A Report on Study of Public and Private Cloud with Implementation Technology

INTERN REPORT

By

Swagat S Kalita

Organization

National Institute of Electronics & Information Technology (NIELIT), ASSAM, INDIA.

S.R.M. Institute of Science and Technology, Kattankulathur, India.

2022-2023

CERTIFICATE

It is certified that Mr. Swagat S Kalita of 5th Semester, B.TECH-CSE Course of SRMIST, Kattankulathur has successfully completed the Research Study of Public and Private Cloud with Implementation Technology under 'FutureSkills PRIME' programme held in the Months of July-August,2022 and successfully submitted to NEILIT, Assam, Guwahati.

Date- 16-08-2022

Mr. Mridul Pachani
Senior Technical officer
NEILIT, Guwahati

ACKNOWLEDGMENT

I wish to express my heartfelt gratitude to the all the people who have played a crucial role in the research for this project, without their active cooperation the preparation of this project could not have been completed within the specified time limit.

I gratefully acknowledge for the assistance, cooperation, guidance and clarifications provided by NEILIT, ASSAM, INDIA during the Study of Public and Private Cloud with Implementation Technology.

I am thankful to our respected Mr Mridul Pachani (Senior Technical Officer, NEILIT, Guwahati), for motivating me to complete this project with complete focus and attention. Without his willing disposition, spirit of accommodation, frankness, timely clarification and above all faith in me, this project could not have been completed in due time.

Date: 16-08-2022 ***Name- Swagat S Kalita***

Abstract

Computers have become an indispensable part of life. We need computers everywhere, be it for work, research or in any such field. As the use of computers in our day-to-day life increases, the computing resources that we need also go up. For companies like Google and Microsoft, harnessing the resources as and when they need it is not a problem. But when it comes to smaller enterprises, affordability becomes a huge factor. With the huge infrastructure come problems like machines failure, hard drive crashes, software bugs, etc. This might be a big headache for such a community.

Cloud Computing offers a solution to this situation. Cloud computing is a paradigm shift in which computing is moved away from personal computers and even the individual enterprise application server to a 'cloud' of computers. A cloud is a virtualized server pool which can provide the different computing resources of their clients. Users of this system need only be concerned with the computing service being asked for. The underlying details of how it is achieved are hidden from the user. The data and the services provided reside in massively scalable data centers and can be ubiquitously accessed from any connected device all over the world.

Cloud computing is the style of computing where massively scaled IT related capabilities are provided as a service across the internet to multiple external customers and are billed by consumption. Many cloud computing providers have popped up and there is a considerable growth in the usage of this service. Google, Microsoft, Yahoo, IBM and Amazon have started providing cloud computing services. Amazon is the pioneer in this field. Smaller companies like SmugMug, which is an online photo hosting site, has used cloud services for the storing all the data and doing some of its services. Cloud Computing is finding use in various areas like web hosting, parallel batch processing, graphics rendering, financial modeling, web crawling, genomics analysis, etc.

Content Table

Chapter 1:

Introduction

The Greek myths tell of creatures plucked from the surface of the Earth and enshrined as constellations in the night sky. Something similar is happening today in the world of computing. Data and programs are being swept up from desktop PCs and corporate server rooms and installed in “the compute cloud”. In general, there is a shift in the geography of computation.

What is cloud computing exactly?

-As a beginning here is a definition

“An emerging computer paradigm where data and services reside in massively scalable data centers in the cloud and can be accessed from any connected devices over the internet”

Like other definitions of topics like these, an understanding of the term cloud computing requires an understanding of various other terms which are closely related to this. While there is a lack of precise scientific definitions for many of these terms, general definitions can be given.

Cloud computing is an emerging paradigm in the computer industry where the computing is moved to a cloud of computers. It has become one of the buzz words of the industry. The core concept of cloud computing is, quite simply, that the vast computing resources that we need will reside somewhere out there in the cloud of computers and we’ll connect to them and use them as and when needed.

Computing can be described as any activity of using and/or developing computer hardware and software. It includes everything that sits in the bottom layer, i.e. everything from raw compute power to storage capabilities. Cloud computing ties together all these entities and delivers them as a single integrated entity under its own sophisticated management.

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices.

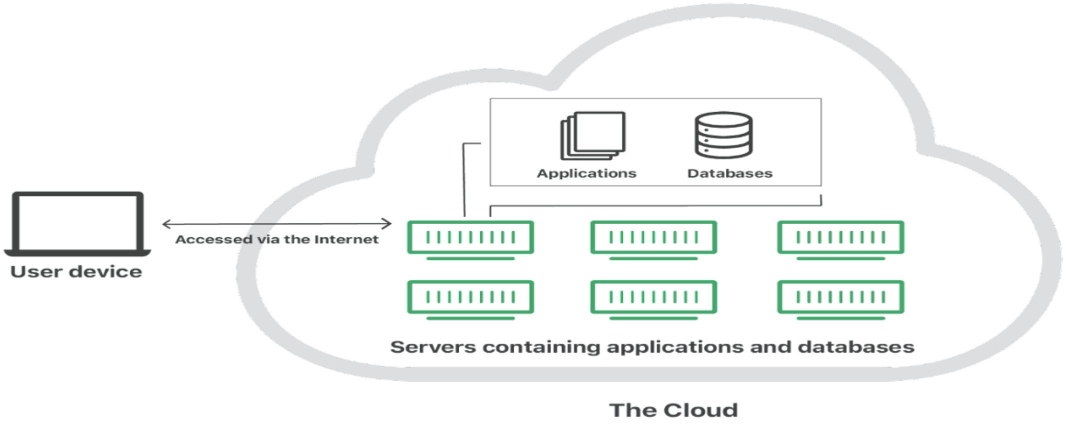
Computing started off with the mainframe era. There were big mainframes and everyone connected to them via “dumb” terminals. This old model of business computing was frustrating for the people sitting at the dumb terminals because they could do only what they were “authorized” to do. They were dependent on the computer administrators to give them permission or to fix their problems. They had no way of staying up to the latest innovations.

The personal computer was a rebellion against the tyranny of centralized computing operations. There was a kind of freedom in the use of personal computers. But this was later replaced by server architectures with enterprise servers and others showing up in the industry. This made sure that the computing was done and it did not eat up any of the resources that one had with him. All the computing was performed at servers. Internet grew in the lap of these servers. With cloud computing we have come a full circle. We come back to the centralized computing infrastructure. But this time it is something which can easily be accessed via the internet and something over which we have all the control.

1.1 What is Cloud?

"The cloud" refers to servers that are accessed over the Internet, and the software and databases that run on those servers. Cloud servers are located in data centers all over the world. By using cloud computing, users and companies do not have to manage physical servers themselves or run software applications on their own machines.

The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data center, instead of locally on the user device.


Applications
Databases
User device
Accessed via the Internet
Servers containing applications and databases
The Cloud

1.2 Cloud Computing

A definition for cloud computing can be given as an emerging computer paradigm where data and services reside in massively scalable data centers in the cloud and can be accessed from any connected devices over the internet.

Cloud computing is a way of providing various services on virtual machines allocated on top of a large physical machine pool which resides in the cloud. Cloud computing comes into focus only when we think about what IT has always wanted - a way to increase capacity or add different capabilities to the current setting on the fly without investing in new infrastructure, training new personnel or licensing new software. Here ‘on the fly’ and ‘without investing or training’ becomes the keywords in the current situation. But cloud computing offers a better solution.

We have lots of compute power and storage capabilities residing in the distributed environment of the cloud. What cloud computing does is to harness the capabilities of these resources and make available these resources as a single entity which can be changed to meet the current needs of the user. The basis of cloud computing is to create a set of virtual servers on the available vast resource pool and give it to the clients. Any web enabled device can be used to access the resources through the virtual servers. Based on the computing needs of the client, the infrastructure allotted to the client can be scaled up or down.

From a business point of view, cloud computing is a method to address the scalability and availability concerns for large scale applications which involves lesser overhead. Since the resource allocated to the client can be varied based on the needs of the client and can be done without any fuss, the overhead is very low.

One of the key concepts of cloud computing is that processing of 1000 times the data need not be 1000 times harder. As and when the amount of data increases, the cloud computing services can be used to manage the load effectively and make the processing tasks easier. In the era of enterprise servers and personal computers, hardware was the commodity as the main criteria for the processing capabilities depended on the hardware configuration of the server. But with the advent of cloud computing, the commodity has changed to cycles and bytes - i.e. in cloud computing services, the users are charged based on the number of cycles of execution performed or the number of bytes transferred. The hardware or the machines on which the applications run are hidden from the user. The amount of hardware needed for computing is taken care of by the management and the client is charged based on how the application uses these resources.

1.2.1 Characteristics of Cloud Computing

1. Self-Healing -

Any application or any service running in a cloud computing environment has the property of self-healing. In case of failure of the application, there is always a hot backup of the application ready to take over without disruption. There are multiple copies of the same application - each copy updating itself regularly so that at times of failure there is at least one copy of the application which can take over without even the slightest change in its running state.

2. Multi-tenancy -

With cloud computing, any application supports multi-tenancy - that is multiple tenants at the same instant of time. The system allows several customers to share the infrastructure allotted to them without any of them being aware of the sharing. This is done by virtualizing the servers on the available machine pool and then allotting the servers to multiple users. This is done in such a way that the privacy of the users or the security of their data is not compromised.

3. Linearly Scalable -

Cloud computing services are linearly scalable. The system is able to break down the workloads into pieces and service it across the infrastructure. An exact idea of linear scalability can be obtained from the fact that if one server is able to process say 1000 transactions per second, then two servers can process 2000 transactions per second.

4. Service-oriented –

Cloud computing systems are all service oriented - i.e. the systems are such that they are created out of other discrete services. Many such discrete services which are independent of each other are combined together to form this service. This allows re-use of the different services that are available and that are being created. Using the services that were just created, other such services can be created.

5. SLA Driven -

Usually, businesses have agreements on the number of services. Scalability and availability issues cause clients to break these agreements. But cloud computing services are SLA driven such that when the system experiences peaks of load, it will automatically adjust itself so as to comply with the service-level agreements. The services will create additional instances of the applications on more servers so that the load can be easily managed.

6. Virtualized -

The applications in cloud computing are fully decoupled from the underlying hardware. The cloud computing environment is a fully virtualized environment.

7. Flexible -

Another feature of the cloud computing services is that they are flexible. They can be used to serve a large variety of workload types - varying from small loads of a small consumer application to very heavy loads of a commercial application.

1.2.2 Advantages of Cloud Computing

1) Back-up and restore data

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

2) Improved collaboration

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

3) Excellent accessibility

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

4) Low maintenance cost

Cloud computing reduces both hardware and software maintenance costs for organizations.

5) Mobility

Cloud computing allows us to easily access all cloud data via mobile.

6) Services in the pay-per-use model

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

7) Unlimited storage capacity

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

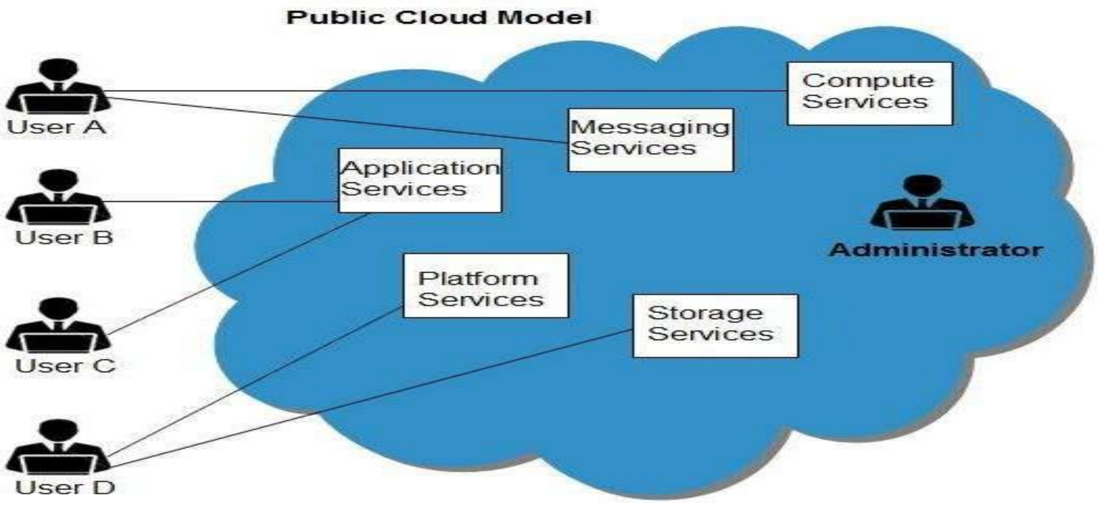
8) Data security

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

1.3 Types of Cloud

1. Public clouds :

Public clouds are cloud environments typically created from IT infrastructure not owned by the end user. Some of the largest public cloud providers include Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure.All clouds become public clouds when the environments are partitioned and redistributed to multiple tenants. Fee structures aren't necessary characteristics of public clouds anymore, since some cloud providers (like the Massachusetts Open Cloud) allow tenants to use their clouds for free. The bare-metal IT infrastructure used by public cloud providers can also b1e abstracted and sold as IaaS, or it can be developed into a cloud platform sold as PaaS.



2. Private clouds :

Private clouds are loosely defined as cloud environments solely dedicated to a single end user or group, where the environment usually runs behind that user or group's firewall. All clouds become private clouds when the underlying IT infrastructure is dedicated to a single customer with completely isolated access.

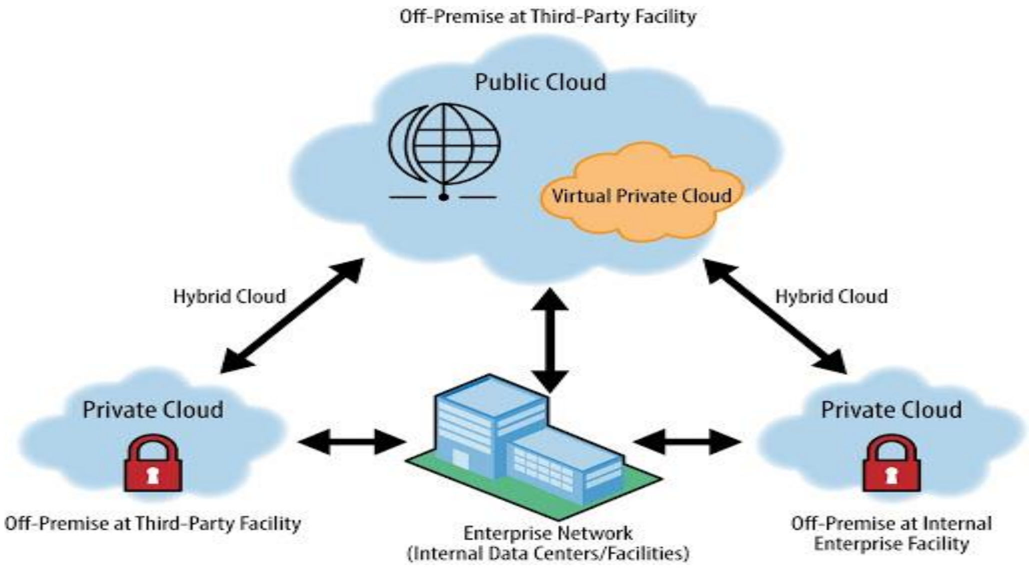
But private clouds no longer have to be sourced from on-premise IT infrastructure. Organizations are now building private clouds on rented, vendor-owned data centers located off-premises, which makes any location and ownership rules obsolete. This has also led to a number of private cloud subtypes, including:

Managed private clouds

Customers create and use a private cloud that's deployed, configured, and managed by a third-party vendor. Managed private clouds are a cloud delivery option that helps enterprises with understaffed or under skilled IT teams provide better private cloud services and infrastructure.

Dedicated clouds

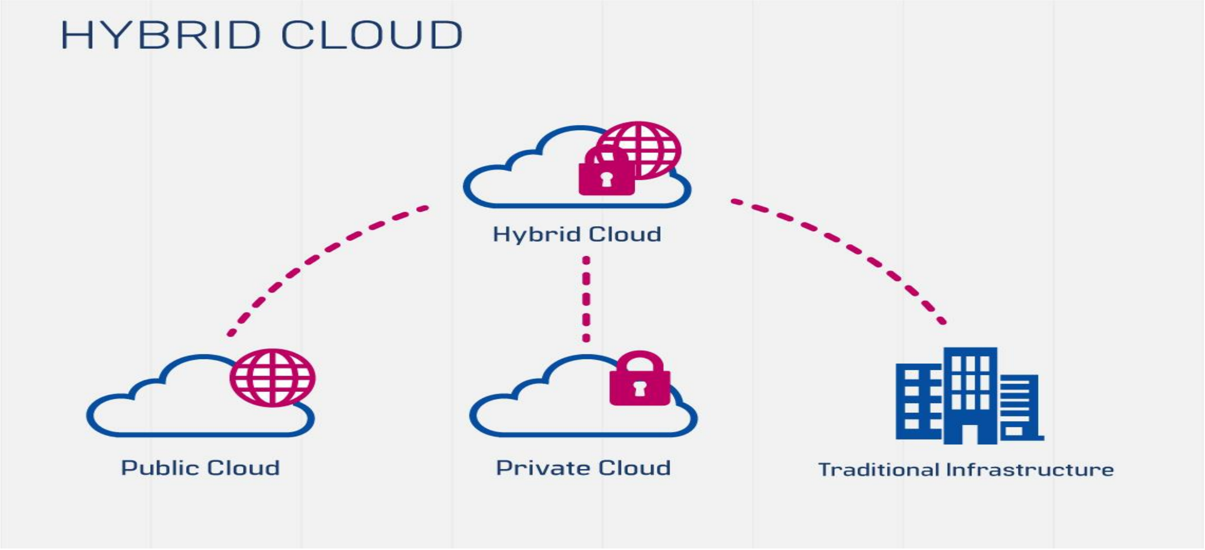
A cloud within another cloud. You can have a dedicated cloud on a public cloud (e.g. Red Hat OpenShift® Dedicated) or on a private cloud. For example, an accounting department could have its own dedicated cloud within the organization's private cloud.



3. **Hybrid Cloud**:

A hybrid cloud is a seemingly single IT environment created from multiple environments connected through local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), and/or APIs.
The characteristics of hybrid clouds are complex and the requirements can differ, depending on whom you ask. For example, a hybrid cloud may need to include:

- At least one private cloud and at least one public cloud
- Two or more private clouds
- Two or more public clouds
- A bare-metal or virtual environment connected to at least one public cloud or private cloud



4. **Multiclouds:**

Multiclouds are a cloud approach made up of more than 1 cloud service, from more than 1 cloud vendor—public or private. All hybrid clouds are multiclouds , but not all multiclouds are hybrid clouds. Multiclouds become hybrid clouds when multiple clouds are connected by some form of integration or orchestration.
A multicloud environment might exist on purpose (to better control sensitive data or as redundant storage space for improved disaster recovery) or by accident (usually the result of shadow IT). Either way, having multiple clouds is becoming more common across enterprises that seek to improve security and performance through an expanded portfolio of environments.

1.4 Delivery Models

1. Software-as-a-Service (SaaS):

Instead of users installing an application on their device, SaaS applications are hosted on cloud servers, and users access them over the Internet. SaaS is like renting a house: the landlord maintains the house, but the tenant mostly gets to use it as if they owned it. Examples of SaaS applications include Salesforce, MailChimp, and Slack.

2. Platform-as-a-Service (PaaS):

In this model, companies don't pay for hosted applications; instead they pay for the things they need to build their own applications. PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet. PaaS can be compared to renting all the tools and equipment necessary for building a house, instead of renting the house itself. PaaS examples include Heroku and Microsoft Azure.

3. Infrastructure-as-a-Service (IaaS):

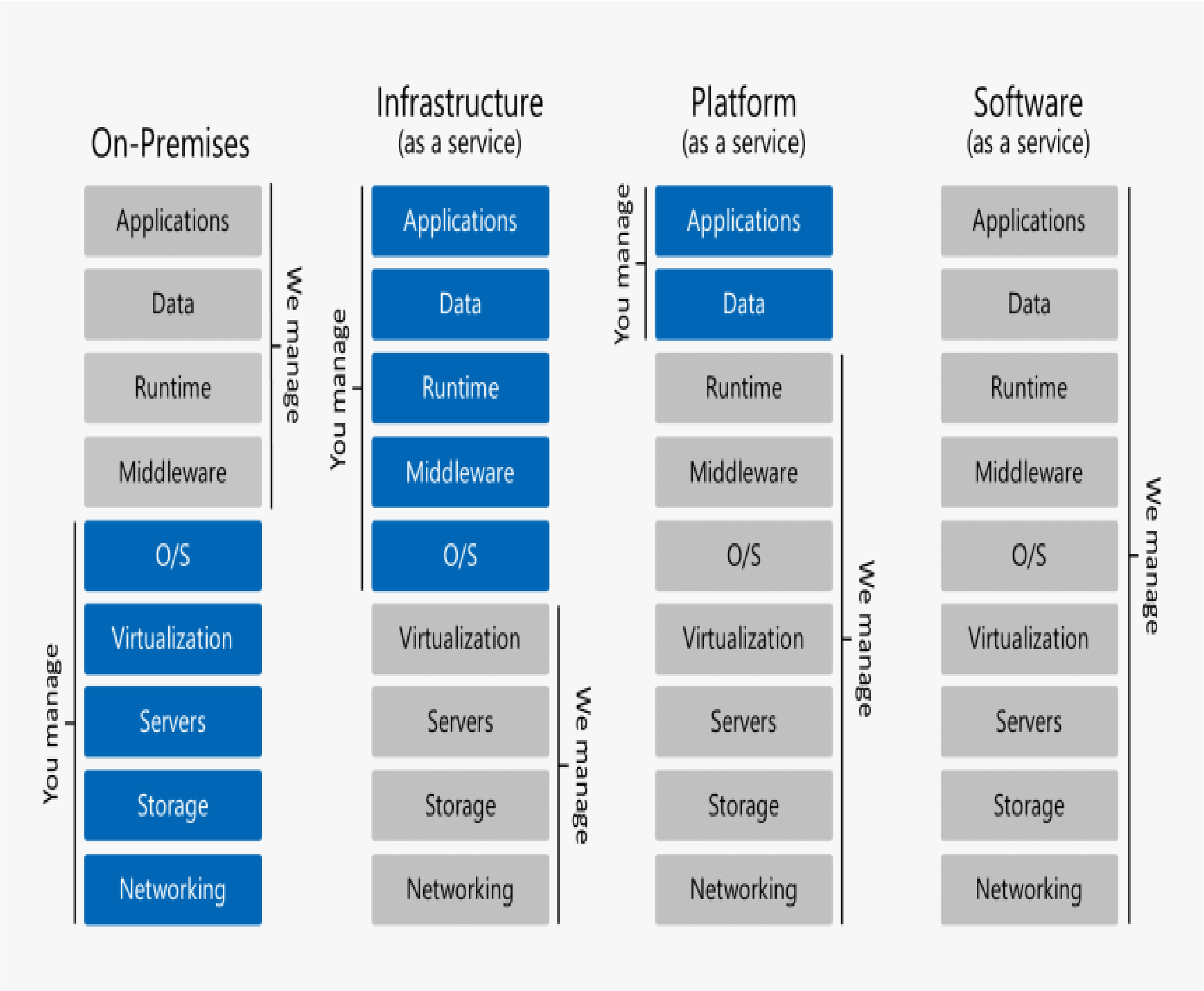
In this model, a company rents the servers and storage they need from a cloud provider. They then use that cloud infrastructure to build their applications. IaaS is like a company leasing a plot of land on which they can build whatever they want — but they need to provide their own building equipment and materials. IaaS providers include DigitalOcean, Google Compute Engine, and OpenStack.

Formerly, SaaS, PaaS, and IaaS were the three main models of cloud computing, and essentially all cloud services fit into one of these categories. However, in recent years a fourth model has emerged.

4. Function-as-a-Service (FaaS):

FaaS, also known as serverless computing, breaks cloud applications down into even smaller components that only run when they are needed. Imagine if it were possible to rent a house one little bit at a time: for instance, the tenant only pays for the dining room at dinner time, the bedroom while they are sleeping, the living room while they are watching TV, and when they are not using those rooms, they don't have to pay rent on them.

FaaS or serverless applications still run on servers, as do all these models of cloud computing. But they are called "serverless" because they do not run on dedicated machines, and because the companies building the applications do not have to manage any servers.



Chapter-2:
Backbone of Cloud - Virtualization

2.1 Introduction to Virtualization

“Virtualization is a technology that combines or divides computing resources to present one or many operating environments using methodologies like hardware and software partitioning or aggregation, partial or complete machine simulation, emulation, time-sharing, and many others”. In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded. Virtualization plays a major role in cloud computing. Virtualization allows single machine to run multiple platforms simultaneously. so, virtualization enables us to use same computer to work on various environment. In virtualization allvirtual environments is arranged to ensure its own security and integrity. Virtual Machine is the one which enables to run multiple platforms in the single machine concurrently. Virtual machine is created using both hardware and software engineering. Cloud computing system is bringing a tremendous fundamental change in Information Technology. Virtualization improves capacity and lowers the cost of IT infrastructure in cloud computing. Virtualization technology provides an abstract environment about the underlying resources and simplifies their use, supports replication and separates users from one another, which increases elasticity of the system. The cloud often includes virtualization software which manipulates the hardware as a part of their service package. With the help of virtualization multiple operating system and applications can run at a single time on the same machine and a same hardware, by this we can increase the flexibility of the hardware.

2.1.1 What is the concept behind Virtualization?

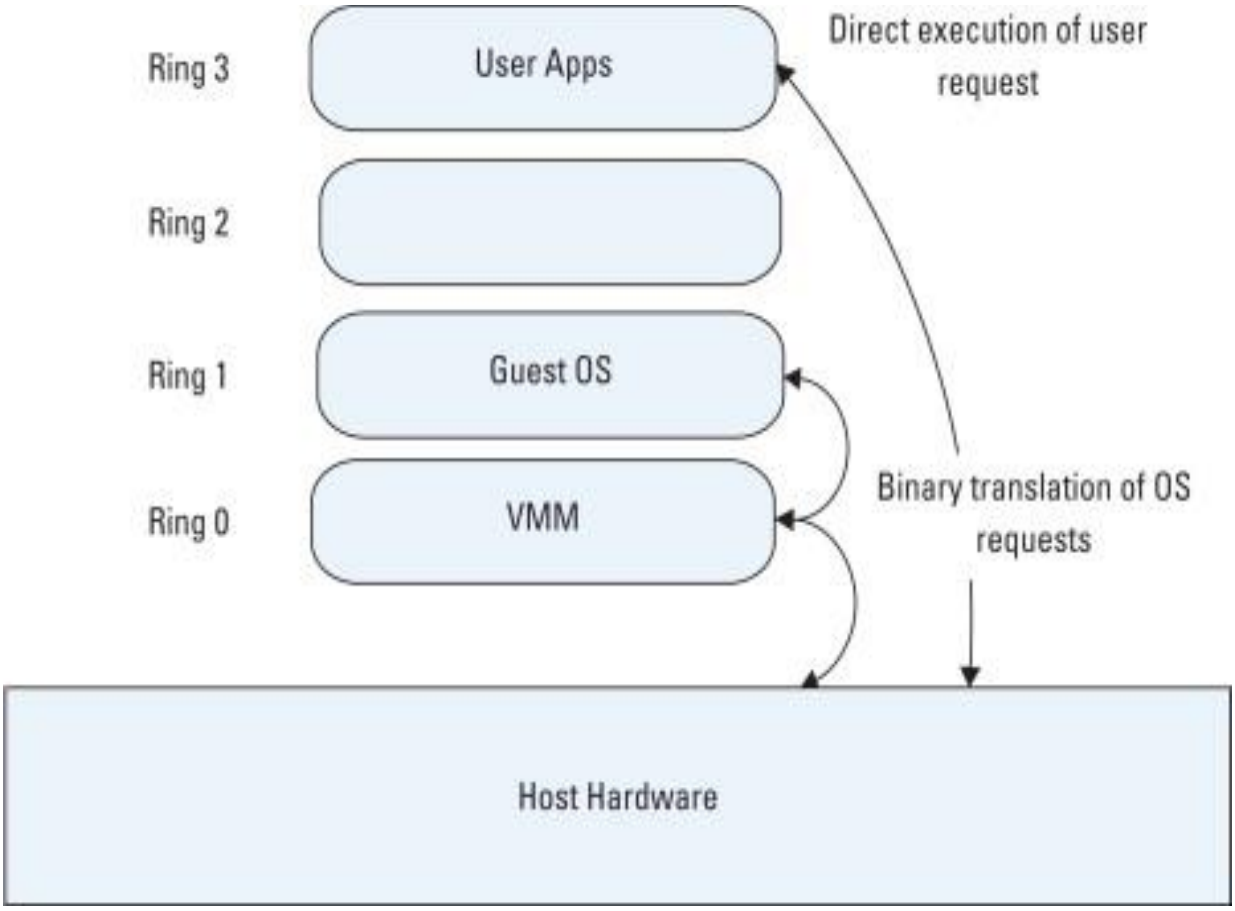
Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**

2.2 Full Virtualization

Full virtualization is a virtualization technique used to provide a VME that completely simulates the underlying hardware. In this type of environment, any software capable of execution on the physical hardware can be run in the VM, and any OS supported by the underlying hardware can be run in each individual VM. Users can run multiple different guest OSes simultaneously. In full virtualization, the VM simulates enough hardware to allow an unmodified guest OS to be run in isolation. This is particularly helpful in a number of situations. For example, in OS development, experimental new code can be run at the same time as older versions, each in a separate VM. The hypervisor provides each VM with all the services of the physical system, including a virtual BIOS, virtual devices, and virtualized memory management. The guest OS is fully disengaged from the underlying hardware by the virtualization layer.

Full virtualization is achieved by using a combination of binary translation and direct execution. With full virtualization hypervisors, the physical CPU executes nonsensitive instructions at native speed; OS instructions are translated on the fly and cached for future use, and user level instructions run unmodified at native speed. Full virtualization offers the best isolation and security for VMs and simplifies migration and portability as the same guest OS instance can run on virtualized or native hardware.


Ring 3
User Apps
Direct execution of user request
Ring 2
Ring 1
Guest OS
Ring 0
VMM
Binary translation of OS requests
Host Hardware

2.3 Para Virtualization

Paravirtualization is an enhancement of virtualization technology in which a guest OS is modified prior to installation inside a virtual machine (VM) in order to allow all guest OSes within the system to share resources and successfully collaborate, rather than attempt to emulate an entire hardware environment.

With paravirtualization, virtual machines can be accessed through interfaces that are similar to the underlying hardware. This capacity minimizes overhead and optimizes system performance by supporting the use of VMs that would otherwise be underutilized in conventional or full hardware virtualization.

The main limitation of paravirtualization is the fact that the guest OS must be tailored specifically to run on top of the virtual machine monitor (VMM), the host program that allows a single computer to support multiple, identical execution environments.

Paravirtualization eliminates the need for the virtual machine to trap privileged instructions. Trapping, a means of handling unexpected or unallowable conditions, can be time-consuming and can adversely impact performance in systems that employ full virtualization.

2.4 Hardware Assisted Virtualization

Also known as native virtualization, in this technique, **underlying hardware provides special CPU instructions to aid virtualization**. This technique is also highly portable as the hypervisor can run an unmodified guest OS. This technique makes hypervisor implementation less complex and more maintainable.

Intel’s Intel-VT and AMD’s AMD-V processors provide CPU virtualization instructions that software vendors use to implement hardware-assisted virtualization.

2.5 ISA x86 ring Architecture

The x86 architecture is an instruction set architecture (ISA) series for computer processors. This is developed by Intel Corporation. x86 is the single most used ISA by major players.

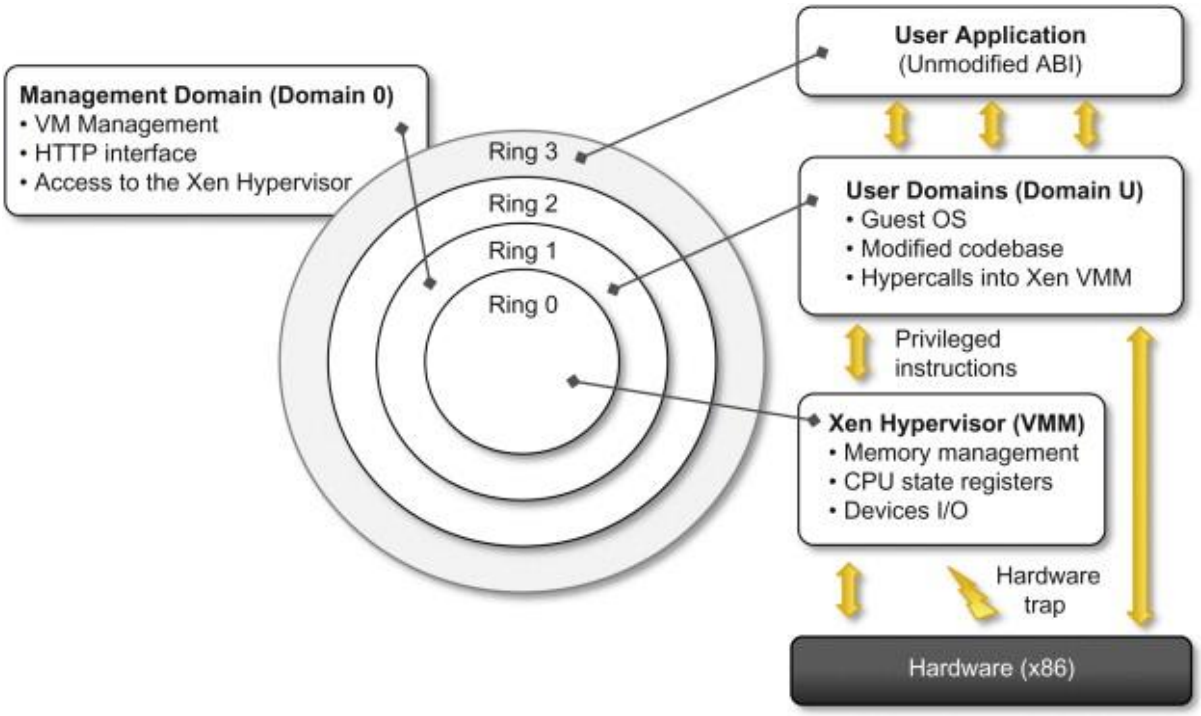
Ring 0: forms the core of the architecture and lies in the centre, comprising of operating system kernel.
Ring 1: Surrounds ring 0 and is generically not used.
Ring 2: Surrounds ring 1 and is generically not used.
Ring 3: Forms the outermost layer of the architecture and surrounds ring 2. User applications are run in this layer.

The intent by Intel in having rings 1 and 2 is for the OS to put device drivers at that level, so they are privileged, but somewhat separated from the rest of the kernel code. Rings 1 and 2 are in a way, "mostly" privileged.

BACKGROUND: THE X86 PRIVILEGE ARCHITECTURE

The Ring Privileges
Modern operating systems on the x86 architecture adapt the two privilege level model in which user programs run in Ring3 and kernel in Ring0. The x86 architecture, in fact, supports four privilege layers – Ring0 through Ring3 where Ring0 is the highest privilege on the system. The x86 architecture's definition of privilege is closely tied to a feature called segmentation. Segmentation divides virtual memory spaces into segments which are defined by a base address, a limit, and a Descriptor Privilege Level (DPL) that indicates the required privilege level for accessing the segment. A segment is defined by segment descriptor in either Global Descriptor Table (GDT) or Local Descriptor Table (LDT).
The privilege level (the Ring number) dictates an executing context's permission to perform sensitive system operations and memory access. Notably, the execution of privileged instructions is only allowed to contexts running with Ring0 privilege. Also, the x86 paging only permits Ring0-2 to access supervisor pages.

Memory Protection
Operating systems use paging to manage memory access control, and the segmented memory model has long been an obsolete memory management technique. However, the paging-based flat memory model, which has become the standard memory management scheme, uses the Ring privilege levels for page access control. The x86 paging defines two-page access privilege: User and Supervisor. The Ring 3 can only access User pages while Ring 0-2 are allowed to access Supervisor pages1 . In general, the pages in the kernel memory space are mapped as Superuser such that they are protected from user applications. Table 1 outlines the privileges of each Ring level.



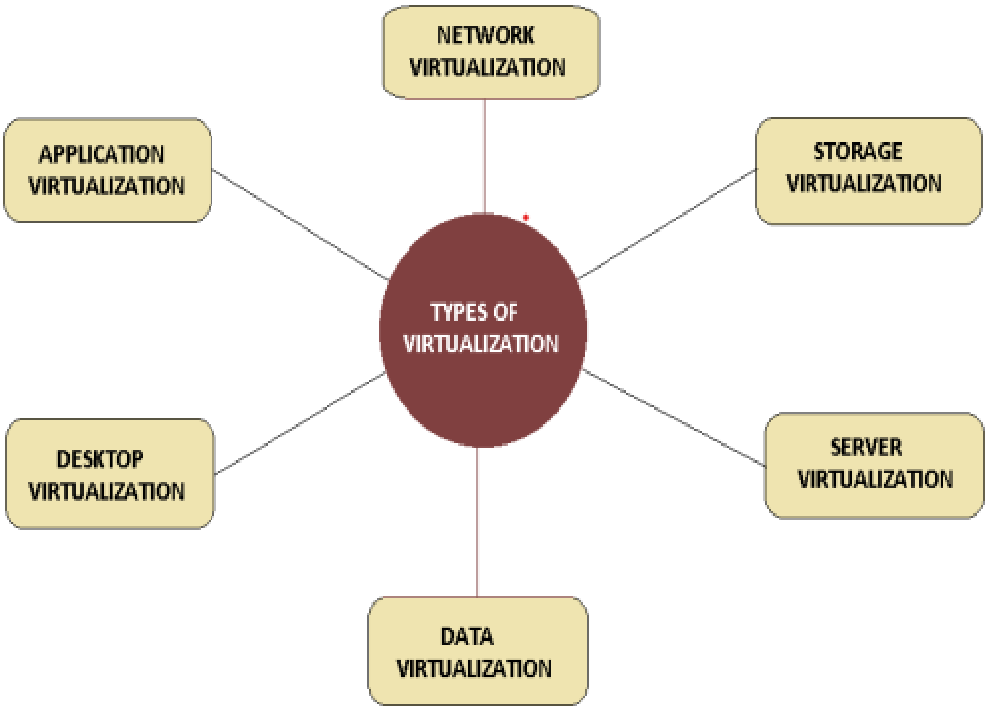
2.6 Role of Virtualization in Cloud Computing

Virtualization plays significant role in cloud computing, which helps to use one system separately by multiple users. This technique is done by giving a logical name to all the physical resources and based on demand it provides a pointer to those physical resources. To share data and information virtualization technique is very important in cloud. From underlying hardware virtual machine is logically separated. A machine called host by which the virtual machine is created and this virtual machine is known as guest machine. The hypervisor is a firmware which user a combination of different types hardware virtualization. The main objective of virtualization is improvement in security, energy saving, flexibility and reduction in cost.

2.6.1 History of Virtualization

Concept of virtualization was first introduced in late 1950s. Since there were no personal computers at that time virtualization did not become successful until 1990s. IT companies realized that they could save money and time by moving from physical to virtual environment. In 1964 IBM began to explore virtualization on mainframes, it released an operating system called VM running on mainframes 1972. In the development of robust time-sharing solution system IBM had invested a lot of effort and in 1999 VMware is launched. In 2004 Intel engineers began adding hardware virtualization support to Xen to prepare the necessary software for the upcoming new processor. Under their efforts Xen 3.0 was released in 2005, which began to officially support Intel's VT technology. Between 2006 and 2010 major traditional IT vendors introduced their own products in terms of virtualization. In 2007 HP introduced HP-UX Integrity virtual machines and Microsoft joined Hyper-V in Windows Server in2008. Since then, virtualization has become very successful in today's IT world.

2.7 Types of Virtualization in Cloud Computing



1. **Network Virtualization:**

   Network virtualization helps user to create multiple individual networks from one physical area network (LAN). In this type of virtualization, all physical networking tools and other resources are combined into a single software-based resource. Network virtualization improves overall network's productivity and efficiency, flexibility, reliability, security and scalability. Few examples of network virtualization are JunosV App Engine, Cisco Nexus and 6WIND Virtual Accelerator.

2. **Storage Virtualization:**

   A virtual storage system manages multiple physical storage arrays which appears to be a single storage device. The resources needed can be increased by the centralized virtual storage system by increasing availability and flexibility. This virtualization software provides various advantages such as maintaining smooth operation, better work flow is created, downtime is reduced, load balancing, cheaper storage and the performance and speed are better optimized. Few examples for storage virtualization are the transitional of physical disk address: CHS—Cylinders, Heads and sectors—

addresses and Logical Block Addresses (LBAs), logical unit number and RAID groups.

3. **Server Virtualization:**

   In Server virtualization' masking of server resources takesplace. Instead of assigning one task to one server, in server virtualization multiple tasks run from one server. This causes an increase in performance and the operating cost is reduced. Few examples of server virtualization are Free VPS, LinuxVserver and OpenVZ.

4. **Data Virtualization:**

   In Data virtualization, data is collected from various sources and it manipulates, segregates, delivers and retrieves data without any data specification. The on-demand integration is delivered to the users by using data virtualization, which also removes latency. The technical details of the data are arranged logically so that its virtual view can be accessed by its interested people and users through various cloud services remotely. Few examples of data virtualization are JBoss, TIBCO Data Virtualization and Denodo.

5. **Desktop Virtualization:**

   The other name for this type of virtualization is client-server computing model. Desktop virtualization enables to store the users' operating system on a server in a data center (this basically gives someone an entire computing platform without the hardware). Through this type of virtualization, employees can work conveniently from their homes. The data transfer is secured, and any risk of data theft is minimized. Few examples of desktop virtualization are VMware ThinApps Citrix XenApps, VMware View and Microsoft Remote Desktop Services.

6. **Application Virtualization:**

   Application virtualization helps a user to run an application ona computer, without relying on the computer hardware or software. Updating, maintaining and fixing the applications will be easier for an organization by using application virtualization. Admin without entering in to the user's desktop, they can modify and control access permissions to the application. Another benefit of this type of virtualization is portability. Few examples of application virtualization are XenApp, VM Thinapp, Zenworks and Microsoft App-V.

2.8 Benefits of Virtualization

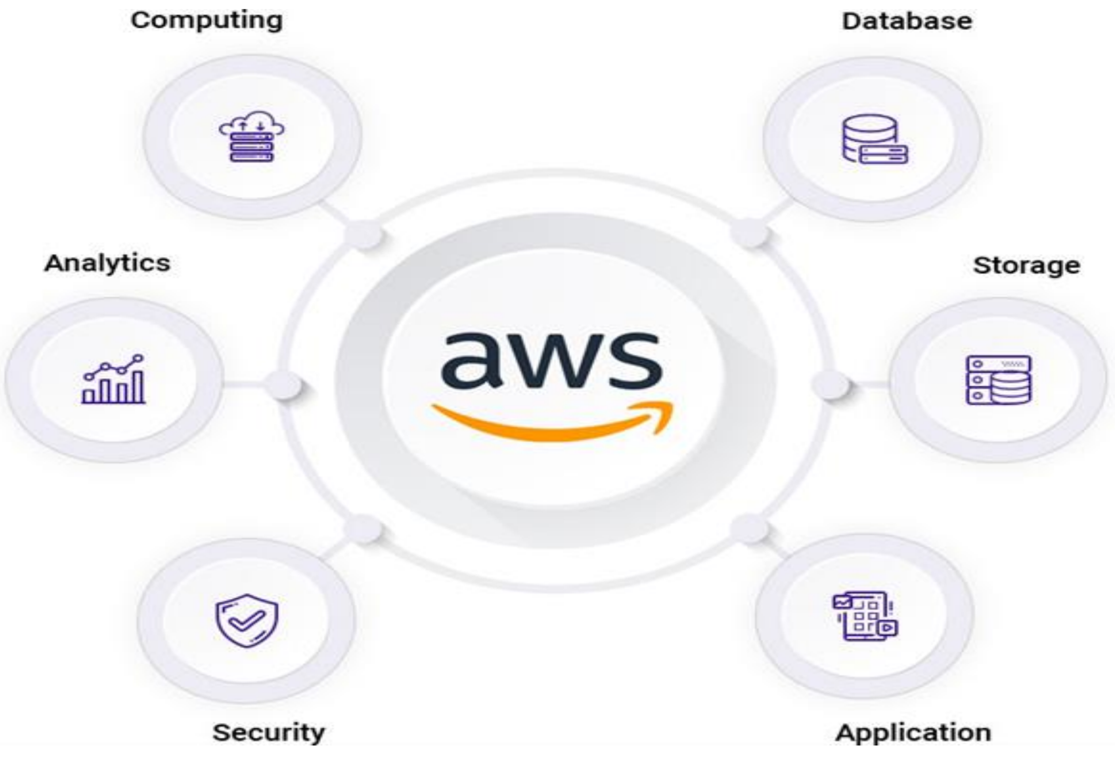
- Virtualization reduces work load.
- Virtualization is cost predictable and it is cheaper.
- Whenever there is a need for more resources, it can be obtained from available pool of resources and this is known as scalability.
- It promotes digital entrepreneurship and offers a better uptime.
- Through virtualization the managing of resources is much easier.
- Virtualized infrastructure can prevent entire system from failure.
- Virtualization allows automatic update to both hardwares and softwares by installing on their third-party provider.
- It improves the efficiency of the resources in the virtual environment.
- The energy can be used efficiently through virtualization.
- The IT operations can be done more smoothly.
- There is an easy transfer of machine or data.
- Faster deployment of resources can be done when virtualization is being used

Chapter-3: Study of Public Cloud (AWS)

3.1 What is AWS?

Amazon Web Services, Inc. (**AWS**) is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. These cloud computing web services provide distributed computing processing capacity and software tools via AWS server farms. One of these services is Amazon Elastic Compute Cloud (EC2), which allows users to have at their disposal a virtual cluster of computers, available all the time, through the Internet. AWS's virtual computers emulate most of the attributes of a real computer, including hardware central processing units (CPUs) and graphics processing units (GPUs) for processing; local/RAM memory; hard-disk/SSD storage; a choice of operating systems; networking; and pre-loaded application software such as web servers, databases, and customer relationship management (CRM).

AWS services are delivered to customers via a network of AWS server farms located throughout the world. Fees are based on a combination of usage (known as a "Pay-as-you-go" model), hardware, operating system, software, or networking features chosen by the subscriber required availability, redundancy, security, and service options. Subscribers can pay for a single virtual AWS computer, a dedicated physical computer, or clusters of either.[8] Amazon provides select portions of security for subscribers (e.g. physical security of the data centers) while other aspects of security are the responsibility of the subscriber (e.g. account management, vulnerability scanning, patching). AWS operates from many global geographical regions



With over 32 percent of the entire world’s public cloud share, it’s no surprise that AWS serves more than 190 countries with scalable, reliable, and low-cost infrastructure. One of its most powerful and commonly used services are Amazon EC2 (Elastic Cloud Compute). Amazon EC2 provides scalable computing capacity in the AWS cloud. Leveraging it enables organizations to develop and deploy applications faster, without needing to invest in hardware upfront. Users can launch virtual servers, configure security and networking, and manage cookies from an intuitive dashboard.

3.2 What is AWS EC2 ?

An **EC2 instance** is nothing but a virtual server in Amazon Web services terminology. It stands for **Elastic Compute Cloud.** It is a web service where an AWS subscriber can request and provision a compute server in AWS cloud.

An **on-demand** EC2 instance is an offering from AWS where the subscriber/user can rent the virtual server per hour and use it to deploy his/her own applications.

The instance will be charged per hour with different rates based on the type of the instance chosen. AWS provides multiple instance types for the respective business needs of the user.Thus, you can rent an instance based on your own CPU and memory requirements and use it as long as you want. You can terminate the instance when it’s no more used and save on costs. This is the most striking advantage of an on-demand instance- you can drastically save on your CAPEX.

3.2.1 Why is AWS EC2 important ?

1. You don’t require any hardware units
2. Easily scalable (up or down)
3. You only pay for what you use
4. You have complete control
5. Highly secure
6. You can access your assets from anywhere in the world

3.2.2 Amazon EC2 and its Advantages

It offers Reliability

Amazon EC2 provides Reliability as it offers 99.9% availability for each Amazon EC2 region. Also, the services are highly reliable where replacement of instances can be done easily and rapidly.

It offers Security

Amazon EC2 offers Security to its users. Amazon works with the Amazon VPC to provide robust networking and security for the compute resources. The compute instances are located in the VPC (Virtual Private Cloud) in the specific IP range. Further, this specific function helps the user in deciding which instances are exposed to the internet and which remains private.

It offers Flexibility

Amazon EC2 provides users with choices of multiple instance types, software packages, instance storage, and operating systems and thus Amazon EC2 offers flexibility. Amazon EC2 lets users configure memory, CPU and boot partition size which is further optimized for the operating system and application.

It offers Cost Savings

Amazon EC2 is inexpensive as it allows the user to select the plans as per the requirement and thus offers Cost-saving pricing. This helps the user to save costs and utilize the resources fully. Amazon EC2 passes the benefits of Amazon’s scale as the user has to pay a very low amount compared to the services they provide.

It offers Complete Computing Solution

The Amazon EC2 works fine with the Amazon RDS, S3, Dynamo DB and Amazon SQS and thus offers the complete computing solution. So, this provides the complete computing, processing and storage solution.

It offers Elastic Web Computing

Amazon EC2 offers Eleatic Web Computing. So, Enterprises can easily increase or decrease capacity within minutes and can commission thousands of server instances simultaneously. Additionally, all the server instances are handled by the web service APIs which can scale the servers up and down depending on requirements.

It offers a Complete Controlled setup

The Amazon EC2 offers complete control over the instances. Also, users can have root access to each instance and enable users to interact with them as with any other machine. The user can stop the instance while retaining the data on the boot partition and restart the same using web service APIs.

Let’s look at EC2(Elastic Cloud Compute) in action-

3.2.3 Use Case: Notifying Users about a Newsletter

Imagine if your user base is enjoying your product. How would you let them know about the other services you offer?

That’s where AWS comes in. With Amazon Simple Notification Service (SNS), EC2, and Simple Storage Service (S3), you should be able to do everything you want with ease. You’ll be able to notify users every time the company creates a newsletter, for example.

Here’s how:

1. Create an AWS account

2. Set up an EC2 instance

If at some point in the future, you wanted to create an application using the resources you’ve stored on S3, you’ll need to create an instance EC2.

2a) Choosing an AMI (Amazon Machine Image):

An AMI is a template that is used to create a new instance—or virtual machine—based on user requirements. The AMI will contain information about the software, operating system, volume, and access permissions. There are two types of AMIs:

i) Predefined AMIs: Amazon creates these, and the user can modify them.

ii) Custom AMIs: The user also creates these, and they can be reused. These AMIs are also available in the AMI Marketplace

2b) Choosing an instance type:

An instance type specifies the hardware specifications that are required in the machine from the previous step. Instance types belong to five main families:

i) Compute-optimized: For situations that require a lot of processing power

ii) Memory-optimized: For setting up something to do with your in-memory cache

iii) GPU optimized: For setting up a gaming system, or something with the requirement of a large graphic

iv) Storage optimized: When you need to set up a storage server

v) General-purpose: When everything is equally balanced

Instance types are fixed, and their configurations cannot be altered.

2c) Configure Instance:

You have to specify the number of instances, purchasing options, the kind of network, the subnet, assign a public IP, set the IAM role, the shutdown behavior, etc. On that note, stopping the system and terminating the system under 'Shutdown behavior' are completely different things.

Stopping = Temporarily shutting down the system

Terminating = Returning control to Amazon

Under the advanced details, users can also add bootstrap scripts that are executed when the virtual machine starts up. It also offers multiple payment options, such as:

i) On-demand instances: Can be launched whenever the user requires normal rates

ii) Reserved instances: These instances are reserved for one year or three years. The entire amount has to be paid upfront or over a span of a few months.

iii) Spot instances: Bidding goes to the bidder with the highest bid. These instances are available at a lesser cost than on-demand instances.

2d) Adding Storage:

You’re tasked with deciding the type of storage, which could be:

i) Ephemeral Storage (temporary and free)

ii) Amazon Elastic Block Store (permanent and paid)

iii) Amazon S3

The size (in GBs), volume type, where the disk is mounted, and whether the volume needs to be encrypted needs to be specified. Free users get to access up to 30 GBs of SSD or magnetic storage (which can be found under ‘Volume Type’).

2e) Adding tags:

This helps to identify instances more quickly.

2f) Configuring security groups:

These are used to specify rules based on which users are given access to the EC2 instance. You set up the type of security, protocol, the port range, and source (from where the incoming traffic is coming from). Incoming traffic has to be explicitly specified, and outgoing traffic is open.

2g) Review

Click on ‘Launch’ and the instance is created. However, there’s a little more work to be done.

Private key: The user downloads the private key

Public key: AWS uses the public key to confirm the identity of the user.

After choosing to create a new pair, a new private key is downloaded as a .pem file.

For the next step, we need to use the following tools: PuTTY and PuTTYgen. PuTTY is generally used when you need to connect a Windows system with a Linux system, which is what we're doing now. PuTTY doesn't accept .pem files.

So, using the PuTTY Key Generator, you create a new .ppk file.

Conversion> Insert Key

And load the .pem file.

Select "Save Private Key" and find a location to save the key.

In the PuTTY configuration tool, provide your IP address and click on "Auth."

Now click on browse and find the corresponding .ppk file

Once that's done, a terminal will open up where you can log in as ec2-user

3. Create an SNS and a topic

4. Make sure the topic is set to "public."

5. Add subscribers:

These are the individuals who have opted-in to be notified about your newsletter

6. Create an S3 bucket

7. Set up an event relating it with SNS:

A notification is sent to the company's subscribers every time something is added to the bucket

8 . Sync the S3 bucket and AWS instance and that's it your users will be notified.

3.3 What is Amazon S3?

Amazon S3 is a program that’s built to store, protect, and retrieve data from “buckets” at any time from anywhere on any device.

Organizations of any size in any industry can use this service. Use cases include websites, mobile apps, archiving, data backups and restorations, IoT devices, enterprise application storage, and providing the underlying storage layer for your data lake.

3.3.1 How Does Amazon S3 Work?

Organizing, storing and retrieving data in Amazon S3 focuses on two key components: buckets and objects that work together to create the storage system.

As AWS describes it, an S3 environment is a flat structure — a user creates a bucket; the bucket stores objects in the cloud.

3.3.2 Amazon S3 Objects

As mentioned above, in Amazon S3 terms, objects are data files, including documents, photos, and videos.

Each object is identified by a unique key within the S3 environment that differentiates it from other stored objects.

The maximum object file size is 160 GB for uploading, however there are various AWS tools to help you add files larger than this.

3.3.3 Amazon S3 Buckets

In an S3 environment, objects need somewhere to go, which is why buckets exist, serving as fundamental storage containers for objects.

You can create up to 100 buckets in each of your AWS cloud accounts, with no limit on the number of objects you can store in a bucket. If needed, you can request up to 1,000 more buckets by submitting a service limit increase.

When you create a bucket, you have the ability to choose the AWS region to store it in. To minimize costs and address latency concerns, it’s best practice to select a region that’s geographically closest to you. Objects that reside in a bucket within a specific region remain in that region unless you transfer the files elsewhere.

It’s also important to know that Amazon S3 buckets are globally unique. No other AWS account in the same region can have the same bucket names as yours unless you first delete your own buckets.

3.3.4 Amazon S3 Console

In the Amazon S3 Console inside AWS Management, you can easily manage objects and buckets. The console provides an intuitive, browser-based user interface for interacting with AWS services.

This is where you can create, configure, and manage buckets, as well as upload, download, and manage objects. The console allows you to organize storage using a logical hierarchy driven by keyword prefixes and delimiters.

Objects and buckets form a folder structure within the console, making it easy to locate files since every Amazon S3 object can be uniquely addressed through the combination of the web service endpoint, bucket name, key — and optionally, version. You can set access permissions for all buckets and objects within the management console.

3.3.5 What are the Advantages of Amazon S3?

If you're looking for secure storage that's simple and robust, Amazon S3 is a great choice. AWS built this tool with a minimal feature set that delivers big advantages. Let's take a look at a few:

1. Scalability

Storage providers often offer predetermined amounts of storage and network transfer capacity, similar to how some cell phone or cable providers bundle data and bandwidth usage. If you stay within your limits, you'll pay a flat rate even if you don't use all of your capacity. But if you exceed your limit, the provider will charge pricey overage fees or perhaps suspend your service until the beginning of the next billing cycle.

Amazon S3 charges only for what you actually use. With no hidden fees or overage charges, this service allows you to scale your storage resources up and down so you can meet your organization's ever-fluctuating demands with ease.

2. Durability and Accessibility

According to AWS, Amazon S3 is "...designed for 99.999999999% (11 9s) of durability, storing data for millions of applications for companies all around the world." The service automatically creates and stores your S3 objects across multiple systems, meaning your data is protected and you can access it quickly whenever you need it.

As AWS notes, "If you store 10,000,000 objects with Amazon S3, you can on average expect to incur a loss of a single object once every 10,000 years."

3.Cost-Effective Storage

When you use Amazon S3, you can store your data in a range of "storage classes" based on the frequency and immediacy you need to access your files.

Storage classes range from the most expensive cost level for immediate access to your mission-critical files to the lowest level for files you rarely touch, but need to have available for regulatory or other long-term needs.

AWS provides tools that allow you to monitor your objects and determine if they should be moved to a less expensive storage class. For example, S3 Intelligent Tiering is a program that's set to automatically move your data from higher-priced storage classes to lower ones based upon your ongoing access patterns.

4.Versioning

While not enabled by default, versioning is a setting that allows for multiple variants of a file or object to exist in the same bucket. This provides an opportunity to roll back or recover a deleted object.

5. Powerful Security

Thanks to encryption features and access management tools, data stored in your AWS S3 environment is protected from unauthorized access. This includes blocking all public access from all of your objects — at both the bucket and account levels.

By default, the users within your organization only have access to the S3 buckets and objects they create. You can use a variety of AWS security management features to change and customize access permissions. Multi-factor authentication (MFA) can also be utilized to allow users to permanently delete an object version — or to modify the versioning state of a bucket.

AWS also offers tools so you can analyze your bucket access policies to quickly find and fix any discrepancies that might allow unauthorized use and/or unintended access.

Chapter-4:
Study of Private Cloud

4.1 What is Private Cloud?

The private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Also called an internal or corporate cloud, private cloud computing gives businesses many of the benefits of a public cloud - including self-service, scalability, and elasticity - with the additional control and customization available from dedicated resources over a computing infrastructure hosted on-premises. In addition, private clouds deliver a higher level of security and privacy through both company firewalls and internal hosting to ensure operations and sensitive data are not accessible to third-party providers. One drawback is that the company's IT department is held responsible for the cost and accountability of managing the private cloud. So private clouds require the same staffing, management, and maintenance expenses as traditional data center ownership.

Two models for cloud services can be delivered in a private cloud. The first is infrastructure as a service (IaaS) that allows a company to use infrastructure resources such as compute, network, and storage as a service. The second is platform as a service (PaaS) that lets a company deliver everything from simple cloud-based applications to sophisticated-enabled enterprise applications. Private clouds can also be combined with public clouds to create a hybrid cloud, allowing the business to take advantage of cloud bursting to free up more space and scale computing services to the public cloud when computing demand increases.

4.1.1 The advantages of using a private cloud

1. **Costs**

The single most important aspect for any company is the **TCO** (total cost of ownership) associated with the IT infrastructure. This is the most important point where public cloud offerings cannot deliver for SMBs.

A Syneto hyper-converged infrastructure deployed as a Private Cloud solution is **10x less expensive** compared to Amazon Web services, over 3 years and for the same workload.

2. **Efficiency & control**

Private clouds are hosted either on-site or on in a third-party datacenter, that is also a privately hosted environment. This gives you more control over your data and infrastructure, allowing you to intervene promptly should changes be needed. Your IT department can monitor application deployment and use advanced analytics to predict and prevent bottlenecks and downtime.

3. Customization

There is no one-size-fits all solution. An important feature of private clouds is the level of customization they offer. Each organization has a set of technical and business requirements that usually vary according to company size, industry, business objectives etc.

With a private cloud, you can choose an infrastructure with specific storage and networking characteristics, so that the system meets your individual needs perfectly.

4. Security & privacy

Another great benefit of private clouds is the improved level of security compared to the public cloud. All data is saved and managed on servers to which no other company has access. This greatly improves data privacy. If the servers are on-site, they are managed by an internal IT team. Therefore, the organization does not need to worry about the physical security of the infrastructure.

If servers are located in a datacenter, the same internal IT team will access the data through highly secure networks instead of using your every-day, unsecured internet connection.

5. Compliance

As previously mentioned, businesses of all shapes and sizes need to comply with national/ internal laws and policies. The private cloud is an ideal option in this case, as it can be deployed in accordance with any retention and access-control policies.

For any company, customer information is considered (by law and common-sense) to be highly sensitive user data. Businesses need to have a great control over their data, in addition to ensuring data privacy. For example, in the case of a data breach, it may be rather difficult to access security logs from a public cloud. Not a problem if you own your private cloud.

6. Ensuring business continuity

Ensuring business continuity is more difficult to achieve if you don’t own your infrastructure. You’re planning to stay in business for a long time and so is your public cloud service provider. But what if it doesn’t?! In this agile, constantly changing business world, there is no guarantee that your provider will stay in business longer than you will. And technology is evolving at a fast pace, we all know that.

Should your provider suddenly go out of business, it will be a long and very difficult process to migrate all of your applications and data to a new cloud. So why take any chances? On a private cloud you have privacy, control and you can ensure the continuity of your business.

The public cloud has had few failures in recent years, but the downtime caused has always created strong panic and frustration, “freezing” websites, applications, gadgets and entire businesses. For example, the recent outage suffered by Amazon Web Services has caused problems for many businesses, big and small for a period of 5 hours or more.

7. Geographic availability

Last but not least, the public cloud is not available everywhere. There are still places in the world where the public cloud is not accessible. Moreover, if your business has several hubs across the world, the compliance requirements may vary greatly according to the location.

In these cases, the private cloud sounds like a good option, doesn’t it?!

4.1.2 Private Cloud Deployment Models

The private cloud deployment model is the exact opposite of the public cloud deployment model. It’s a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else. The distinction between private and public cloud is in how you handle all of the hardware. It is also called the “internal cloud” & it refers to the ability to access systems and services within a given border or organization. The cloud platform is implemented in a cloud-based secure environment that is protected by powerful firewalls and under the supervision of an organization’s IT department.

4.1.3 Advantages of the private cloud model:

- **Better Control:**
  You are the sole owner of the property. You gain complete command over service integration, IT operations, policies, and user behaviour.

- **Data Security and Privacy:**
  It’s suitable for storing corporate information to which only authorized staff have access. By segmenting resources within the same infrastructure, improved access and security can be achieved.

- **Supports Legacy Systems:**
  This approach is designed to work with legacy systems that are unable to access the public cloud.

- **Customization:** Unlike a public cloud deployment, a private cloud allows a company to tailor its solution to meet its specific needs.

4.2 The Three Deployment Strategies for Modern Private Cloud

When private clouds first emerged more than a decade ago, there was essentially just one deployment model: a DIY deployment approach where companies set up private cloud services themselves on their own infrastructure.

Today, the evolution of the private cloud ecosystem offers a much richer set of deployment options. They range from the DIY approach to a fully-managed, turnkey deployment strategy, with some other deployment strategies falling in between those two options.

1) Self-Service Private Cloud Deployment (i.e., the DIY approach)

It's still certainly possible to use a DIY private cloud deployment strategy. (The more formal term for this approach would be to call it a self-service option.) Under this approach, you take private cloud software and deploy and manage it on your own infrastructure.

This deployment strategy gives users the highest degree of control, and it could potentially save money – if (and this is a big 'if') a team truly has the in-house expertise it needs to deploy and manage a private cloud on its own.

Generally speaking, however, a self-service deployment model comes with several drawbacks:

- Because the private cloud ecosystem now relies heavily on open source platforms like OpenStack (which is different from a decade ago, when proprietary private cloud frameworks were more common), there is no official support channel that self-service deployment teams can turn to when they run into issues.
- The scale of today's clouds is larger than ever, making a DIY deployment harder to manage at the scale that companies typically need.
- In almost all cases, self-service deployments take a long time to complete: At least six months, as a rule of thumb. That delay comes with a considerable productivity loss, which may not be enough to offset the cost savings of a self-service deployment model.
- Even if a team has the expertise required to deploy a private cloud on its own today, the ever-changing nature of the cloud ecosystem means that it may not have the skills it needs to integrate whichever platforms or tools appear tomorrow.

Overall, these drawbacks make self-service deployment a poor approach for most private clouds today.

2) Hybrid Self-Service Deployment Using Public Cloud Services

The appearance of new hybrid and multi-cloud frameworks – like Azure Stack, Azure Arc and Google Anthos – has enabled a new take on the self-service private cloud deployment model. Today, you could take one of these frameworks and use it to extend the control plane of a public cloud into your own data center in order to build your private cloud.

This is very different from deploying an open source platform like OpenStack to build a private cloud; because in this approach, you depend centrally on a public cloud to make your private cloud tick. There is thus a degree of lock-in at play (which may be lesser or greater, depending on which specific framework you use: Azure Stack will lock you in more than Anthos, for example, because Azure Stack works only with Azure, whereas Anthos works with any public cloud provider).

The upside of this approach, however, is that it requires somewhat less effort and expertise than a traditional DIY deployment. The vendors behind modern hybrid and multi-cloud cloud frameworks provide support services. They don't offer fully-managed clouds – that is a different deployment model, as we'll discuss below – but they don't leave you on your own as much as you would be if you deployed a platform like OpenStack, without any outside assistance.

3) Fully-Managed Private Cloud Deployments

A third deployment option is to take advantage of fully-managed services to deploy private clouds.

There are actually different subcategories within this overarching approach to deployment.

Fully-managed hybrid cloud

One subcategory involves using a fully-managed hybrid cloud service, like AWS Outposts. This is similar to the hybrid self-service deployment model described above, with the exception that Outposts provides a turnkey solution for deploying a private cloud using AWS services.

Managed Kubernetes services in public clouds

Another subcategory is to deploy a private cloud using a managed public cloud service like Amazon EKS or Azure Kubernetes Service. With this approach, you can build a private cloud using a relatively painless and almost turnkey deployment process. In most cases, you'll be limited to hosting your private cloud on public cloud infrastructure, although in some cases you can use on-premises infrastructure as well.

The major drawback in all cases, however, is that currently, the managed services that offer this type of deployment option are based on Kubernetes. That means they're useful only if you are able to deploy your applications using containers and work within the Kubernetes ecosystem. The big-name public cloud providers don't offer managed services for deploying a private cloud framework like OpenStack.

Third-party management services

The third subcategory of fully-managed private cloud deployment options is to adopt a service like Platform9's, which lets you deploy and manage Kubernetes or OpenStack on virtually any private infrastructure – your own data center, a public cloud or both at the same time – without the hassle of having to set up and manage the deployment yourself.

This option gives you greater flexibility and protection from lock-in, because you are not tied to one public cloud platform or one private cloud platform. It also saves you from having to master the private cloud ecosystem in order to keep abreast of the latest developments and integrations. With a managed service, you can deploy the newest private cloud technologies without having to know much about how they work at a low level.

4.2.1 Conclusion

There are a number of different ways to deploy private clouds today. The major differences between them lie in how much effort and expertise they require on the part of users, as well as how much flexibility they offer (in terms of the infrastructure, private cloud platforms and cloud services you can use).

Each option has its own advantages and disadvantages. But generally speaking, if flexibility and freedom from lock-in are priorities, a managed private cloud service offers the greatest value.

4.3 What is Open Stack ?

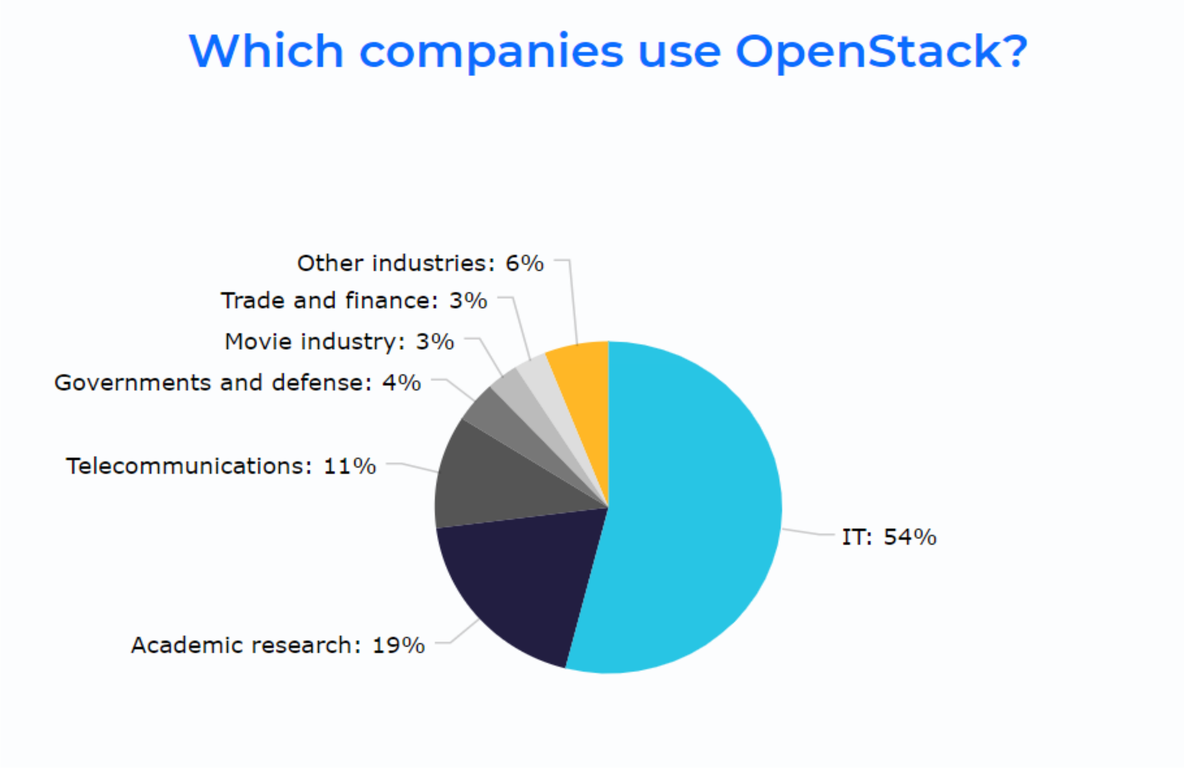
The OpenStack project is an open source cloud computing platform that supports all types of cloud environments. The project aims for simple implementation, massive scalability, and a rich set of features. Cloud computing experts from around the world contribute to the project.

OpenStack provides an Infrastructure-as-a-Service (IaaS) solution through a variety of complementary services. Each service offers an Application Programming Interface (API) that facilitates this integration.

This guide covers step-by-step deployment of the major OpenStack services using a functional example architecture suitable for new users of OpenStack with sufficient Linux experience. This guide is not intended to be used for production system installations, but to create a minimum proof-of-concept for the purpose of learning about OpenStack.

After becoming familiar with basic installation, configuration, operation, and troubleshooting of these OpenStack services, you should consider the following steps toward deployment using a production architecture:

- Determine and implement the necessary core and optional services to meet performance and redundancy requirements.
- Increase security using methods such as firewalls, encryption, and service policies.
- Use a deployment tool such as Ansible, Chef, Puppet, or Salt to automate deployment and management of the production environment. The OpenStack project has a couple of deployment projects with specific guides per version: - Yoga release - Xena release - Wallaby release - Victoria release - Ussuri release - Train release - Stein release - Rocky release - Queens release - Pike release



4.3.1 Advantages

1) Scaling is easier than ever

Scaling, elasticity or flexibility – whatever the name, it has been an important argument for cloud adoption. In a nutshell, it’s a way to adjust your computing capacity to the demands of a particular task. Does your website have a spike in visitors at a particular hour? Do you need to sometimes run several demanding calculations at once? Or are you in charge of a web-based app that is mostly used during the dinnertime? Where a physical server would be caught short of breath, cloud can keep up with the demand and provide the virtual server with more resources.

OpenStack makes this process easier. It’s designed to be ready for scaling, and it doesn’t matter whether that’s scaling up or down. It’s also designed to be ready for infrastructure not being always available or parts of it outright failing. And it makes admins’ jobs easier. Creating another instance happens at the drop of a hat. Deleting them when they’re not needed is just as quick. When a company uses cloud based on OpenStack, it can depend on it adjusting to its demands quickly. It doesn’t even matter if the company wants to run five instances or five thousand instances. OpenStack can do it all.

2) Rule the cloud through automatization

OpenStack offers admins powerful tools that can make managing a cloud a breeze. Many of the usual hassles can be automated. Its application program interface or API allows complete control over the cloud through other programs. This makes it easy to build an own app that can for instance fire up another virtual machine. This simplifies development of specific apps. The friendly API certainly makes development faster, which can make it cheaper overall.

3) Open platform allows fast development

One of the largest advantages OpenStack has is the fact that it's an open platform. Because the source code is publicly available, the development of the platform has seen experts from all around the world pitching in. This also means that OpenStack is not a child of a specific company that could use it as a license to print money because of the lack of competition. Even though the behemoths of IT industry like Intel, IBM or Dell are taking part in developing OpenStack, any company or a start-up can bring out its own products based on the platform.

It's a similar system to Linux. There are many different "distributions" of the operation system, each with its own features, even though they mostly share the same core. Many companies offer their own versions of OpenStack modules. Even though the "basic" source code is free, these distributions are usually paid. Experts argue that this makes it a perfect breeding ground for innovation – everyone starts from the same spot and needs to show creativity and come up with something new and better to offer their clients.

Thanks to the code being open, anyone can try OpenStack on their own. If it doesn't do exactly what people need, they can code the desired function themselves and share it with other devs . In the case of a proprietary software, they would have to wait for the original developers to add the feature in themselves, which might not happen for a long time (or ever, in case of very specific needs).

Instead anyone can code their own solution themselves. This allows cloud solution to move forward at a quick pace. The development is therefore very quick. The OpenStack Foundation that is running the ship pushes out a hefty update twice a year. The most recent one was Liberty, the twelfth version of the platform so far.

4) Benefits of a huge community: tips, documentation and experience

Because OpenStack is an open platform, it can boast about great number of users and developers all over the world. Similarly to Linux, it has managed to do something most open source projects dream about. It has successfully built a community around it.

According to the newest data, the development has been helped along by more than four thousand developers.

5) Advantage for businesses: Ready-made OpenStack

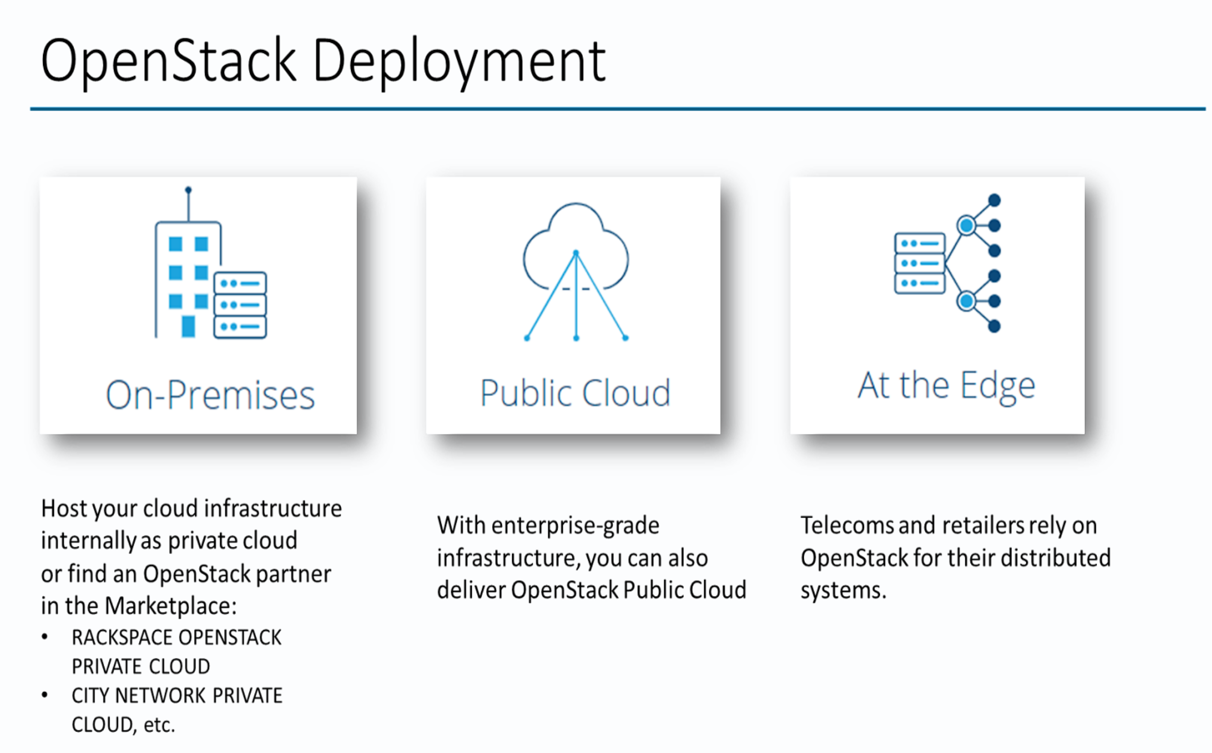
Everyone can run OpenStack on their hardware. However, as some observers have suggested, doing so might not be quite simple. It does require some proficiencies. There’s a need for an expert, but experts are in short supply on the job market, so they can charge their own weight in gold. That’s why the best solution for some companies might be buying a ready-to-go OpenStack cloud. All the complicated processes of starting up your copy of the platform are taken care of by a qualified team of the provider.

Managing the cloud can then be done even by administrators who have no previous experience with OpenStack. After they get more experienced with the platform, they can try building it on their own. This solution is quite useful for small companies. Their already very busy admins will have an easier time migrating into a cloud run on OpenStack. And the company can very quickly benefit from the OpenStack platform.

6) OpenStack cloud can be inexpensive

Cloud computing is usually considered to be an expensive affair. But it doesn't have to be. An OpenStack cloud can be acquired quite on the cheap.Building a cloud on OpenStack is perhaps not completely simple. Some experts even propose that this is an avenue that should be pursued only by bigger companies who can spare the people to build and develop the cloud. But there's still a way for small and medium-sized companies to benefit from OpenStack. They can do this through renting a ready-made cloud from cloud providers. This means the company doesn't have to cover the costs of building, configuring and completing the platform. It's done by the provider who can divide these expenses among his many customers, therefore making it much cheaper for all of them while providing the same-quality service.All such customers can get a working OpenStack cloud quickly and very cheaply. Master DC, for instance, offers a basic OpenStack cloud for less than a dollar per day.

4.3.2 OpenStack Deployment



OpenStack Deployment

On-Premises

Public Cloud

At the Edge

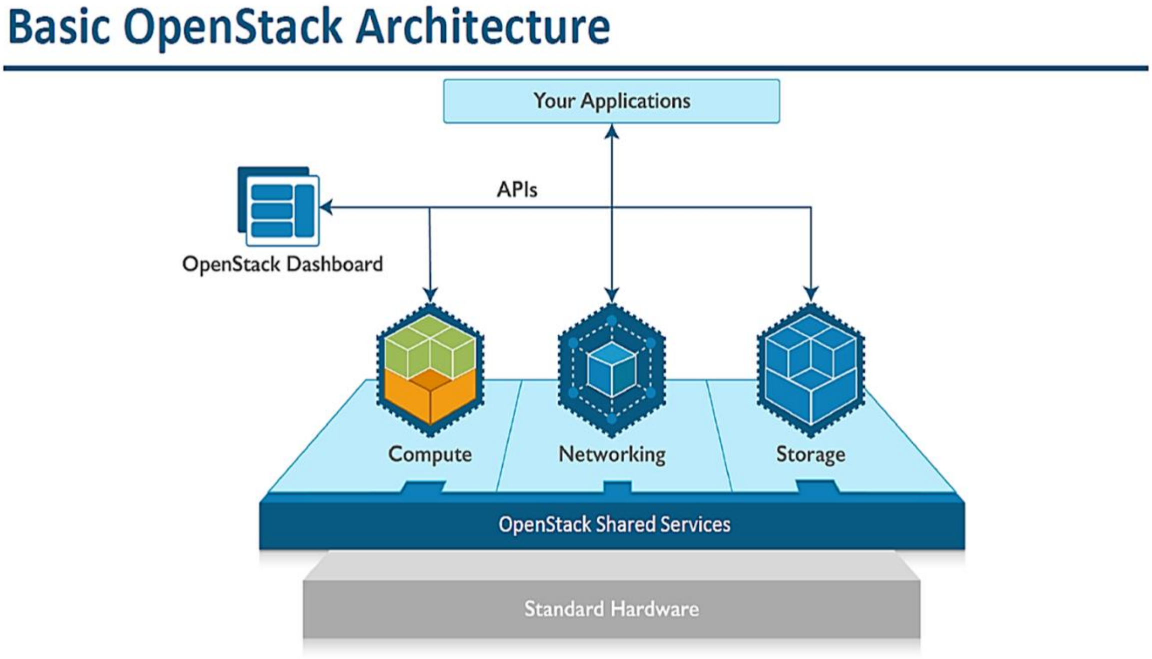
Host your cloud infrastructure internally as private cloud or find an OpenStack partner in the Marketplace:

- RACKSPACE OPENSTACK PRIVATE CLOUD
- CITY NETWORK PRIVATE CLOUD, etc.

With enterprise-grade infrastructure, you can also deliver OpenStack Public Cloud

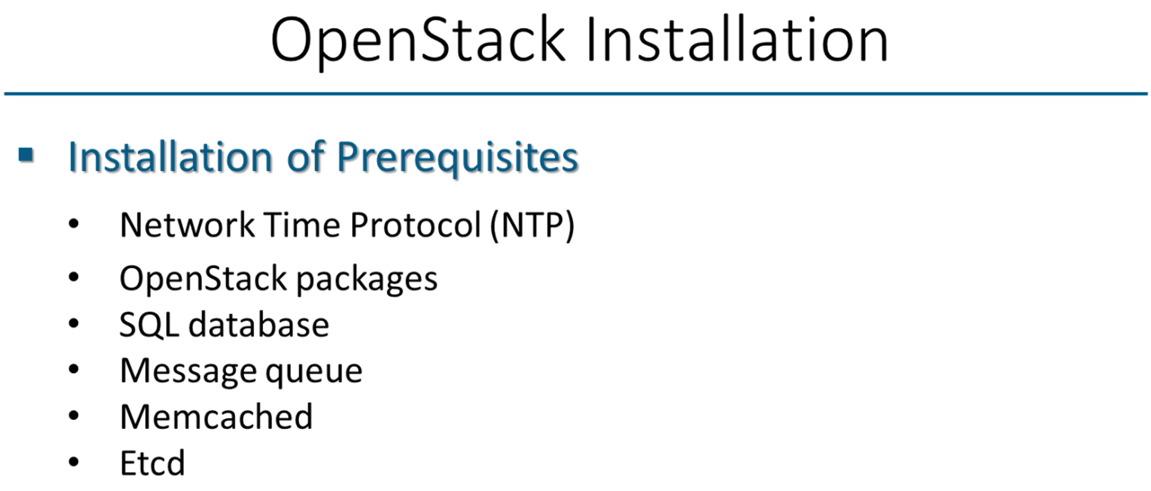
Telecoms and retailers rely on OpenStack for their distributed systems.

4.3.3 OpenStack Architecture



Basic OpenStack Architecture

4.3.4 OpenStack Installation



OpenStack Installation

- Installation of Prerequisites
  - Network Time Protocol (NTP)
  - OpenStack packages
  - SQL database
  - Message queue
  - Memcached
  - Etcd

OpenStack Installation: Prerequisites

- Network Time Protocol (NTP): (Controller, Other, verify)
  - To properly synchronize services among nodes, you can install Chrony, an implementation of NTP. We recommend that you configure the controller node to reference more accurate (lower stratum) servers and other nodes to reference the controller node.
- OpenStack packages (All Nodes)
  - Distributions release OpenStack packages as part of the distribution or using other methods because of differing release schedules. Perform these procedures on all nodes.
- SQL database (Controller Node)
  - Most OpenStack services use an SQL database to store information. The database typically runs on the controller node. The procedures in this guide use MariaDB or MySQL depending on the distribution. OpenStack services also support other SQL databases including PostgreSQL.

- Message queue (Controller Node)
  - OpenStack uses a message queue to coordinate operations and status information among services. The message queue service typically runs on the controller node. OpenStack supports several message queue services including RabbitMQ, Qpid, and ZeroMQ. However, most distributions that package OpenStack support RabbitMQ message queue service.
- Memcached (Controller Node)
  - The Identity service authentication mechanism for services uses Memcached to cache tokens. The memcached service typically runs on the controller node. For production deployments, we recommend enabling a combination of firewalling, authentication, and encryption to secure it.
  - Etcd (Controller Node)
- Etcd (Controller Node)
  - OpenStack services may use Etcd, a distributed reliable key-value store for distributed key locking, storing configuration, keeping track of service live-ness and other scenarios.

Minimum Hardware Requirement

- Controller
  - The controller node runs the Identity service, Image service, Placement service, management portions of Compute, management portion of Networking, various Networking agents, and the Dashboard. It also includes supporting services such as an SQL database, message queue, and NTP.
  - Optionally, the controller node runs portions of the Block Storage, Object Storage, Orchestration, and Telemetry services.
  - The controller node requires a minimum of two network interfaces.
- Compute
  - The compute node runs the hypervisor portion of Compute that operates instances. By default, Compute uses the KVM hypervisor. The compute node also runs a Networking service agent that connects instances to virtual networks and provides firewalling services to instances via security groups.
  - You can deploy more than one compute node. Each node requires a minimum of two network interfaces.

OpenStack Installation using DevStack

- Recommended System Configuration
  - **OS**: Ubuntu 20.04 (or Any Linux Distribution)
  - **RAM**: Min 8 GB
  - **Storage**: 30 GB
  - **Static IP**

- **Note:** Update, Upgrade and Reboot the System before installation

- Installation Guide:
  - https://docs.openstack.org/devstack/latest/

Chapter-5:
Cloud Security

5.1 What is Cloud Security?

Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

The terms digital transformation and cloud migration have been used regularly in enterprise settings over recent years. While both phrases can mean different things to different organizations, each is driven by a common denominator: the need for change.

5.1.1 Why is Cloud Security important?

In modern-day enterprises, there has been a growing transition to cloud-based environments and IaaS, Paas, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring a number of challenges to enterprises when adequately resourcing their departments. These as-a-service models give organizations the ability to offload many of the time-consuming, IT-related tasks.

As companies continue to migrate to the cloud, understanding the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability doesn't necessarily shift along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when protecting data, applications, and workloads running on the cloud.

Security threats have become more advanced as the digital landscape continues to evolve. These threats explicitly target cloud computing providers due to an organization's overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information, regardless of where it is stored.

5.1.2 Aspects of Cloud Security

1: Top-of-the-Line Perimeter Firewall

Top-of-the-line firewalls, such as Palo Alto Networks' perimeter firewall solution will check the contents of the file packet to examine the type of file in addition to source, destination, and integrity. Such granularity is necessary to thwart the most advanced persistent threats out there today.

2: Intrusion Detection Systems with Event Logging

Numerous IT security compliance standards require businesses to have a means of tracking and recording intrusion attempts. So, for any business that wants to meet compliance standards such as PCI or HIPAA, using IDS event logging solutions is a must.

3: Internal Firewalls for Individual Applications, and Databases

While having a strong perimeter firewall can block external attacks, internal attacks are still a major threat. Infrastructures that lack internal firewalls to restrict access to sensitive data and applications cannot be considered secure.

4: Data-at-Rest Encryption

Encrypting the data that is stored on your cloud infrastructure can be an effective way to keep your most sensitive information from being accessed by the wrong party. Strong encryption can minimize the risk of stolen data being used against your company or your customers/clients

5: Tier IV Data Centers with Strong Physical Security

Tier IV data centers help protect cloud environments by restricting access to the physical systems that run the cloud environment. A secure Tier IV facility will use measures such as:

- Armed security patrols
- Controlled access checkpoints with biometric security controls
- 24/7 CCTV monitoring

5.2 Cloud Security Issues

1.Misconfiguration

Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Several factors contribute to this. Cloud infrastructure is designed to be easily usable and to enable easy data sharing, making it difficult for organizations to ensure that data is only accessible to authorized parties. Also, organizations using cloud-based infrastructure also do not have complete visibility and control over their infrastructure, meaning that they need to rely upon security controls provided by their cloud service provider (CSP) to configure and secure their cloud deployments

2.Unauthorized Access

Unlike an organization's on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization's cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization's knowledge.

3.Insecure Interfaces/APIs

CSPs often provide a number of application programming interfaces (APIs) and interfaces for their customers. In general, these interfaces are well-documented in an attempt to make them easily-usable for a CSP's customers.

However, this creates potential issues if a customer has not properly secured the interfaces for their cloud-based infrastructure. The documentation designed for the customer can also be used by a cybercriminal to identify and exploit potential methods for accessing and exfiltrating sensitive data from an organization's cloud environment.

4.Hijacking of Accounts

Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions. An attacker with an employee's credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account.

Additionally, in the cloud, organizations often lack the ability to identify and respond to these threats as effectively as for on-premises infrastructure.

5.Lack of Visibility

An organization's cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own.

As a result, many traditional tools for achieving network visibility are not effective for cloud environments, and some organizations lack cloud-focused security tools. This can limit an organization's ability to monitor their cloud-based resources and protect them against attack.

6.External Sharing of Data

While this easy data sharing is an asset, it can also be a major cloud security issue. The use of link-based sharing – a popular option since it is easier than explicitly inviting each intended collaborator – makes it difficult to control access to the shared resource.

The shared link can be forwarded to someone else, stolen as part of a cyberattack, or guessed by a cybercriminal, providing unauthorized access to the shared resource. Additionally, link-based sharing makes it impossible to revoke access to only a single recipient of the shared link.

7.Malicious Insiders

On the cloud, detection of a malicious insider is even more difficult. With cloud deployments, companies lack control over their underlying infrastructure, making many traditional security solutions less effective.

This, along with the fact that cloud-based infrastructure is directly accessible from the public Internet and often suffers from security misconfigurations, makes it even more difficult to detect malicious insiders.

8.Cyberattacks

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data.

Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations’ cloud deployments are a common target of cyberattacks.

9.Denial of Service Attacks

The cloud is essential to many organizations’ ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications.

This means that a successful Denial of Service (DoS) attack against cloud infrastructure is likely to have a major impact on a number of different companies. As a result, DoS attacks where the attacker demands a ransom to stop the attack pose a significant threat to an organization’s cloud-based resources.

5.3 Cloud Security models

The cloud security architecture model is usually expressed in terms of:

- **Security controls**—which can include technologies and processes. Controls should take into account the location of each service—company, cloud provider, or third party.
- **Trust boundaries**—between the different services and components deployed on the cloud
- **Standard interfaces and security protocols**—such as SSL, IPSEC, SFTP, LDAPS, SSH, SCP, SAML, OAuth, etc.)
- **Techniques used for token management**—authentication, and authorization
- **Encryption methods** including algorithms like 128-bit AES, Triple DES, RSA, Blowfish.
- **Security event logging**—ensuring all relevant security events are captured, prioritized, and delivered to security teams.

Each security control should be clearly defined using the following attributes:

- **Service function -**
  what is the service's role? For example, encryption, authorization, event data collection.

- **Logical location -**
  public cloud service, third party service, or on-premises. Location affects performance, availability, firewall policies, and service management.

- **Protocol -**
  what protocol is used to access the service? For example, REST, HTTPS, SSH.

- **Input/Output -**
  what does the service receive and what is it expected to deliver? For example, input is a JSON feed and output is the same feed with encrypted payload data.

- **Control mechanisms -**
  what types of control does the service achieve? For example, data at rest protection, user authentication, application authentication.

- **Users and operators -**
  who operates or benefits from the service? For example, endpoint devices, end users, business managers, security analysts.

5.4 Cloud Computing Security Architecture Per Cloud Service Model

The cloud security architecture model differs depending on the type of cloud service: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), or SaaS (Software as a Service). Below we explain different security considerations for each model.

IaaS Cloud Computing Security Architecture

IaaS provides storage and network resources in the cloud. It relies heavily on APIs to help manage and operate the cloud. However, cloud APIs are often not secure, because they are open and easily accessible from the web.
The cloud service provider (CSP) is responsible for securing the infrastructure and abstraction layer used to access the resources. Your organization's security obligations cover the rest of the layers, mainly containing the business applications.
To better visualize cloud network security issues, deploy a Network Packet Broker (NPB) in an IaaS environment. The NPB sends traffic and data to a Network Performance Management (NPM) system, and to the relevant security tools. In addition, establish logging of events occurring on network endpoints.
IaaS cloud deployments require the following additional security features:

- Network segmentation
- Intrusion Detection System and Intrusion Prevention System (IDS/IPS)

- Virtual firewalls placed in front of web applications to protect against malicious code, and at the edge of the cloud network
- Virtual routers

SaaS Cloud Computing Security Architecture

SaaS services provide access to software applications and data through a browser. The specific terms of security responsibility may vary between services, and are sometimes up for negotiation with the service provider.

Cloud Access Security Brokers (CASB) offers logging, auditing, access control and encryption capabilities that can be critical when investigating security issues in a SaaS product. In addition, make sure your SaaS environment has:

- Logging and alerting
- IP whitelists and/or blacklists
- API gateways, in case the service is accessed via API

PaaS Cloud Computing Security Architecture

PaaS platforms enable organizations to build applications without the overhead and complexity associated with managing hardware and back-end software. In a PaaS model, the CSP protects most of the environment. However, the company is still responsible for the security of the applications it is developing.

Therefore, a PaaS security architecture is similar to a SaaS model. Ensure you have CASP, logging and alerting, IP restrictions and an API gateway to ensure secure internal and external access to your application’s APIs.

REFERENCES

https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html

https://enlyft.com/tech/products/openstack

https://arxiv.org/pdf/1805.11912.pdf

https://syneto.eu/2016/10/20/benefits-of-choosing-private-cloud/

https://www.geeksforgeeks.org/cloud-deployment-models/

https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-private-cloud/

https://www.projectpro.io/recipes/explain-amazon-ec2-and-advantages-of-ec2

https://docs.openstack.org/install-guide/overview.html

https://aws.amazon.com/s3/getting-started/

https://www.irjmets.com/uploadedfiles/paper/volume3/issue_7_july_2021/14969/1628083581.pdf

https://www.guru99.com/creating-amazon-ec2-instance.html

https://www.vmware.com/topics/glossary/content/public-cloud.html#:~:text=Definition%20of%20Public%20Cloud,multiple%20tenants%20via%20the%20Internet.

https://aws.amazon.com/what-is-cloud-computing/

https://www.salesforce.com/in/products/platform/best-practices/benefits-of-cloud-computing/

https://www.geeksforgeeks.org/features-components-of-private-cloud/