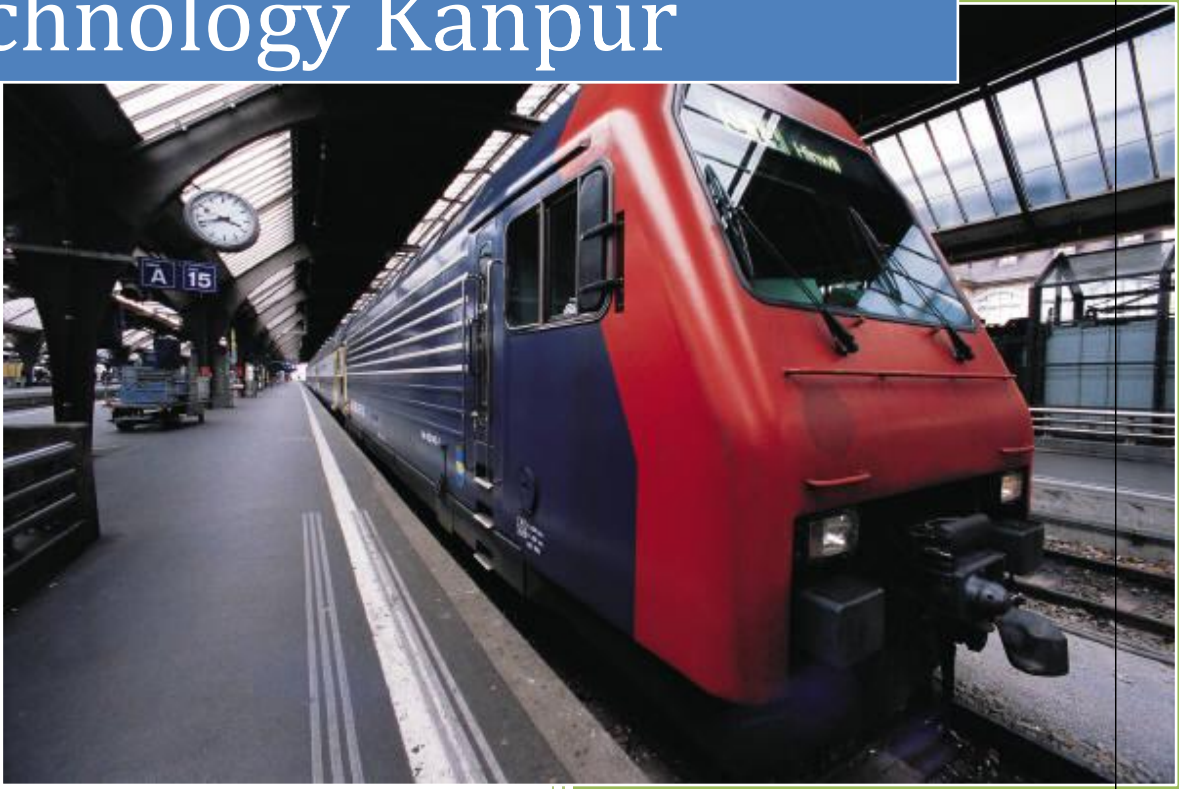
Cloud Computing, KOE081

2023

Vision Institute Of Technology Kanpur



By Kaptan Yadav

HOD, Electrical & Electronics Engineering

2/6/2023

KOE081: CLOUD COMPUTING

Unit-1

Introduction: Cloud Computing – Definition of Cloud – Evolution of Cloud Computing – Underlying Principles of Parallel and Distributed, History of Cloud Computing - Cloud Architecture **- Types of Clouds** - Business models around Clouds – Major Players in Cloud Computing, issues in Clouds - Eucalyptus - Nimbus - Open Nebula, CloudSim.

Unit-2

Types of Cloud services: Software as a Service, Platform as a Service –Infrastructure as a Service - Database as a Service - Monitoring as a Service –Communication as services. Service
providers- Google, Amazon, Microsoft Azure, IBM, Sales force.

Unit-3

Collaborating Using Cloud Services:
Email Communication over the Cloud - CRM Management – Project Management-Event Management - Task Management – Calendar - Schedules - Word Processing – Presentation – Spreadsheet - Databases – Desktop - Social Networks and Groupware.

Unit-4

Virtualization for Cloud: Need for Virtualization – Pros and cons of Virtualization – Types of Virtualization –System VM, Process VM, Virtual Machine monitor – Virtual machine properties - Interpretation
and binary translation, HLL VM - supervisors – Xen, KVM, VMware,Virtual Box, Hyper-V.

Unit-5

Security, Standards and Applications:
Security in Clouds: Cloud security challenges – Software as a Service Security, Common Standards: The Open Cloud Consortium – The Distributed management Task Force – Standards for application Developers – Standards for Messaging – Standards for Security, End user access to cloud computing, Mobile Internet devices and the cloud.
Hadoop – MapReduce – Virtual Box — Google App Engine – Programming Environment for Google App Engine

Unit-4th

Virtualization in Cloud Computing

Virtualization is the "creation of a virtual (rather than actual) , such as a server, a desktop, a storage device, an operating system or network resources".

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.

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.**

Pointer: A pointer points to a memory location where data is stored, rather than containing the data itself.

Types of Virtualization:

1) **Hardware Virtualization:** When the virtual machine software or virtual machine manager (VMM) is directly installed on the hardware system is known as hardware virtualization. The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources. After virtualization of hardware system we can install different operating system on it and run different applications on those OS.
   Usage: Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.
2) **Operating System Virtualization:** When the virtual machine software or virtual machine manager (VMM) is installed on the Host operating system instead of directly on the hardware system is known as operating system virtualization.
   Usage: Operating System Virtualization is mainly used for testing the applications on different platforms of OS.
3) **Server Virtualization**: When the virtual machine software or virtual machine manager (VMM) is directly installed on the Server system is known as server virtualization.
   Usage: Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.
4) **Storage Virtualization:** Storage virtualization is the process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device. Storage virtualization is also implemented by using software applications.
   Usage: Storage virtualization is mainly done for back-up and recovery purposes.

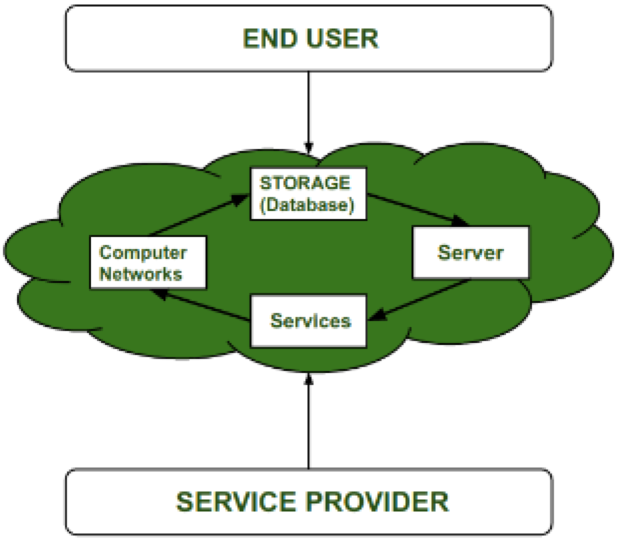
What is a hypervisor :

A hypervisor, also known as a virtual machine monitor or VMM. The hypervisor is a piece of software that allows us to build and run virtual machines which are abbreviated as VMs.

A hypervisor allows a single host computer to support multiple virtual machines (VMs) by sharing resources including memory and processing.

Why Virtualization in Cloud Computing ?

Virtualization is very important concept in cloud computing. In cloud computing, a cloud vendor who will provide cloud services have all physical resources like server, storage device, network device etc. and these physical services are rented by cloud vendors so that user’s will not worry about these physical services.



But it is very costly to provide physical services per customer on rent because firstly it becomes very costly and also user's will not use the fully services. So this problem can be solved by Virtualization. It is very cool approach for not only efficient use of Physical services but also reduce costs of vendors. Thus cloud vendor's can vitalize their single big server and provide smaller spec server to multiple customer's

Pros of Virtualization in Cloud Computing :

Utilization of Hardware Efficiently –

With the help of Virtualization Hardware is Efficiently used by user as well as Cloud Service Provider. In this the need of Physical Hardware System for the User is decreases and this results in less costly.In Service Provider point of View, they will vitalize the Hardware using Hardware Virtualization which decrease the Hardware requirement from Vendor side which are provided to User is decreased. Before Virtualization, Companies and organizations have to set up their own Server which require extra space for placing them, engineer's to check its performance and require extra hardware cost but with the help of Virtualization the all these limitations are removed by Cloud vendor's who provide Physical Services without setting up any Physical Hardware system.

Availability increases with Virtualization –

One of the main benefit of Virtualization is that it provides advance features which allow virtual instances to be available all the times. It also has capability to move virtual instance from one virtual Server another Server which is very tedious and risky task in Server Based System. During migration of Data from one server to another it ensures its safety. Also, we can access information from any location and any time from any device.

Disaster Recovery is efficient and easy –

With the help of virtualization Data Recovery, Backup, Duplication becomes very easy. In traditional method , if somehow due to some disaster if Server system Damaged then the surety of Data Recovery is very less. But with the tools of Virtualization real time data backup recovery and mirroring become easy task and provide surety of zero percent data loss.

Virtualization saves Energy –

Virtualization will help to save Energy because while moving from physical Servers to Virtual Server's, the number of Server's decreases due to this monthly power and cooling cost decreases which will Save Money as well. As cooling cost reduces it means carbon production by devices also decreases which results in Fresh and pollution free environment.

Quick and Easy Set up –

In traditional methods Setting up physical system and servers are very time-consuming. Firstly Purchase them in bulk after that wait for shipment. When Shipment is done then wait for Setting up and after that again spend time in installing required software etc. Which will consume very time. But with the help of virtualization the entire process is done in very less time which results in productive setup.

Cloud Migration becomes easy –

Most of the companies those who already have spent a lot in the server have a doubt of Shifting to Cloud. But it is more cost-effective to shift to cloud services because all the data that is present in their server's can be easily migrated into the cloud server and save something from maintenance charge, power consumption, cooling cost, cost to Server Maintenance Engineer etc.

Cons of Virtualization :

Data can be at Risk –

Working on virtual instances on shared resources means that our data is hosted on third party resource which put's our data in vulnerable condition. Any hacker can attack on our data or try to perform unauthorized access. Without Security solution our data is in threaten situation.

Learning New Infrastructure –

As Organization shifted from Servers to Cloud. They required skilled staff who can work with cloud easily. Either they hire new IT staff with relevant skill or provide training on that skill which increase the cost of company.

High Initial Investment –

It is true that Virtualization will reduce the cost of companies but also it is truth that Cloud have high initial investment. It provides numerous services which are not required and when unskilled organization will try to set up in cloud they purchase unnecessary services which are not even required to them.

Characteristic of Virtualization

Increased Security: The ability to control the execution of a guest program 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.

Managed Execution: In particular, sharing, aggregation, emulation, and isolation are the most relevant features.

Sharing: Virtualization allows the creation of a separate computing environment within the same host.

Aggregation: It is possible to share physical resources among several guests, but virtualization also allows aggregation, which is the opposite process.

What is a virtual machine :

A Virtual Machine (VM) is a compute resource that uses software instead of a physical computer to run programs and deploy apps. One or more virtual "guest" machines run on a physical "host" machine. Each virtual machine runs its own operating

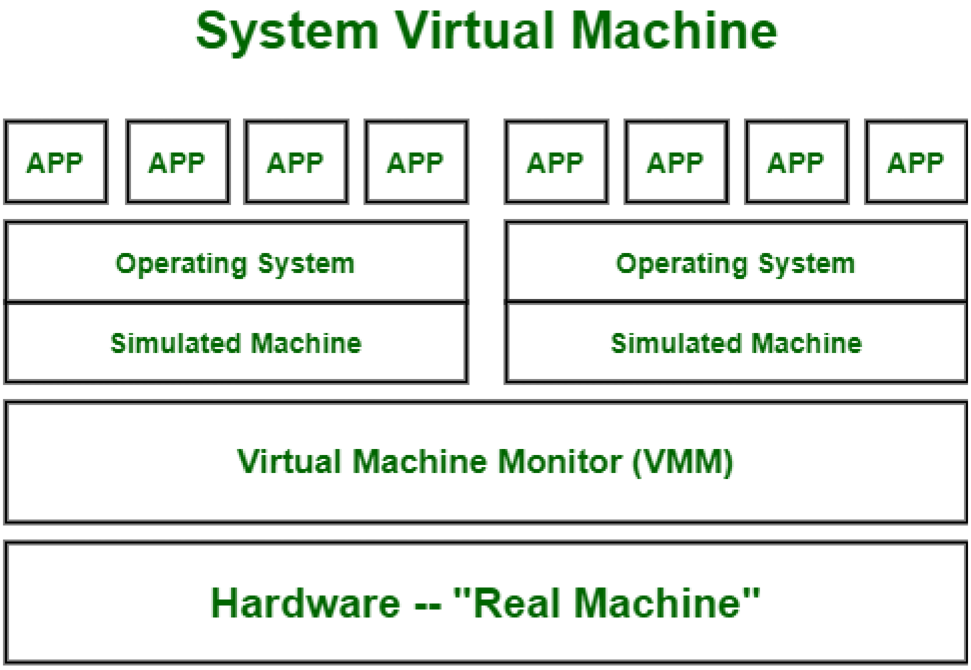
Advantages of virtual machines

Virtual machines are easy to manage and maintain, and they offer several advantages over physical machines:

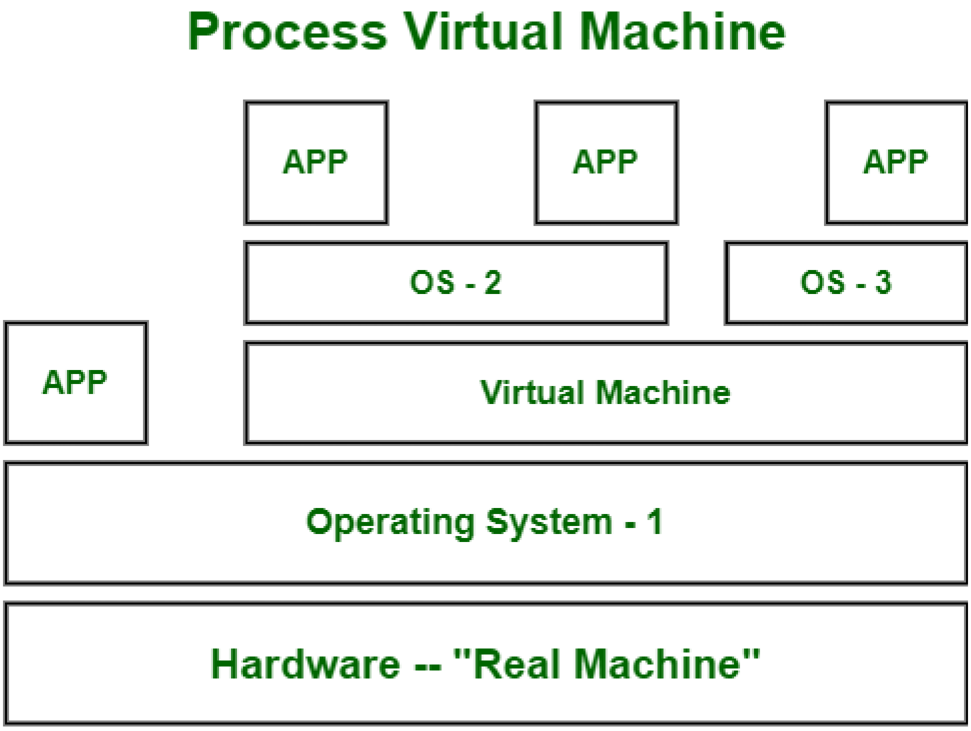
- VMs can run multiple operating system environments on a single physical computer, saving physical space, time and management costs.
- Virtual machines support legacy applications, reducing the cost of migrating to a new operating system. For example, a Linux virtual machine running a distribution of Linux as the guest operating system can exist on a host server that is running a non-Linux operating system, such as Windows.
- VMs can also provide integrated disaster recovery and application provisioning options.

Types of virtual machines

1. **System Virtual Machine :** These types of virtual machines gives us complete system platform and gives the execution of the complete virtual operating system. Just like virtual box, system virtual machine is providing an environment for an OS to be installed completely. We can see in below image that our hardware of Real Machine is being distributed between two simulated operating systems by Virtual machine monitor. And then some programs, processes are going on in that distributed hardware of simulated machines separately.



2. **Process Virtual Machine :** While process virtual machines, unlike system virtual machine, does not provide us with the facility to install the virtual operating system completely. Rather it creates virtual environment of that OS while using some app or program and this environment will be destroyed as soon as we exit from that app. Like in below image, there are some apps running on main OS as well some virtual machines are created to run other apps. This shows that as those programs required different OS, process virtual machine provided them with that for the time being those programs are running. Example – Wine software in Linux helps to run Windows applications.



3. **HLL VM (High Level Language Virtual Machine):** HLL VM stands for High Level Language Virtual Machine, and it is a type of virtual machine that is used in cloud computing to run high-level programming languages, such as Java, Python, and Ruby, among others. HLL VMs, such as the Java Virtual Machine (JVM), are designed to run high- level programming languages that are compiled into bytecode. The HLL VM translates the bytecode into machine language that can be executed by the underlying hardware. This provides a layer of abstraction between the high-level programming language and the hardware, which makes it easier to write and deploy applications.

Cloud Security : Cloud security refers to the set of policies, technologies, and controls that are implemented to protect data, applications, and infrastructure in cloud computing environments. Cloud security aims to ensure the confidentiality, integrity, and availability of information stored or processed in the cloud, as well as to protect against threats such as data breaches, unauthorized access, and other types of cyber attacks.

Cloud security involves a range of measures, including access controls, encryption, network security, data protection, identity and access management, and vulnerability management. These measures are implemented by cloud service providers and cloud users to protect their data and applications from various types of cyber threats.

Cloud security is essential for businesses and organizations that rely on cloud computing to store and process their sensitive data. A breach of cloud security can result in significant financial losses, damage to a company's reputation, and legal consequences. Therefore, it is crucial to implement robust cloud security measures to protect against cyber threats and ensure the security of cloud-based operations.

Cloud Security Challenges

Cloud security challenges refer to the difficulties and risks associated with protecting data, applications, and infrastructure in cloud computing environments.
In simpler terms, cloud security challenges are the obstacles and problems that arise when trying to keep data and applications secure in the cloud. Some of the common challenges include:

1. Data breaches: Unauthorized access to data can lead to data theft, loss of intellectual property, and damage to the company's reputation.
2. Compliance and regulatory issues: Companies must comply with various regulations, such as HIPAA, GDPR, and PCI DSS, which require them to maintain strict security and privacy standards.
3. Lack of control: Cloud users may not have full control over the security of their data and applications, as they are hosted and managed by third-party providers.
4. Vulnerability to cyber attacks: Cloud environments are susceptible to cyber attacks, such as malware, phishing, and ransomware.
5. Shared security responsibility: Cloud security is a shared responsibility between cloud providers and cloud users, and it can be challenging to determine who is responsible for what.

To address these challenges, it is essential to implement robust security measures, such as encryption, access controls, and intrusion detection and prevention systems. Companies should also regularly assess their cloud security posture and stay up-to-date with the latest security threats and best practices.

Software as a Service Security : SaaS (Software as a Service) security refers to the measures and processes implemented to protect the data and applications hosted by a SaaS provider. This typically includes measures such as encryption, authentication, access controls, network security, and data backup and recovery.

Challenges in SaaS security
Some of the most significant challenges in SaaS security include:

1. Lack of Control
SaaS providers typically host applications and data in the cloud, meaning that customers have less direct control over their security. This can make it challenging for customers to monitor and manage security effectively.

2. Access Management
SaaS applications typically require users to log in and authenticate their identity. However, managing user access can be challenging, particularly if the provider is hosting applications for multiple customers with different access requirements.

3. Data Privacy
SaaS providers may be subject to data privacy regulations, which can vary by jurisdiction. This can make it challenging to ensure compliance with all relevant laws and regulations, particularly if the provider hosts data for customers in multiple countries.

4. Third-party integration
SaaS providers may integrate with third-party applications, such as payment processors or marketing platforms. However, this can increase the risk of security incidents, as vulnerabilities in third-party software can potentially affect the entire system.

5. Continuous monitoring
SaaS providers must continuously monitor their systems for security threats and vulnerabilities. This requires a high level of expertise and resources to detect and respond to security incidents effectively.