TYBSC-CS CLOUD COMPUTING UNIT-III

1. Virtualization :-

- **Virtualization** is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".
- Virtualization is a technique, which allows to share single physical instance of an application or resource among multiple organizations or tenants (customers).
- It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource on demand.
- It is the process of creating a virtual version of something like computer hardware.
- It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource.
- With the help of Virtualization multiple operating systems and applications can run on same Machine and its same hardware at the same time increasing the utilization and flexibility of hardware.
- The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.
- The machine on which the virtual machine is going to be build is known as Host Machine and that virtual machine is referred as a Guest Machine.

Benefits of virtualization:

- Minimize the hardware cost.
- Multiple virtual servers on one single physical hardware.
- Easily moves VM's to other data center.
- It provides hardware maintenance.
- Increased device utilization.
- Free up unused physical resource.
- Pay per use of the IT infrastructure on demand.
- Enhance development productivity.
- It lowers the cost of IT infrastructure.
- Remote access and rapid scalability.

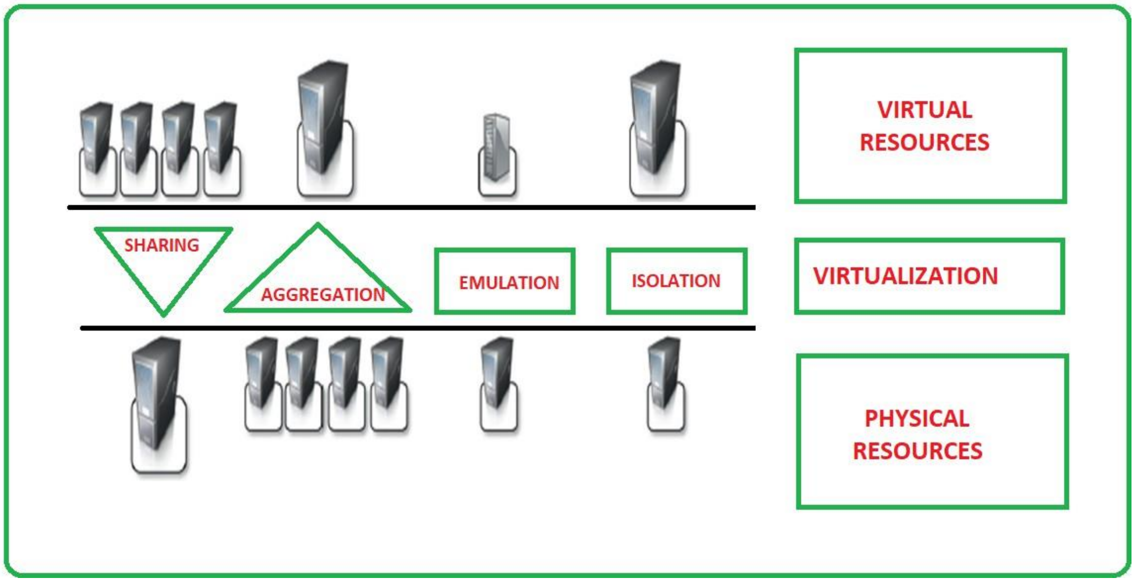
Characteristics Of Virtualized Environments: -

i. **Increased Security :-**

- The ability to control the execution of a guest programs in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment.
- All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
- A virtual machine manager can control and filter the activity of the guest programs, thus preventing some harmful operations from being performed.
- Resources exposed by the host can then be hidden or simply protected from the guest.
- Increased security is a requirement when dealing with untrusted code.

ii. **Managed Execution :-**

- Virtualization of the execution environment not only allows increased security, but a wider range of features also can be implemented.
- In particular, sharing, aggregation, emulation, and isolation are the most relevant features.



a. **Sharing :-**

- Virtualization allows the creation of a separate computing environments within the same host. This basic feature is used to reduce the number of active servers and limit power consumption.

b. **Aggregation:-**

- Not only it is possible to share physical resource among several guests, but virtualization also allows aggregation, which is the opposite process. A group of separate hosts can be tied together and represented to guests as a single virtual host.
- This functionality is implemented with cluster management software, which harnesses the physical resources of a homogeneous group of machines and represents them as a single resource.

c. **Emulation :-**

- Guest programs are executed within an environment that is controlled by the virtualization layer, which ultimately is a program. Also a completely different environment with respect to the host can be emulated, thus allowing the execution of guest programs requiring specific characteristics that are not present in the physical host.

d. **Isolation :-**

- Virtualization allows providing guests—whether they are operating systems, applications, or other entities—with a completely separate environment, in which they are executed.
- The guest program performs its activity by interacting with an abstraction layer, which provides access to the underlying resources.

- The virtual machine can filter the activity of the guest and prevent harmful operations against the host.

iii Probability:-

- The concept probability applies in different ways according to the specific type of virtualization considered . In case the hardware virtualization solution the guest is packaged into a virtual image that , in most cases, can be safely moved and executed on the top of different virtual machine.
- In programming level virtualization which is implemented in JVM and .NET runtime, the binary code representing application components can run without any recompilation on any implementation of the corresponding virtual machine.

2. The Virtualization Reference Model:-

- Virtualizationisabroadconceptthatreferstothecreationofavirtualversionofsomething, whether hardware, a software environment, storage ,or a network.
- In a virtualized environment there are three major components:

i. Guest
ii. Host
iii. Virtualization layer.

i. **Guest:-**

- Virtual machine is referred as a guest machine
- The guest represents the system component that interacts with the virtualization layer rather than with the host ,as would normally happen.
- Guests usually consist of one or more virtual disk files, and a VM definition file.
- Virtual Machines are centrally managed by a host application that sees and manages each virtual machine as a different application.

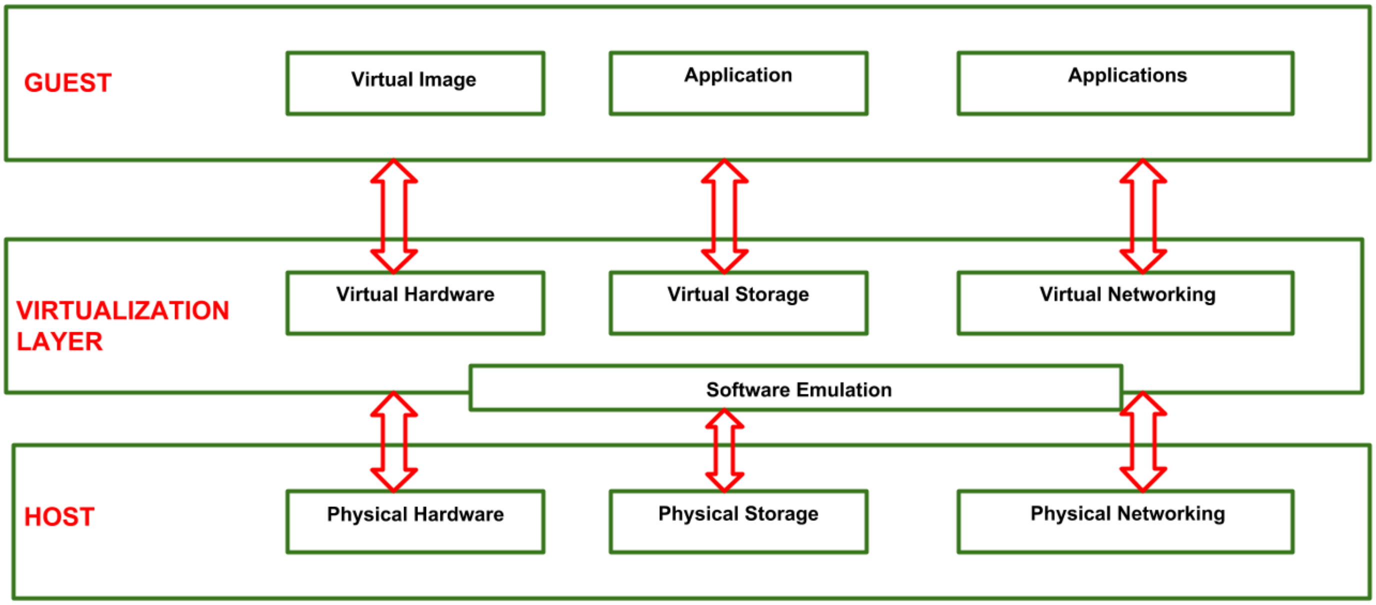
ii. **Host:-**

- The machine on which the virtual machine is created is known as host machine .
- The host represents the original environment where the guest is supposed to be managed.
- Each guest runs on the host using shared resources donated to it by the host.
- The operating system, works as the host and manages the physical resource management, and the device support.

iii. **Virtualization layer:-**

- The virtualization layer is responsible for recreating the same or a different environment where the guest will operate.
- It is an additional abstraction layer between a network and storage hardware, computing, and the application running on it.

- Usually it helps to run a single operating system per machine which can be very inflexible compared to the usage of virtualization.



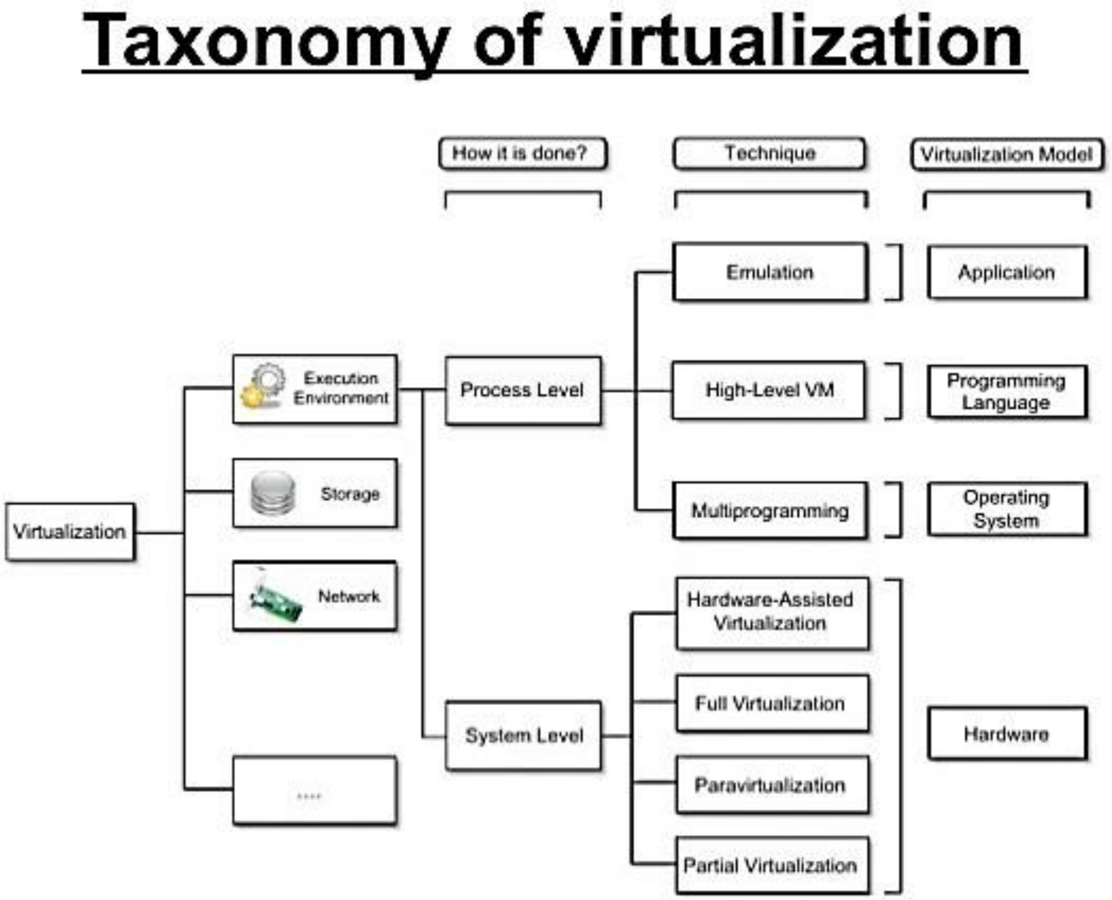
3. TAXONOMY OF VIRTUALIZATION TECHNIQUES:-

- Virtualization covers a wide range of emulation (hardware or software that enables one computer system to behave like another computer system) techniques that are applied to different areas of computing.
- A classification of these techniques helps us better understand their characteristics and use.
- The first classification discriminates against the service or entity that is being emulated. Virtualization is mainly used to emulate execution environments, storage, and networks.
- Among these categories, execution virtualization constitutes the oldest, most popular, and most developed area.
- Therefore, it deserves major investigation and a further categorization.
- In particular we can divide these execution virtualization techniques into two major categories by considering the type of host they require.
- Process-level techniques are implemented on top of an existing operating system, which has full control of the hardware.
- System-level techniques are implemented directly on hardware and do not require a minimum of support from—an existing operating system.
- Within these two categories we can list various techniques that offer the guest a different type of virtual computation environment :bare hardware, operating system resources low-level programming language, and application libraries.

A. Execution virtualization:-

- Execution virtualization includes all techniques that aim to emulate an execution environment that is separate from the one hosting the virtualization layer.

- All these techniques concentrate their interest on providing support for the execution of programs, whether these are the operating system, a binary specification of a program compiled against an abstract machine model, or an application.
- Therefore, execution virtualization can be implemented directly on top of the hardware by the operating system, an application, or libraries dynamically or statically linked to an application image.

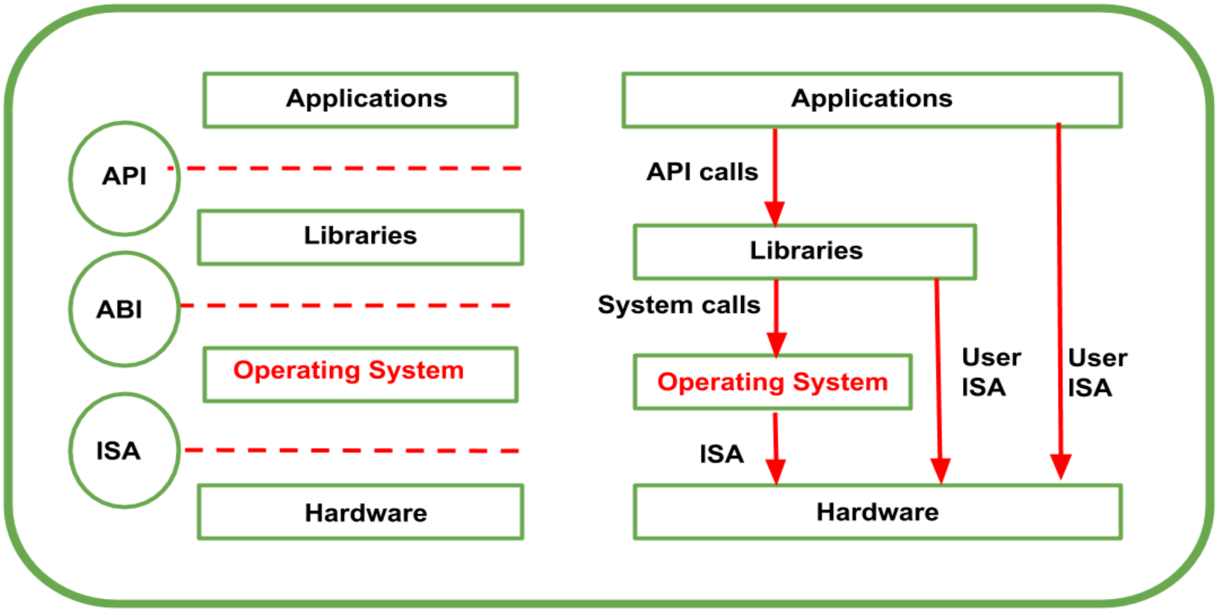


i. MACHINE REFERENCE MODEL:-

- Virtualizing an execution environment at different levels of the computing stack requires a reference model that defines the interfaces between the levels of abstractions, which hide implementation details.
- From this perspective, virtualization techniques actually replace one of the layers and intercept the calls that are directed toward it.
- Therefore, a clear separation between layers simplifies their implementation, which only requires the emulation of the interfaces and a proper interaction with the underlying layer.
- Modern computing systems can be expressed in terms of the reference model described in At the bottom layer, the model for the hardware is expressed in terms of the Instruction Set Architecture (ISA), which defines the instruction set for the processor, registers, memory, and interrupt management.

- ISA is the interface between hardware and software, and it is important to the operating system(OS) developer(System ISA) and developers of applications that directly manage the underlying hardware (User ISA).
- The application binary interface (ABI) separates the operating system layer from the applications and libraries, which are managed by the OS.

- ABI covers details such as low-level data-types, alignment, and call conventions and defines a format for executable programs.
- System calls are defined at this level.
- This interface allows portability of applications and libraries across operating systems that implement the same ABI.
- The highest level of abstraction is represented by the application programming interface(API), which interfaces applications to libraries and/or the underlying operating system.
- For any operation to be performed in the application level API, ABI and ISA are responsible for making it happen.
- The high-level abstraction is converted into machine-level instructions to per- form the actual operations supported by the processor.
- The machine-level resources, such as processor registers and main memory capacities, are used to perform the operation at the hardware level of the central processing unit (CPU).
- This layered approach simplifies the development and implementation of computing systems and simplifies the implementation of multitasking and the coexistence of multiple executing environments.
- In fact, such a model not only requires limited knowledge of the entire computing stack, but it also provides ways to implement a minimal security model for managing and accessing shared



resources.

ii. HARDWARE-LEVEL VIRTUALIZATION:-

- Hardware-level virtualization is a virtualization technique that provides an abstract execution environment in terms of computer hardware on top of which a guest operating system can be run.
- In this model, the guest is represented by the operating system, the host by the physical computer hardware, the virtual machine by its emulation, and the virtual machine manager by the hypervisor.
- The hypervisor is generally a program or a combination of software and hardware that allows the abstraction of the underlying physical hardware.
- Hardware-level virtualization is also called system virtualization, since it provides ISA to virtual machines, which is the representation of the hardware interface of a system.
- This is to differentiate it from process virtual machines, which expose ABI to virtual machines.

Hypervisor:-

- A fundamental element of hardware virtualization is the hypervisor, or virtual machine manager (VMM).
- Hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time.
- A hypervisor is sometimes also called a virtual machine manager (VMM).
- There are two major types of hypervisor: Type I and Type II.

i. Type-I:-
  - Type I hypervisors run directly on guest hardware.
  - Therefore, they take the place of the operating systems and interact directly with the ISA interface exposed by the underlying hardware, and they emulate this interface in order to allow the management of guest operating systems.
  - This type of hypervisor is also called a native or bare metal virtual machine since it runs natively on hardware.
  - Modern hypervisors include Xen, Oracle VM Server for SPARC, Oracle VM Server for x86, Microsoft Hyper-V and VMware's ESX/ESXi.

ii. Type-II:-
  - Type II hypervisors require the support of an operating system to provide virtualization services.
  - This means that they are programs managed by the operating system, which interact with it through the ABI and emulate the ISA of virtual hardware for guest operating systems.
  - This type of hypervisor is also called a hosted virtual machine since it is hosted within an operating system.
  - Examples of Type 2 hypervisors include VMware Workstation, VMware Player, VirtualBox and Parallels Desktop for Mac.

Benefits of hypervisors

- Even though VMs can run on the same physical hardware, they are still logically separated from each other. This means that if one VM experiences an error, crash or a malware attack, it doesn't extend to other VMs on the same machine, or even other machines.

- VMs are also very mobile – because they are independent of the underlying hardware, they can be moved or migrated between local or remote virtualized servers a whole lot easier than traditional applications that are tied to physical hardware.

HARDWARE VIRTUALIZATION TECHNIQUES: -

- Hardware virtualization also known as hardware-assisted virtualization or server virtualization runs on the concept that an individual independent segment of hardware or a physical server, may be made up of multiple smaller hardware segments or servers, essentially consolidating multiple physical servers into **virtual servers** that run on a single primary physical server.
- Each small server can host a virtual machine, but the entire cluster of servers is treated as a single device by any process requesting the hardware.
- The hardware resource allotment is done by the hypervisor.
- The main advantages include increased processing power as a result of maximized hardware utilization and application uptime.
- Virtualization techniques are used to generate numerous isolated partitions on a single physical server and these techniques vary in the Virtualization solutions methods and the level of abstraction while offering similar traits and traveling towards the same goal.

  The most popular virtualization techniques are:

i. Hardware-assisted virtualization
ii. Full virtualization.
iii. Para virtualization.
iv. Partial virtualization.

i. Hardware-assisted virtualization:-

- This term refers to a scenario in which the hardware provides architectural support for building a virtual machine manager able to run a guest operating system in complete isolation.
- **hardware-assisted virtualization** is a platform virtualization approach that enables efficient full virtualization using help from hardware capabilities, primarily from the host processors.
- Hardware-assisted virtualization is also known as **accelerated virtualization**; Xen calls it **hardware virtual machine** (**HVM**), and Virtual Iron calls it **native virtualization**.

ii. Full Virtualization:-

- This technique fully virtualizes the main physical server to support applications and software to operate in a much similar way on virtualized divisions.
- This creates an environment as if it is working on a unique server.
- Full virtualization technique enables the administrators to run unchanged and entirely virtualized operating system.
- A full virtualization is used to emulate a complete hardware environment, or virtual machine, in which an unmodified guest operating system (using the same instruction set as the host machine) effectively executes in complete isolation.

iii. Para virtualization:-

- This methodology clearly runs modified versions of operating systems.
- Only the software and programs are carried out in a precise manner to work for their exclusive websites without executing any kind of hardware simulation.
- Using this technique, the guest is very well aware of its environment as the para-virtualized OS is altered to be alert about its virtualization.

- Paravirtualization is a technique in which the hypervisor provides an API and the OS of the guest virtual machine calls that API, requiring OS modifications.

iv. Partial Virtualization:-

- Virtual machines are popularly known as VMs, imitate certain factual or illusory hardware requiring the valid resources from the host, which is nothing but the actual machine operating the VMs.
- A virtual machines monitor (VMM) is used in certain cases where the CPU directives need extra privileges and may not be employed in user space.

iii. Programming Language-Level Virtualization: -

- Programming language-level virtualization is mostly used to achieve ease of deployment of applications, managed execution, and portability across different platforms and operating systems.
- It consists of a virtual machine executing the byte code of a program, which is the result of the compilation process.
- Compilers implemented and used this technology to produce a binary format representing the machine code for an abstract architecture.
- The characteristics of this architecture vary from implementation to implementation.
- Generally, these virtual machines constitute a simplification of the underlying hardware instruction set and provide some high-level instructions that map some of the features of the languages compiled for them.
- Programming language-level virtualization has a long trail in computer science history and originallywasusedin1966fortheimplementationof Basic Combined Programming Language a language for writing compilers and one of the ancestors of the C programming language.
- Virtual machine programming languages become popular again with Sun’s introduction of the Java platform in 1996.
- Originally created as a platform for developing Internet applications, Java became one of the technologies of choice for enterprise applications, and a large community of developers formed around it.

Advantages: -

- The main advantage of programming level virtual machines , also called process virtual machines, istheabilitytoprovideauniformexecutionenvironmentacrossdifferentplatforms.
- Programs compiled into byte code can be executed on any operating system and platform for which a virtual machine able to execute that code has been provided.
- The implementation of the virtual machine for different platforms is still a costly task, but it is done once and not for any application.
- Moreover, process virtual machines allow for more control over the execution of programs since they do not provide direct access to the memory.
- Security is another advantage of managed programming languages; by filtering the I/O operations, the process virtual machine can easily support sandboxing of applications. As an example, both Java and .NET provide an infrastructure for pluggable security policies and code access security frameworks.

iv. Application-Level Virtualization:-

- Application-level virtualization is a technique allowing applications to be run in runtime environments that do not natively support all the features required by such applications.
- In this scenario, applications are not installed in the expected runtime environment but are run as though they were.
- In general, these techniques are mostly concerned with partial file systems, libraries, and operating system component emulation.
- Such emulation is performed by a thin layer—a program or an operating system component—that is in charge of executing the application.
- Emulation can also be used to execute program binaries compiled for different hardware architectures.
- In this case, one of the following strategies can be implemented:
  i. Interpretation.
  ii. Binary translation

i. Interpretation:-

- In this technique every source instruction is interpreted by an emulator for executing native ISA instructions, leading to poor performance.
- Interpretation has a minimal startup cost but a huge overhead, since each instruction is emulated.

ii. Binary translation:-

- In this technique every source instruction is converted to native instructions with equivalent functions.
- After a block of instructions is translated, it is cached and reused.
- Binary translation has a large initial overhead cost, but over time it is subject to better performance, since previously translated instruction blocks are directly executed.

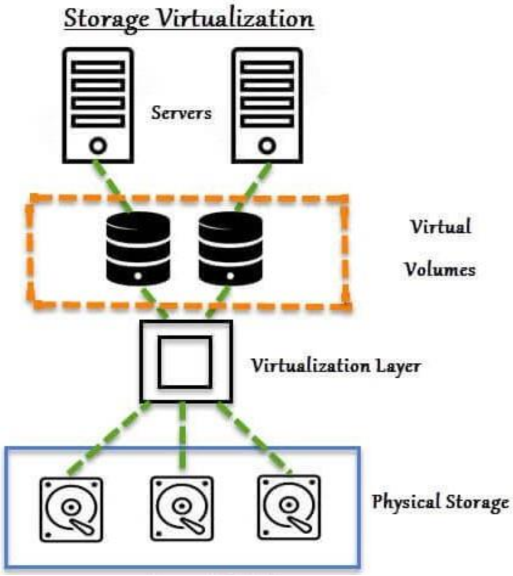
Advantage:-

- Application virtualization is a good solution in the case of missing libraries in the host operating system; in this case a replacement library can be linked with the application, or library calls can be remapped to existing functions available in the host system.
- Another advantage is that in this case the virtual machine manager is much lighter since it provides a partial emulation of the runtime environment compared to hardware virtualization.
- This technique allows incompatible applications to run together.
- Compared to programming-level virtualization, which works across all the applications developed for that virtual machine, application-level virtualization works for a specific environment: It supports all the applications that run on top of a specific environment.

Other Types Of Virtualization:- Other than execution virtualization, other types of virtualization provide an abstract environment to interact with. These mainly cover storage, networking, and client/server interaction.

i. Storage virtualization:-

- Storage virtualization in Cloud Computing is nothing but the sharing of physical storage into multiple storage devices which further appears to be a single storage device. It can be also called as a group of an available storage device which simply manages from a central console.
- This whole process requires very less time and works in an efficient manner. Storage virtualization in Cloud Computing does not show the actual complexity of the Storage Area Network (SAN). This virtualization is applicable to all levels of SAN.
- The software actually constantly monitors the various I/O requests from any virtual/physical system and it intercepts them and sends it to the appropriate location where the combined storages are maintained in a virtual environment.
- This technique of storage virtualization actually helps the administrator for any recovery or backup or archival of data in an effective and efficient manner by making comparatively less time than the usual.

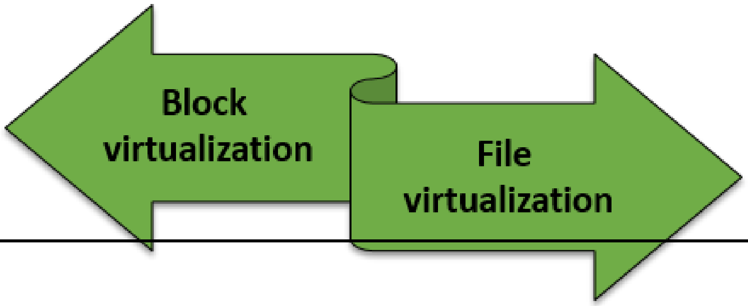


Why Storage Virtualization should be implemented?

Following are the reasons shows why we storage virtualization in Cloud Computing implements:

- If this virtualization implements in IT environment it will improve the management of the storage**.** As each and everything will properly store and manage there won’t be any congestion and the task will perform quickly.
- There will be very less downtime as the storage availability is better. All these problems eliminate with the help of an automated management system.
- Storage virtualization will provide better storage utilization as storing most information in a particular place can cause loss of data, congestion, and any other problems. So, properly dividing storage and storing data can be useful.

Types of Storage Virtualization



File-based Storage Virtualization

- This type of virtualization is used for a specific purpose and can apply to network-attached storage (NAS) system.
- File-based storage virtualization in Cloud Computing utilizes server message block or network file system protocols and with its help of it breaks the dependency in a normal network attached storage array.
- This is done between the data being accessed and the location of the physical memory. It also provides a benefit of better handling file migration in the background which improves the performance.

Block-based Virtual Storage

- The Block based virtual storage is more widely used than the virtual storage system as the virtual storage system is sometimes used for a specific purpose.
- The block-based virtual storage system uses logical storage such as drive partition from the physical memory in a storage device. It also abstracts the logical storage such as a hard disk drive or any solid state memory device.
- This also allows the virtualization management software to get familiar with the capacity of the available device and split them into shared resources to assign.

Methods of Virtualization

- Virtualization typically refers to the pooling of different available storage and maintaining them in single storage in virtual environment, recent technologies such as hyper-converged infrastructure makes use of not only virtual storage but also power and network as well.
- Let us discuss the different ways in which these storages can be used in a virtual environment:

Host-Based Storage Virtualization –

- In the approach, the virtualization is done at the host level, where we present the user with virtual storage with different capacity sets where the hosts are multiple, irrespective of whether the end-user is using a virtual machine or a personal computer that accesses the cloud storage.
- The virtualization is done with the help of software and for our physical storage we can make use of any device. Let us see some of the advantages and disadvantages of this approach.
- The major positives are its simple for designing and coding, it can support any type of storage and helps in improving the utilization of storage.
- Some of the concerns are that it has unique software for each OS, synchronization of the host is a difficult task, and optimization can only be done on a cost basis.

Network-Based Storage Virtualization –

- This is the approach that is widely famously used in many of the big enterprises today.
- In this approach, it makes use of a fiber channel wherein any network device such as a purpose-built server or a smart switch, connect to a SAN (storage area network) and will be represented as a virtual storage pool to the guest user.
- The major advantage of this approach is that it helps in achieving the true form of heterogeneous virtualization, helps in improving the performance, only one management device for all the storage that are involved and it is easy in replicating the services across all the devices.
- Some of the major disadvantages are very difficult in interpreting the matrices involved, adds some latency to I/O, difficult to design and code, and it is difficult to implement when we are dealing with fast metadata.

Array-Based Storage Virtualization –

- In this method, we basically represent our storage as an array of devices that represents the physical storage, where usually these storages consist of HDD's (Hard disk drive) and SDD's (Solid-state drives).
- We make use of different software's to handle these arrays of storage and we hide them at the user/guest level. A few advantages in this method is that we would not require any type of additional hardware/infrastructure and there is zero latency in attending a particular I/O.
- Some of the disadvantages are that all the storages such as primary, secondary, etc. would require the same amount of bandwidth and hence there is a need for infrastructure, it is specific to vendor's matrix, and optimization of the storage utilization not done overall

Storage Virtualization Risks

Limited Adoption

- The one-third of the enterprise is reporting in a computer economics survey that they are increasing the funds for storage virtualization. There are some understanding of adoption rates, return of investment and the cost of ownership.

Problems in Naming

- Before very less VMS was used but now there has been a rapid growth of VMS which makes it difficult to distinguish between the important and the important VMS. To make it more future proof building a naming system and sharing with it with all involved parties should be done.

Failure

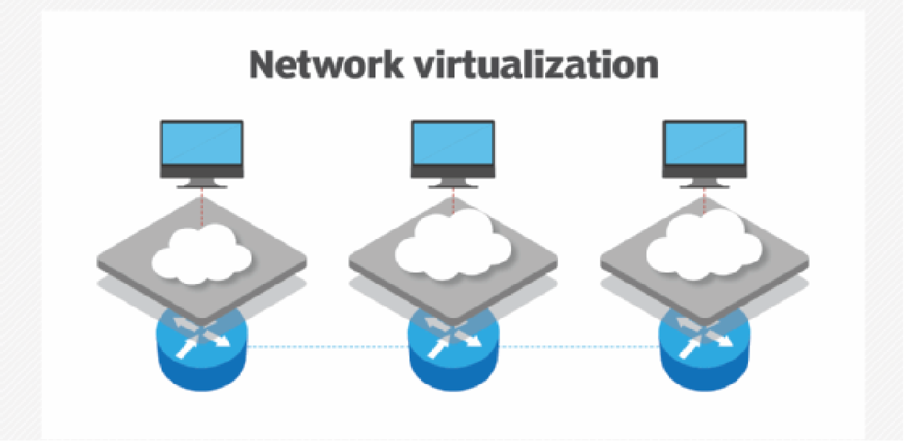
- The failure occurs due to downtime and data loss. The installation of VMware which hosts crucial services becomes a single point of failure. So to eliminate this threat the protection of virtual machine data should prioritize to the top.

Benefits of Storage Virtualization

- Now that we have seen what is storage virtualization and its types and also how do we implement them, now let us understand some of the benefits of going to storage virtualization:
- Our data does not get compromised easily even if the host fails as we store our data in a different and convenient place.
- It is easy for us to protect, provide and use our data as we implement some level of abstraction in our storage
- Additional functions such as recovery, duplication, replication, etc. can be done with ease.

ii. Network virtualization:-

- **Network Virtualization** (NV) refers to abstracting network resources that were traditionally delivered in hardware to software. NV can combine multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.
- Network virtualization software allows network administrators to move virtual machines across different domains without reconfiguring the network. The software creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.



Why network virtualization?

- Network virtualization is rewriting the rules for the way services are delivered, from the software-defined data center (SDDC), to the cloud, to the edge.
- This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized. Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications.
- With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or updated in minutes for rapid time to value.

How does network virtualization work?

- Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network.
- It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane.
- Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.
- Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application.
- When a workload is moved to another host, network services and security policies move with it. And when new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Benefits of network virtualization

Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:

- Reduce network provisioning time from weeks to minutes
- Achieve greater operational efficiency by automating manual processes
- Place and move workloads independently of physical topology
- Improve network security within the data center

Network Virtualization Example

- One example of network virtualization is virtual LAN (VLAN). A VLAN is a subsection of a local area network (LAN) created with software that combines network devices into one group, regardless of physical location. VLANs can improve the speed and performance of busy networks and simplify changes or additions to the network.
- Another example is network overlays. There are various overlay technologies. One industry-standard technology is called virtual extensible local area network (VXLAN). VXLAN provides a framework for overlaying virtualized layer 2 networks over layer 3 networks, defining both an encapsulation mechanism and a control plane. Another is generic network virtualization encapsulation (GENEVE), which takes the same concepts but makes them more extensible by being flexible to multiple control plane mechanisms.
- VMware NSX Data Center – Network Virtualization Platform
  VMware NSX Data Center is a network virtualization platform that delivers networking and security components like firewalling, switching, and routing that are defined and consumed in software. NSX takes an architectural approach built on scale-out network virtualization that delivers consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.

iii. **Desktop virtualization:-**

- Desktop virtualization is a technology that allows the creation and storage of multiple user desktop instances on a single host, residing in a data center or the cloud.

- It is achieved by using a hypervisor, which resides on top of the host server hardware to manage and allow virtual desktops to utilize the computing power of the underlying server hardware.
- The hypervisor creates VMs that simulate the user's desktop environments, which can hold different operating systems, applications, personalized settings, and user data. Users can remotely access as well as operate these desktops from any endpoint device.

Types of Desktop Virtualization

Desktop virtualization has two major deployment models: Hosted Desktop and Client Virtualization.

i. Hosted Desktop Virtualization

- Under this model, a server, which resides in a data center, hosts the virtual machines.
- Users can connect to the server through standard protocols such as Remote Desktop Protocol (RDP) or connection brokers. There are three major variants under Hosted Desktop Virtualization:

a. Virtual Desktop Infrastructure (VDI)

- In VDI, the OS runs VMs—which contains the desktop image—on a server within the datacenter.
- VDI technology leverages a hypervisor to split a server into different desktop images that users can remotely access via their end-devices.
- VDI provisions a dedicated VM running its own OS to each user within the virtualized environment.

b. Remote Desktop Services (RDS)

- RDS—also called Remote Desktop Session Host(RDSH), and formerly Terminal Services—allows users to remotely access shared desktops and Windows applications on Microsoft Windows Server OS.
- In RDS, users access remote desktops by sharing the hardware, OS (in this case, a Windows Server), apps, and host resources.

c. Desktop-as-a-Service (DaaS)

- DaaS's functionality is similar to that of VDI: users access their desktops and apps from any end-device or platform.
- However, in VDI, you have to purchase, deploy, and manage all the hardware components yourself.
- In DaaS, though, you outsource desktop virtualization to the third party to help you develop and operate virtual desktops.

ii. Client Virtualization

- In Client virtualization, you install a hypervisor on a client device to allow you to run multiple OSes.

- Client virtualization eliminates the need for users to have their own dedicated hardware and software. Client virtualization deployment has two variants:

a. **Presentation virtualization**

Presentation virtualization provides a web-based portal through which users leverage to interact with published desktops and apps. Organizations can use this approach to deliver apps or desktops from a shared server.

b. **Application virtualization**

Application virtualization allows apps to run on other platforms. For example, you can run Windows apps on Linux. You can use Application virtualization to simplify OS migration by creating portable software. You can then transfer applications between computers without having to install them.

Benefits

Depending on the deployment model you choose, virtualized desktops offer many benefits. However, six prominent ones stand out:

- **Simplified administration**. Desktop virtualization enables IT admins to manage a server from a centralized location, allowing for quicker deployments and simplified maintenance. This saves IT resources and time for an organization.
- **Secure and mobile access to apps**. Organizations can use virtualized desktops to provide their remote employees high-throughput apps by enabling GPU sharing via a secure connection from any end-device or platform.
- **Enhanced employee productivity**. Employees can securely access their corporate virtual desktops from any end-device, location, and at any time. Desktop virtualization is a perfect fit for telework because employees access specialized apps and functionalities on-the-go as opposed to typical mobile computing technologies.
- **Reduced downtimes and accelerated deployments**. With virtualized desktops, users can easily be migrated to other VMs in case there is a hardware failure. As such, there’s no lost time and productivity. Similarly, IT admins can quickly deploy new hardware within a centralized infrastructure—getting new employees on board and up to speed.
- **Reduced IT costs**. Desktop virtualization allows organizations to shift their IT budgets from the capital to operating expenditures. By delivering computationally-intensive apps on VMs that are hosted on a data center, organizations can extend the shelf life of older PCs or even less powerful machines. Besides, you also save on software licensing requirements because you only need to install apps on a single, centralized server as opposed to individual workstations.
- **Enhanced user experience**. Desktop virtualization can provide feature-rich experience without sacrificing the hardware on which apps run on. For example, users can still access USB ports or printing services on their end-devices.

iv. **Application virtualization**

- Application virtualization or app virtualization is technology that allows users to access and use an application from a separate computer than the one on which the application is installed.
- Using application virtualization software, IT admins can set up remote applications on a server then deliver the apps to an end user’s computer.

- For the user, the experience of the virtualized app is the same as using the installed app on a physical machine.

How does application virtualization work?

- The most common way to virtualize applications is the server-based approach. This means an IT administrator implements remote applications on a server inside an organization's data center or via a hosting service.
- The IT admin then uses application virtualization software to deliver the applications to a user's desktop or other connected device.
- The user can now access and use the application as though it were locally installed on their machine, and the user's actions are conveyed back to the server to be executed.

What are the top three benefits of application virtualization?

1. **App Management:**
   Application virtualization makes it much easier for IT departments to manage and maintain applications across an organization. Rather than manually installing applications to every users' machine, app virtualization lets IT admins install an app once on a central server and then deploy the app as needed on user devices. Besides saving installation time, this also makes it simpler to update or patch applications because IT only has to do so on a single server.
2. **Scalability:**
   Application virtualization lets IT admins deploy virtual applications to all kinds of connected devices, regardless of those devices' operating systems or storage space. This allows thin client provisioning in which users access an application on a low-cost machine while centralized servers handle all the computing power necessary to run that application. As a result, the organization spends much less on computing hardware because employees only require basic machines to access the apps they need for work. App virtualization also allows users to access applications that normally would not work on their machines' operating system, because the app is actually running on the centralized server. This is commonly used to virtually run a Windows application on a Linux operating system.
3. **Security:**
   Application virtualization software gives IT admins central control over which users can access which applications. If a user's app permissions within an organization change, the IT admin can simply remove that user's access to an application. Without app virtualization, the IT admin would have to physically uninstall the app from the user's device. This central control over app access is especially important if a user's devices are lost or stolen, because the IT admin can revoke remote access to sensitive data without having to track down the missing device.

4. PROS AND CONS OF VIRTUALIZATION:-

- Virtualization has now become extremely popular and widely used, especially in cloud computing.
- The primary reason for its wide success is the elimination of technology barriers that prevented virtualization from being an effective and viable solution in the past.
- The most relevant barrier has been performance.
- Today, the capillary diffusion of the Internet connection and the advancements in computing technology have made virtualization an interesting opportunity to deliver on-demand IT infrastructure and services.
- Despite its renewed popularity, this technology has benefits and also drawbacks.

Advantages of virtualization(pros):-

- Managed execution and isolation are perhaps the most important advantages of virtualization.
- In the case of techniques supporting the creation of virtualized execution environments, these two characteristics allow building secure and controllable computing environments.
- A virtual execution environment can be configured as a sandbox, thus preventing any harmful operation to cross the borders of the virtual host.
- Moreover, allocation of resources and their partitioning among different guests is simplified, being the virtual host controlled by a program.
- This enables fine-tuning of resources, which is very important in a server consolidation scenario and is also a requirement for effective quality of service.
- Portability is another advantage of virtualization, especially for execution virtualization techniques.
- Virtual machine instances are normally represented by one or more files that can be easily transported with respect to physical systems.
- they also tend to be self-contained since they do not have other dependencies besides the virtual machine manager for their use.
- Portability and self-containment simplify their administration.
- Portability and self-containment also contribute to reducing the costs of maintenance, since the number of hosts is expected to be lower than the number of virtual machine instances.

The other side of the cons: disadvantages:-

i. **Performance degradation:-**

- Performance is definitely one of the major concerns in using virtualization technology.
- Since virtualization interposes an abstraction layer between the guest and the host, the guest can experience increased latencies.
- For instance, in the case of hardware virtualization, where the intermediate emulates a bare machine on top of which an entire system can be installed, the causes of performance degradation can be traced back to the overhead introduced by the following activities:
  - Maintaining the status of virtual processors
  - Support of privileged instructions (trap and simulate privileged instructions)
  - Support of paging within VM
  - Console functions.
- when hardware virtualization is realized through a program that is installed or executed on top of the host operating systems, a major source of performance degradation is represented by the fact that the virtual machine manager is executed and scheduled together with other applications, thus sharing with them the resources of the host.

ii. **Inefficiency and degraded user experience:-**

- Virtualization can sometime lead to an inefficient use of the host. In particular, some of the specific features of the host cannot be exposed by the abstraction layer and then become inaccessible.
- In the case of hardware virtualization, this could happen for device drivers: The virtual machine can sometime simply provide a default graphic card that maps only a subset of the features available in the host.

- In the case of programming-level virtual machines, some of the features of the underlying operating systems may become inaccessible unless specific libraries are used.
- For example, in the first version of Java the support for graphic programming was very limited and the look and feel of applications was very poor compared to native applications.
- These issues have been resolved by providing a new framework called Swing for designing the user interface , and further improvements have beendonebyintegratingsupportfortheOpenGLlibrariesinthesoftwaredevelopmentkit.

iii. Security holes and new threats:-

- Virtualization opens the door to a new and unexpected form of phishing.
- The capability of emulating a host in a completely transparent manner led the way to malicious programs that are designed to extract sensitive information from the guest.
- In the case of hardware virtualization, malicious programs can preload themselves before the operating system and act as a thin virtual machine manager toward it.
- The operating system is then controlled and can be manipulated to extract sensitive information of interest to third parties.

5. VIRTUALIZATION USING KVM:-

KVM:-

i. Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux.
ii. Specifically, KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs).

How does KVM work?

- KVM converts Linux into a type-1 (bare-metal) hypervisor.
- All hypervisors need some operating system-level components—such as a memory manager, process scheduler, input/output (I/O) stack, device drivers, security manager, a network stack, and more—to run VMs.
- KVM has all these components because it’s part of the Linux kernel.
- Every VM is implemented as a regular Linux process, scheduled by the standard Linux scheduler, with dedicated virtual hardware like a network card, graphics adapter, CPU(s), memory, and disks.

KVM Feautres:-There are many useful features and advantages which you will gain when you use KVM to deploy your virtual platform. KVM hypervisor supports following features***:***

1. **Over-committing** : Which means allocating more virtualized CPUs or memory than the available resources on the system.
2. **Thin provisioning** : Which allows the allocation of flexible storage and optimizes the available space for every guest virtual machine.
3. **Disk I/O throttling** : Provides the ability to set a limit on disk I/O requests sent from virtual machines to the host machine.

4. **Automatic NUMA(non-uniform memory access) balancing** : Improves the performance of applications running on NUMA hardware systems.
5. **Virtual CPU hot add capability** : Provides the ability to increase processing power as needed on running virtual machines, without downtime.

KVM management tools:-There are two KVM management tools:

i. virsh
ii. virt-manager.

- From the command line, virsh can streamline KVM management. Because it's a master command with numerous subcommands, the learning curve is steep.
- Virt-manager, on the other hand, is a graphical user interface that simplifies the management of virtual machines in Red Hat Enterprise Linux.
- Virsh has a larger feature set, but virt-manager's point-and-click interface can perform most administrative tasks.

6. CLOUD COMPUTING OPEN CHALLENGES:-

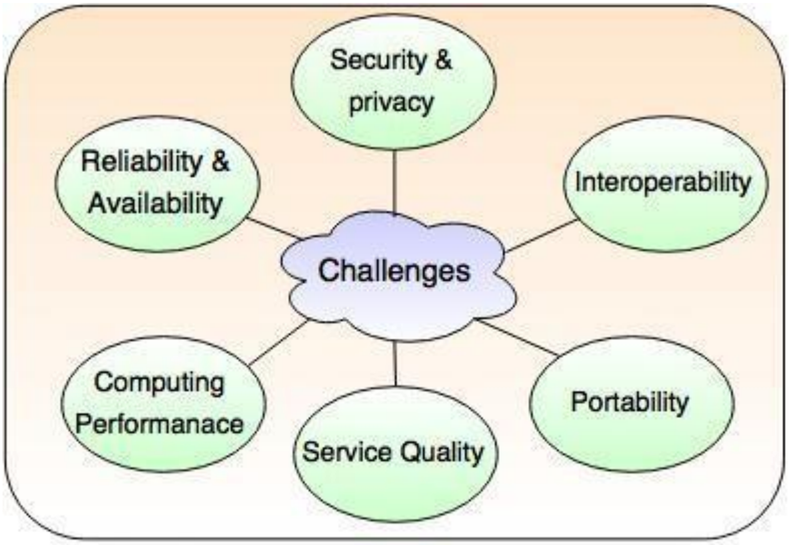


Fig. - Challenges in Cloud Computing

Security and Privacy

- Security and privacy are the main challenge in cloud computing.
- These challenges can reduced by using security applications, encrypted file systems, data loss software.

Interoperability

- The application on one platform should be able to incorporate services from the other platform. This is known as **Interoperability.**
- It is becoming possible through web services, but to develop such web services is complex.

Portability

- The applications running on one cloud platform can be moved to new cloud platform and it should operate correctly without making any changes in design, coding.
- The portability is not possible, because each of the cloud providers uses different standard languages for their platform.

Service Quality

- The Service-Level Agreements (SLAs) of the providers are not enough to guarantee the availability and scalability.
- The businesses disinclined to switch to cloud without a strong service quality guarantee.

Computing Performance

- High network bandwidth is needed for data intensive applications on cloud, this results in high cost.
- In cloud computing, low bandwidth does not meet the desired computing performance.

Reliability and Availability

- Most of the businesses are dependent on services provided by third-party, hence it is mandatory for the cloud systems to be reliable and robust.

7. CLOUD COMPUTING AND VIRTUALIZATION/CLOUD VS VIRTUALIZATION:-

- Cloud infrastructure cannot be established without the help of virtualization. It is the foundation of cloud networks.
- In IT infrastructure, cloud computing and virtualization are used together to build a cloud infrastructure.
- Virtualization separates the hardware from physical machine to create multiple virtual machines on the same server while cloud gets build using multiple virtual infrastructures which combines the multiple virtualize applications/software/servers to create one instance for each application or software or server for users.
- Google Docs is the best example of cloud computing

Key Points	**Cloud Computing**	**Virtualization**
Scalability	Cloud can be extended as much as you want.	Virtual machine configuration limits its scalability.
Quick setup	Setting up the cloud is a very tedious task.	It is very simple to set up a virtual environment.
Flexibility	It is very flexible for user access. A user can access its cloud from any location with internet (depending upon permission).	Proper authentication is required before accessing the virtual machines.
Service Type	IaaS	SaaS
Dedicated hardware	Multiple hardware creates a cloud computing	Dedicated hardware required for multiple virtual machines
Integration	Cloud integration allows future expansion of Users,	Virtualization integration allows the expansion of new

	applications, etc.	machines within the same infrastructure.
Dependency	Multiple users can access the network using the same link.	Multiple OS can be installed on a single server/computer
Accessibility	It can be accessed from all over the world. (Internet-based cloud)	Proper permissions are required for accessing from outside the network.
Disaster Recovery	Not depend upon one machine.	Single machine failure can bring done multiple virtual machines.
Types	Private Cloud and Public Cloud	Hardware virtualization and Application virtualization.