized environment, there are a number of virtualization management tools available and the selection of appropriate tools may help to manage the virtual resources efficiently. This tool may help to seamlessly migrate the virtual machine from one system to another with zero downtime. This may be required when any server needs maintenance or is not performing well.
- **Single point Administration:** The virtualized environment can be managed and monitored through single virtualization management tools. However, the selection of efficient tools that

provide all the virtualization services properly is important. The appropriate tool will help to create and provision virtual machines efficiently, balance the workload, manage the security of the individual virtual machines, monitor the performance of the infrastructure, and guarantee to maximize the utilization of the resources. Here all the different services can be administered by a single tool.

3.5 Machine or Server Level Virtualization

Server virtualization is a technique to divide a physical server into various small virtual servers and each of these independent virtual servers runs its own operating system. These virtual servers are also called virtual machines and the process of creation of such virtual machines is achieved by hypervisors like Microsoft Hyper-V, Citrix XenServer, Oracle VM, Red Hat's Kernel-based Virtual Machine, VMware vSphere. Here it should be noted that each virtual machine runs in isolation on the same host physical machine and are unaware of any other virtual machine running on the same host physical machine. To achieve this kind of functionality and transparency different kinds of virtualization techniques are used. Further, there are different types of server-level virtualization and they are as follows:

- ★ Hypervisor
- ★ Para Virtualization
- ★ Full Virtualization
- ★ Hardware-Assisted Virtualization
- ★ Kernel level Virtualization
- ★ System-Level or Operating System Virtualization

There are numerous advantages associated with server virtualization. Some of them are as follows:

- ➔ In the case of server virtualization, each virtual machine may be restarted independently without affecting the execution of other virtual machines running on the same host physical machine.
- ➔ Server virtualization can partition a single physical server into many small virtual servers and allows to utilize the hardware of the existing physical servers efficiently. Therefore this minimizes the requirement of the extra physical servers and the initial investment cost.
- ➔ As each small virtual server executes in isolation, if any virtual machine faces any kind of issues then it will not affect the execution of other virtual machines running on the same host physical machine.

In addition to some of the advantages server virtualization also have some disadvantages and they are as follows:

- ➔ In the case of a host physical machine, the server faces any problem and it goes offline then all the guest virtual machines will also get affected and will go offline. This will decrease the overall uptime of the services or applications running on an individual virtual machine.
- ➔ Server virtualization allows the running of many numbers of virtual machines on the same physical server, this may reduce the performance of the overall virtualized environment.
- ➔ Generally, server virtualization environments are not easy to set up and manage.

3.6 Hypervisor

The hypervisor can be seen as an emulator or simply a software layer that can efficiently coordinate and run independent virtual machines over single physical hardware such that each virtual machine has physical access to the resources it needs. It also ensures that virtual machines have their own address space and execution on one virtual machine does not conflict with the other virtual machine running on the same host physical machine.

Prior to the notion of Hypervisor, most computers could only run one operating system at most and this increased the reliability of the services and applications because the entire system's hardware had to handle requests from a single operating system. However, the demerit of this idea is that the system cannot utilize all of the computing capacity. However, using a hypervisor minimizes the need for space, energy, and maintenance. The hypervisor is also referred to as a virtual machine monitor and it helps to manage virtual machines and their physical resource demands. It isolates virtual machines from one another by logically provisioning and assigning computing power, memory, and storage. Thus at any point of time if any virtual machine operation is vulnerable then it will not affect the execution of another machine.

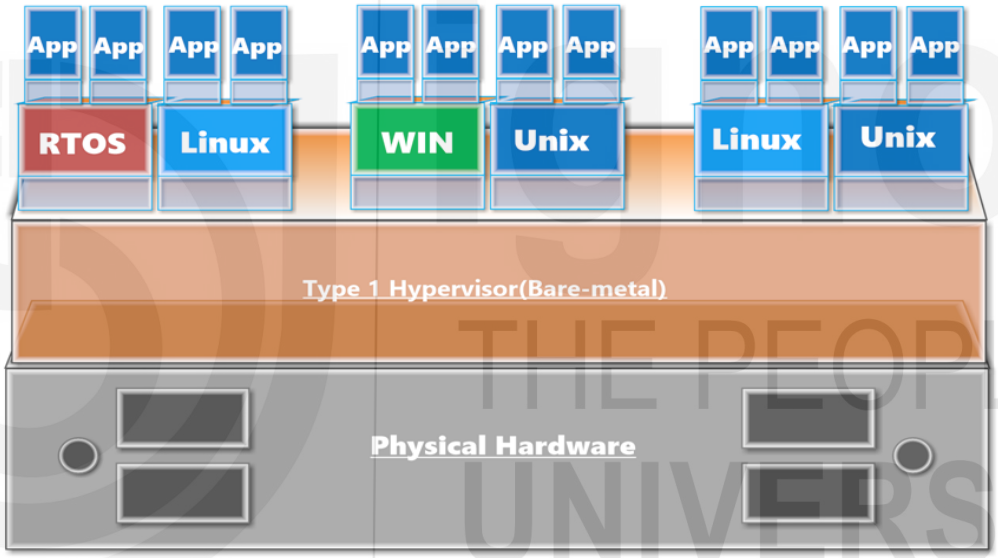

Figure 5: Type 1 Hypervisor

There are basically two types of hypervisor (i) Type 1 or bare metal and (ii) Type 2 or Hosted. Hypervisors enable virtualization because they translate requests across virtual and physical resources. Type 1 hypervisors may also be embedded into the firmware around the same layer as the motherboard basics input/output system (BIOS). This helps the host operating system to access and use the virtualization software.

- ➔ **Type 1 hypervisor:** This is also termed as “Bare metal” hypervisor. This type of hypervisor runs directly on the underlying physical resources. For running this kind of hypervisor operating system is not required and it itself acts as a host operating system. These kinds of hypervisors are most commonly used in virtual server scenarios (See Figure 5.).

Pros: These types of Hypervisor are highly effective as they can directly communicate with physical hardware. It also raises the level of security, and there was nothing in between them that could undermine security.

Cons: To administrate different VMs and manage the host hardware, a Type 1 hypervisor frequently requires a separate administration system.

Example:

Hyper-V hypervisor: Hyper-V is a Microsoft-designed hypervisor for use on Windows systems. It is classified as a Type 1 hypervisor, although it differs from other Type 1 hypervisors in that it does not install on Windows and instead runs directly on the actual hardware as the Host OS. As a result, it gains a performance edge.

Citrix XenServer: It is a commercial Type 1 Hypervisor that supports Linux and Windows OS. It was developed by IBM and is generally known as Citrix hypervisor. Xen supports virtualization technologies such as Intel VT and AMD-V hardware-assisted environments. It also supports paravirtualization, which alters the guest OS to work with the hypervisor, improving performance.

ESXi hypervisor: VMware ESXi (Elastic Sky X Integrated) is a bare-metal hypervisor mainly designed for server virtualization in the Data Center. It can efficiently manage the group of Virtual machines.

VSphere hypervisor: Customers can download VMware ESXi for free as part of the Free vSphere hypervisor, which also offers basic server virtualization. Large businesses will purchase a more comprehensive vSphere solution that includes a VMware's vCenter Server license. It is a separate server used to manage the vSphere environment on physical hosts.

➔ **Type 2 hypervisor:** This hypervisor is not compatible with the hardware it is running on. It runs as a program on a computer's operating system. This type of hypervisor takes the help of an operating system to deliver virtualization-based services. Type 2 hypervisors are best suited for endpoint devices such as personal computers that run an alternative operating system known as Guest OS. Type 2 hypervisors frequently provide a different toolkit that enhances the connection between Guest and Host operating systems (See Figure 6.).

Pros: A type 2 hypervisor allows for rapid and easy access to a Guest OS while the main operating system runs on the host physical machine. This kind of facility immensely helps the end-user in their work. For example, a user can use Cortana to access their favorite Linux-based tool (in Windows, only found a speech dictation system).

Cons: Type 2 hypervisors can cause performance overhead because they always need a host operating system in between the guest Operating system and underlying physical device. It also poses latency concerns and a potential security risk if the Host OS is compromised.

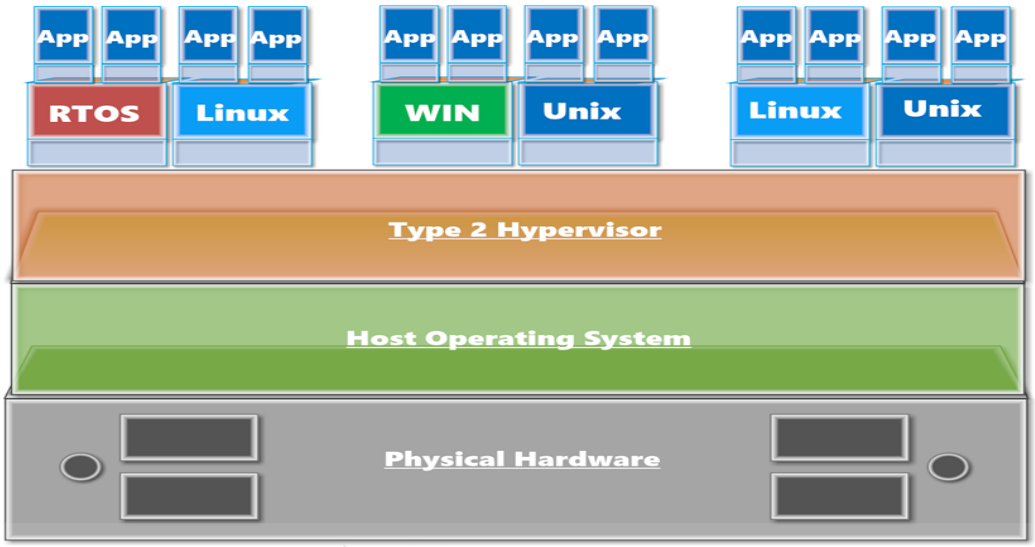

Figure 6. Type 2 Hypervisor

Example:

VMware Workstation: It is the product of VMware focused on Linux and Windows users, and its free Version (Player) allows it to run a single guest OS while its paid version(Pro) allows users to run multiple operating systems on a single personal computer.

Check your Progress 2

1) Explain live and offline virtual machine migration.

……
……

……
……

……
……

2) Write three advantages and disadvantages of server virtualization.

……
……

……
……

……
……

3) Compare between Type 1 hypervisor and Type 2 hypervisor.

……
……

……
……

……
……

3.6.1 Full Virtualization:-

Full virtualization is a technique to run an application or operating system directly on a VM without any alteration and it seems to the operating system that it is running on the real physical hardware. In order to achieve this, the virtual machine manager provides an environment that fully imitates the complete real hardware. In other words, full virtualization is a strategy for creating a virtual machine environment that entirely imitates the physical hardware. Every software can run on the underlying devices executed in the Virtual machine. One of the important benefits with respect to full virtualization is that it allows the execution of the unaltered guest operating systems in isolation. These kinds of features provide extra security and enable the running of different unmodified operating systems in the same environment. For example in the case of operating design, newly developed code for experiments can run alongside previous versions of operating systems in isolated virtual machines. The virtual machine manager helps each virtual machine to obtain all of the existing services of the underlying physical system. The virtual machine completely isolates the guest operating system from the underlying hardware.

A binary translation and direct execution are used together to accomplish full virtualization. The hardware CPU runs non-sensitive commands at normal speed for full virtualization hypervisors. Operating system-related instructions are interpreted on the fly for further use. As similar kinds of guest operating system instances can execute on virtualized or real physical systems, the full virtualization technique delivers the most required isolation and security solution for virtual instances running on the virtual environment (see Figure 7).

Further, binary translation is a method of establishing full virtualization that does not necessitate hardware virtualization. It entails looking for "unsafe" instructions in the virtual guest's executable code, translating them into "safe" equivalents, and running the translated code. If we talk with respect to VMware hypervisor, both direct execution and binary translation techniques may be used to virtualize an operating system.

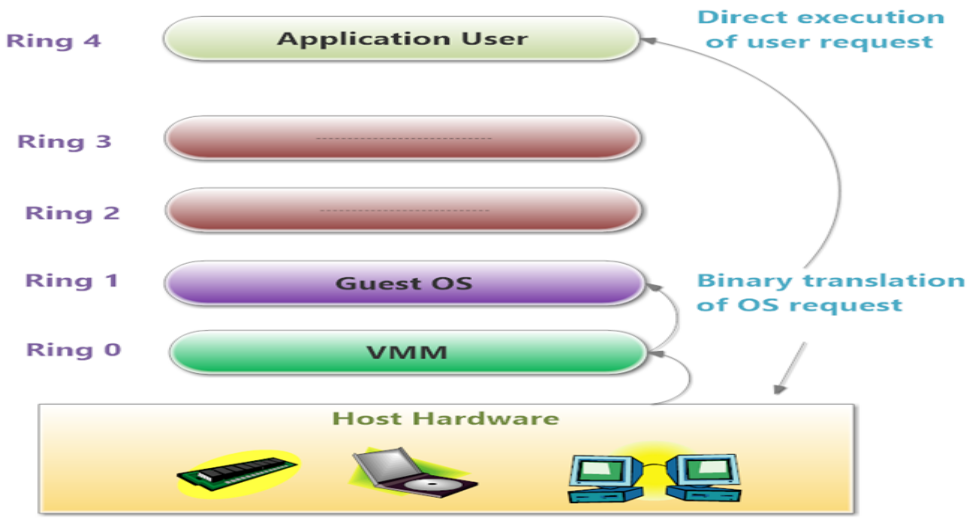

Figure 7: The figure depicts the full virtualization paradigm.

3.6.2 Paravirtualization:-

Paravirtualization is a virtualization approach for computing devices that enables virtual machines (VMs) to get an interface comparable to the underlying or guest hardware. This strategy seeks to increase the VM's performance (OS) by altering the guest operating system. The guest OS is updated within paravirtualization. It recognizes that it is executing in a virtualized environment on top of something like a hypervisor (the VM's hardware) rather than on actual hardware.

Paravirtualization, which means "alongside virtualization," refers to communication between the guest OS and the hypervisor to improve performance and efficiency. As shown in Figure 8 paravirtualization entails replacing non-virtualizable instructions, with hyper calls connecting directly, with the hypervisor's virtualization layer. Other essential kernel tasks, including memory management, interrupt handling, and timekeeping, have hyper-call interfaces provided by the hypervisor.

Full virtualization, in which the unmodified OS is unaware that it is virtualized and sensitive OS calls are captured using binary translation, is not the same as paravirtualization. Paravirtualization's value proposition is decreased virtualization overhead. However, the performance advantage of paravirtualization over full virtualization varies substantially depending on the workload. Paravirtualization's compatibility and portability are limited because it cannot support unmodified operating systems (e.g., Windows 2000/XP). Because it necessitates profound OS kernel alterations, paravirtualization can cause substantial support and maintainability concerns in production situations. The open-source Xen project, for example, uses a modified Linux kernel to virtualize the processor and memory and proprietary guest OS device drivers to virtualize the I/O.

While the more complex binary translation support required for full virtualization is complicated, changing the guest OS to enable paravirtualization is reasonably

straightforward. For years, VMware has deployed paravirtualization approaches in VMware tools and optimized virtual device drivers throughout the VMware product range. The VMware tools service gives access to the VMM Hypervisor's backdoor, which can do tasks like time synchronization, logging, and guest termination. Vmxnet is a hypervisor-sharing para-virtualized I/O device driver. It can take advantage of the capabilities of the host device to increase throughput while lowering CPU usage. The VMware tools service and the VMXnet device driver are not CPU paravirtualization solutions, which should be noted for clarity. They are minor, non-intrusive adjustments that do not require any changes to the guest OS kernel. VMware is assisting development in the future. In the future, VMware will assist in creating para-virtualized Linux versions to enable proofs of concept and product development.

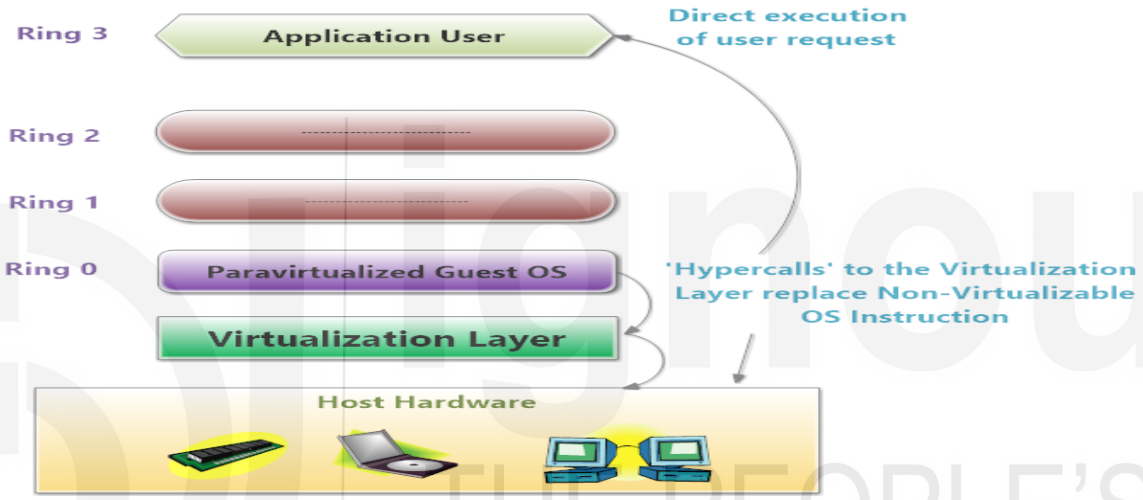

Figure 8: The figure depicts the paravirtualization paradigm

3.6.3 Hardware-Assisted Virtualization:-

The other name for this virtualization is native virtualization, accelerated virtualization, or hardware virtualization. In this type of virtualization, a special CPU instruction is provided by real physical hardware to support virtualization. The adopted methodology is very portable as the virtual machine manager can run an unaltered guest operating system. This kind of methodology minimizes the implementation complexity of the hypervisor and allows the hypervisor to manage the virtualized environment efficiently. This sort of virtualization technique was initially launched on the IBM System / 370 in 1972, and it was made available on Intel and AMD CPUs in 2006. In this kind of virtualization methodology, sensitive calls are by default forwarded to the hypervisor. It is no longer necessary to use binary translation during full virtualization or hyper calls during paravirtualization. See Figure 9 depicts the hardware-assisted virtualization techniques.

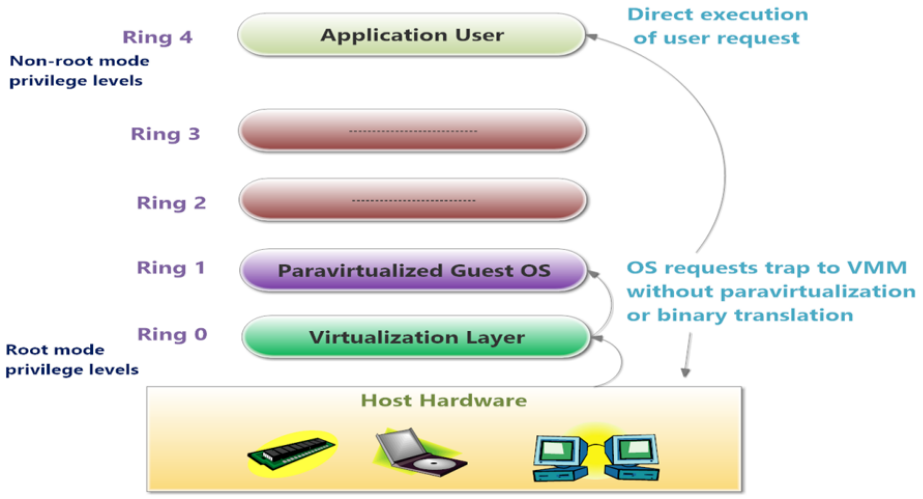

Figure 9: The figure depicts the hardware-assisted virtualization techniques.

3.7 Network virtualization:-

Network virtualization is the process of converting a hardware-dependent network into such a software-based network. The underlying purpose of network virtualization is to virtualize network routing protocol, forwarding, and different addressing schemes. Further, network virtualization will also allow every form of IT virtualization to create a layer of abstraction between virtual hardware and the activities that use it. Network virtualization, in particular, allows network functionalities, hardware resources, and software resources to be offered as a virtual network, independent of hardware. It is used to join virtual machines (VMs), partition a physical network, or merge many physical networks. IT can improve digital service providers' overall performance, flexibility, and reliability.

3.8 Storage virtualization:-

Storage virtualization (sometimes referred to as software-defined storage or virtual SAN) is the process of combining different physical massive volumes of data from SANs into a virtualized storage device. The pool may combine disparate storage gear from multiple networks, manufacturers, or data centers into a unified logical perspective and control it through a single window. Virtualizing storage removes the storage management software from the underlying physical infrastructure to give more flexibility and sustainable pools of storage resources. Furthermore, it may abstract storage hardware (arrays and discs) into online storage pools. Figure 10 shows the storage virtualization.

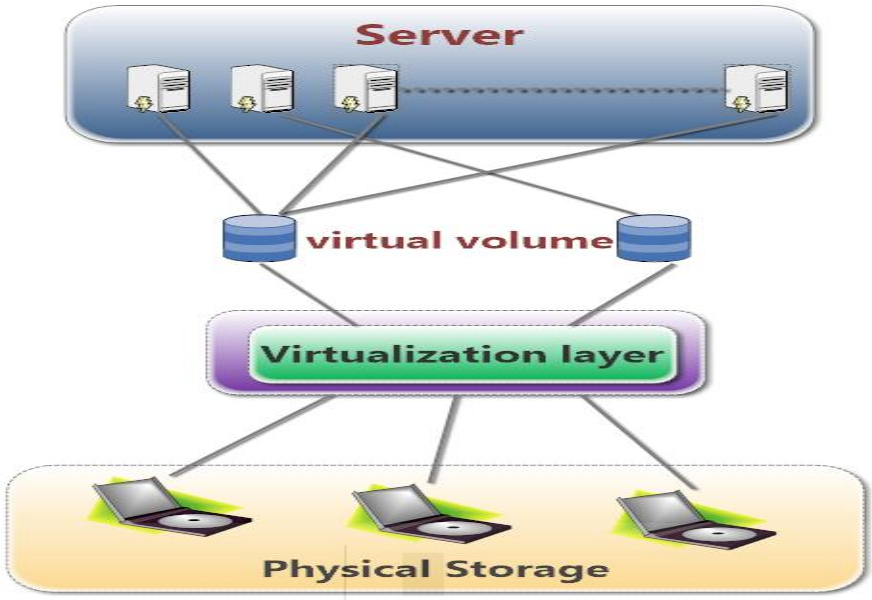

Figure 10: Depicts the Storage virtualization

3.9 Desktop virtualization:-

In this type of virtualization, a software-based virtualized version of users' workstations is created such that the virtual environment may be accessed from any place remotely. This type of virtualized environment may enable any user to connect themselves through any devices having network connectivity. A very important element of digital workspace includes desktop virtualization. In a desktop virtualization environment, mostly virtual machines are used to run the workload. Further, it should be also noted that, in this type of virtualization technique, all the information and data of end-users are present in the server. Thus risk involved with respect to loss of any user data is minimum if devices are lost. There are a number of ways through which desktop virtualization may be implemented. However, the most acceptable ones are local and remote desktop virtualization.

3.10 Operating system virtualizations:-

Operating system virtualization is a modified version of a standard operating system that allows several users to access and use different applications. This entire procedure should be completed on a single machine at a time. The virtual vision environment within operating system virtualizations accepts commands from any client operating it and does various tasks within the same machine while running various applications. Whenever an operating system virtualization occurs, a program does not interfere with another even though they run on the same computer. An operating system's kernel allows for the existence of several segregated user-space instances. Software containers, or virtualization engines, are what these instances are referred to as. Operating system Virtualization is of two types (i) Linux Virtualization and (ii) Windows Virtualization.

- **Linux Operating System virtualization:** To virtualize Linux computers, VMware Workstation software is utilized. Furthermore, to install any software using virtualization, the user must first install VMware software.

- **Windows Operating System Virtualizations:** This sort of virtualization is similar to the previous in that it requires the installation of VMware software before any other software can be installed.

3.11 XenServer Vs VMware

Next, we will discuss the major difference between two very well-known hypervisors Citrix XenServer and VMware.

VMware vSphere ESXi Hypervisor	**Citrix XenServer Hypervisor**
VMware is generally used by small and mid-sized businesses. VMware requires a proprietary license and is Provided per-processor basis.	Citrix XenServer is a virtualization platform that is utilized by individuals as well as small and medium businesses. XenServer is Open source and also provides per-server licensing. However, the free version also includes almost all the features.
Features like dynamic resource allocation is supported	The features like dynamic resource allocation is not supported
VMware has 128 Virtual CPUs (VCPUs) per Virtual machine. It can run on either Intel-Vt or AMD-V intelligent devices.	Citrix XenServer has 32 Virtual CPUs per Virtual machine. It can only run on Intel-Vt or AMD-V intelligent systems.
Only MS-DOS and FreeBSD are supported as hosts in VMware vSphere. As a guest OS, VMware vSphere supports MS-DOS, Sun Java Desktop System, and Solaris X86 Platform Edition.	Citrix XenServer supports various host OS such as Win NT Server, Win XP, Linux ES, e.t.c. Citrix XenServer also supports various guest operating systems, but not MS-DOS, Sun Java Desktop Environment, or Solaris X86 platform edition. To run, it will need AMD-V competent hardware.
Support Failover and Live migration. Supports Dynamic Resource allocation and Thin Provisioning.	Doesn't support Failover or even Live migration.(* Newer version supports Live migration but not that efficiently). Supports only Thin Provisioning.
The graphic support is not exhaustive.	The graphic support is exhaustive and had better support than VMware.
BusyBox is used by the VMware server management system for managing the environment.	It provides almost all the required features and ability to create and manage the virtualization environment and it uses XenCenter for managing the environment.

Check your Progress 3

1) **What is the difference between full virtualization and paravirtualization?**

……
……
……
……
……
……

2) **Discuss briefly network and storage virtualization.**

……
……
……
……
……
……

3) **State that the statement is True (T) and False (F):**

a. Full virtualization is a technique to run an application or operating system directly on a VM without any alteration and it seems to the operating system that it is running on the real physical hardware. [ ]

b. A binary translation and direct execution are used together to accomplish full virtualization. [ ]

c. Paravirtualization, which means "alongside virtualization," refers to communication between the guest OS and the hypervisor to improve performance and efficiency.[ ]

d. Native virtualization is also called as Hardware-Assisted Virtualization [ ]

e. Network virtualization is the process of converting a software-dependent network into such a hardware-based network. [ ]

3.12 SUMMARY

Virtualization is the fundamental technology that helps to create an abstraction layer over the available System hardware elements like processor, storage, and memory. Virtualization allows to

hide the intricacy of the underlying environment and provides a secure and isolated environment for any user application. The created computing environment is virtual and it simulates an environment similar to a real computer. The use of the virtual infrastructure is smooth as the user finds almost no difference in the experience when compared to a real computing environment. In this regard, a detailed overview of virtualization is given in this unit. We have discussed some very important topics related to virtualization like advantages of virtualization, different virtualization techniques, and its characteristics with an example. For further clarity of existing virtualization techniques like full virtualization and paravirtualization, we have compared the two very well-known hypervisors Citrix XenServer and VMware.

3.13 SOLUTIONS/ANSWERS

Check your Progress 1

Ans 1: Cloud Computing is a framework where different kinds of services related to networks, computing resources, storage, development platform, and application are provisioned through the internet. Further, Virtualization is the fundamental technology that creates an abstraction to hide the complexity of computing infrastructure, storage, and networking. The virtualization technique provides a secure and isolated environment for cloud users such that the computing environment of one user does not affect the computing environment of another user.

Ans 2: In the case of virtualization more than one guest virtual machine runs on a single host machine, and on each virtual machine different virtual applications are executed. Further, it is very important to run each virtual machine in isolation such that no two applications running on different virtual machines interfere with each other. In this respect, virtual machine manager (VMM) plays an important role by managing virtual machines efficiently and providing enough security. The operations of the different virtual machines are observed by VMM and filtered accordingly such that no unfavorable activity is permitted. Sometimes it becomes important to hide some sensitive or important data of the host from other guest applications running on the same system. This kind of functionality is automatically provided by the virtualization environment with the help of VMM.

Ans 3: In the case of emulation, the virtualization environment allows different guest applications to run on top of the host physical machine. Here the underlying virtualized environment is a software program and hence can be controlled more efficiently. Further, based on the requirement of guest application or program the underlying environment can be adjusted or modified for smooth execution.

In case of isolation, the virtualization environment enables guest virtual machines to run in isolation such that no virtual machines running on the same host physical machine interfere with each other. The guest virtual application accesses the underlying resources through the abstraction layer. The virtual machine manager monitors the operation of each guest application and tries to prevent vulnerable activity operation if any.

Check your Progress 2

Ans 1: Virtualization maximizes the availability and reliability of the service, by allowing virtual machines to move from one host machine to another and this is called a virtual machine migration. The migration of virtual machines is achievable as the underlying environment is virtual. The virtual machine migration can be achieved offline or live. In case of offline migration

the guest virtual machine is temporarily stopped and after copying the image of the virtual machine's memory to the destination host machine virtual machine is restarted. Next in the case of live migration an active virtual machine is moved from one host machine to another. It should also be noted that virtualization technology prefers to migrate virtual machines from one host machine to another when some kind of load balancing is required.

Ans 2: The advantages associated with server virtualization are as follows:

- In the case of server virtualization, each virtual machine may be restarted independently without affecting the execution of other virtual machines running on the same host physical machine.
- Server virtualization can partition a single physical server into many small virtual servers and allows to utilize the hardware of the existing physical servers efficiently. Therefore this minimizes the requirement of the extra physical servers and the initial investment cost.
- As each small virtual server executes in isolation, if any virtual machine faces any kind of issues then it will not affect the execution of other virtual machines running on the same host physical machine.

The advantages associated with server virtualization are as follows:

- In the case of a host physical machine, the server faces any problem and it goes offline then all the guest virtual machines will also get affected and will go offline. This will decrease the overall uptime of the services or applications running on an individual virtual machine.
- Server virtualization allows the running of many numbers of virtual machines on the same physical server, this may reduce the performance of the overall virtualized environment.
- Generally, server virtualization environments are not easy to set up and manage.

Ans 3: Type 1 hypervisor: This is also termed as "Bare metal" hypervisor. This type of hypervisor runs directly on the underlying physical resources. For running this kind of hypervisor operating system is not required and it itself acts as a host operating System. These kinds of hypervisors are most commonly used in virtual server scenarios. The examples are Hyper-V hypervisor, Citrix XenServer, and ESXi hypervisor.

Type 2 hypervisor: This hypervisor is not compatible with the hardware it is running on. It runs as a program on a computer's operating system. This type of hypervisor takes the help of an operating system to deliver virtualization-based services. Type 2 hypervisors are best suited for endpoint devices such as personal computers that run an alternative operating system known as Guest OS. An example is VMware Workstation.

Check your Progress 3

Ans 1: Full virtualization is a technique to run an application or operating system directly on a VM without any alteration and it seems to the operating system that it is running on the real physical hardware. In order to achieve this, the virtual machine manager provides an environment that fully imitates the complete real hardware. In other words, full virtualization is a strategy for creating a virtual machine environment that entirely imitates the physical hardware. Every software can run on the underlying devices executed in the Virtual machine. One of the important benefits with respect to full virtualization is that it allows the execution of the unaltered guest operating systems in isolation. These kinds of features provide extra security and enable the running of different unmodified operating systems in the same environment.

Paravirtualization is a virtualization approach for computing devices that enables virtual machines (VMs) to get an interface comparable to the underlying or guest hardware. This strategy seeks to increase the VM's performance (OS) by altering the guest operating system. The guest OS is updated within paravirtualization. It recognizes that it is executing in a virtualized environment on top of something like a hypervisor (the VM's hardware) rather than on actual hardware.

Ans 2:

a. True
b. True
c. True
d. True
e. False

Ans 3: Network virtualization is the process of converting a hardware-dependent network into such a software-based network. The underlying purpose of network virtualization is to virtualize network routing protocol, forwarding, and different addressing schemes. Further, network virtualization will also allow every form of IT virtualization to create a layer of abstraction between virtual hardware and the activities that use it. Network virtualization, in particular, allows network functionalities, hardware resources, and software resources to be offered as a virtual network, independent of hardware. It is used to join virtual machines (VMs), partition a physical network, or merge many physical networks. IT can improve digital service providers' overall performance, flexibility, and reliability.

Storage virtualization (sometimes referred to as software-defined storage or virtual SAN) is the process of combining different physical massive volumes of data from SANs into a virtualized storage device. The pool may combine disparate storage gear from multiple networks, manufacturers, or data centers into a unified logical perspective and control it through a single window. Virtualizing storage removes the storage management software from the underlying physical infrastructure to give more flexibility and sustainable pools of storage resources. Furthermore, it may abstract storage hardware (arrays and discs) into online storage pools.

9. FURTHER READINGS

There are a host of resources available for further reading on the topic of Virtualization.

1. R. Buyya, C. Vecchiola,, and S. T. Selvi, S. T. (2013). Mastering cloud computing: foundations and applications programming. Newnes.
2. S. A. Babu, M. J. Hareesh, J. P. Martin, S. Cherian, and Y. Sastri, "System Performance Evaluation of Para Virtualization, Container Virtualization, and Full Virtualization Using Xen, OpenVZ, and XenServer," 2014 Fourth International Conference on Advances in Computing and Communications, 2014, pp. 247-250, doi: 10.1109/ICACC.2014.66.
3. https://www.ibm.com/in-en/cloud/learn/hypervisors#toc-type-1-vs--Ik2a8-2y
4. https://www.vmware.com/topics/glossary/content/hypervisor.html
5. https://www.sciencedirect.com/topics/computer-science/full-virtualization#:~:text=Full%20virtualization%20is%20a%20virtualization,run%20in%20each%20individual%20VM.