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.

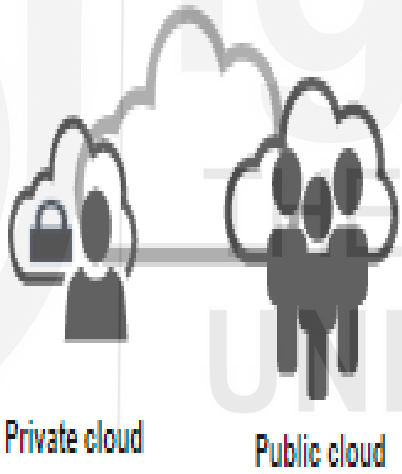

Fig. 2.2.4 Hybrid Cloud

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.

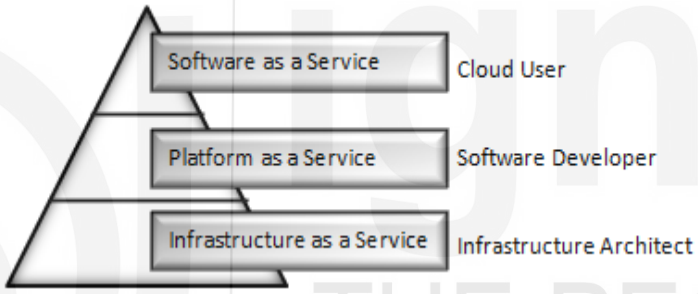

Fig. 2.4.1 Cloud Service delivery models

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

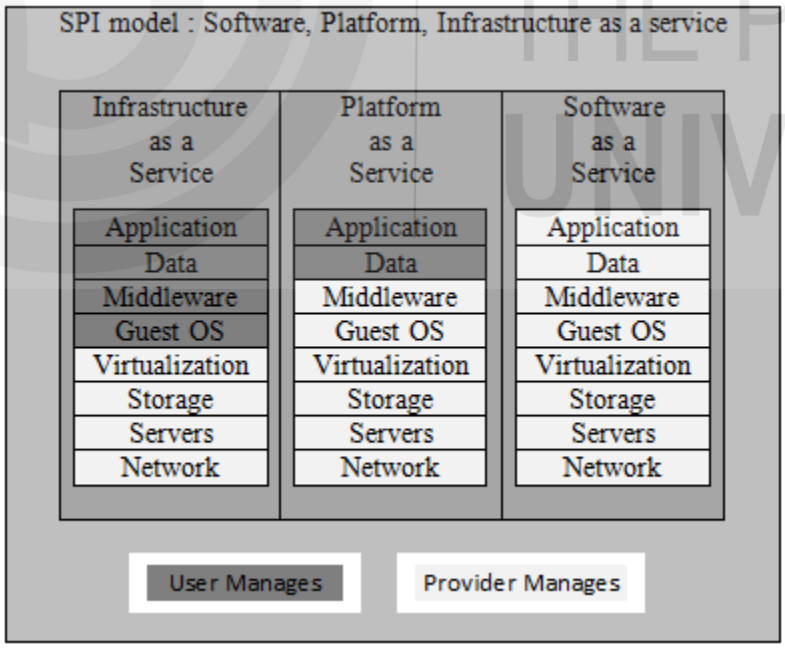

Fig. 2.4.2 Service provider and User management responsibilities of SPI model

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.

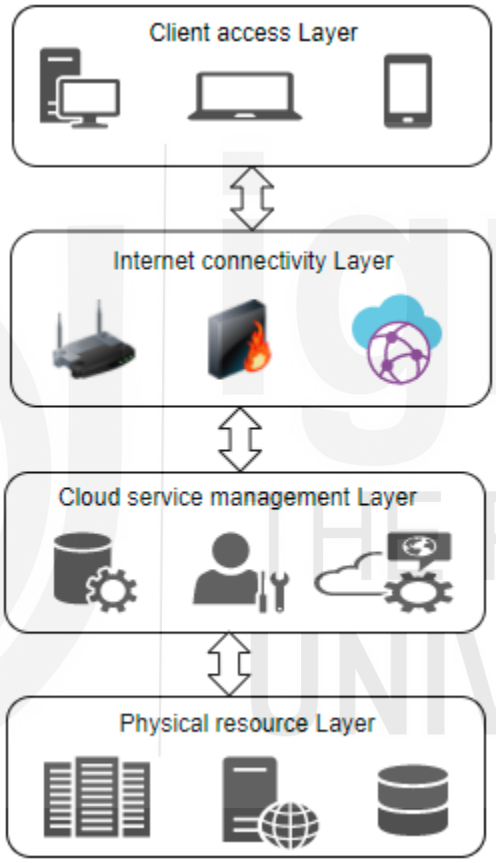

Fig. 2.5.1 Cloud Architecture

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.

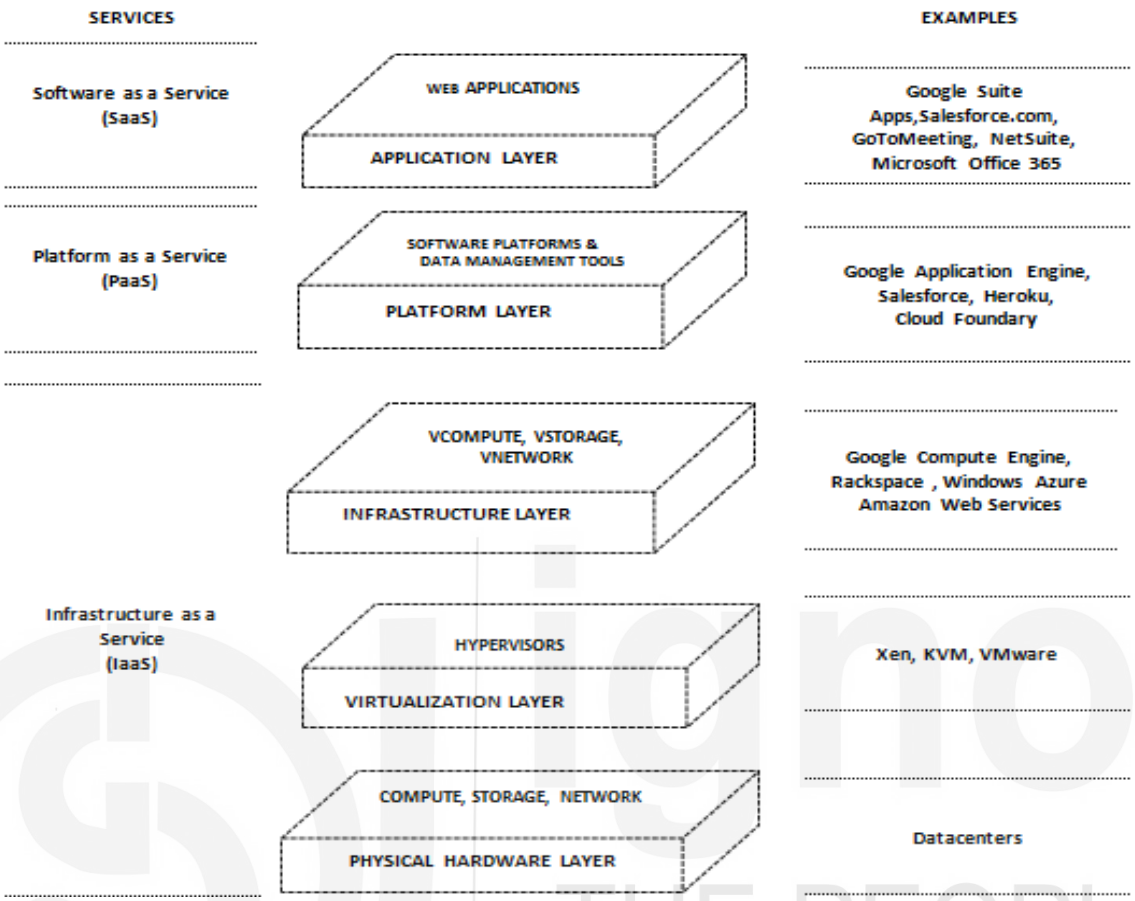

Fig.2.6.1 Layers of Cloud Anatomy

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.