Experiment No:01

Aim: Virtualization Usecase Study

Cloud Computing:

Cloud computing is a general term for the delivery of hosted computing services and IT resources over the internet with pay-as-you-go pricing. Users can obtain technology services such as processing power, storage and databases from a cloud provider, eliminating the need for purchasing, operating and maintaining on-premises physical data centers and servers.

A cloud can be private, public or a hybrid. A public cloud sells services to anyone on the internet. A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people, with certain access and permissions settings. A hybrid cloud offers a mixed computing environment where data and resources can be shared between both public and private clouds. Regardless of the type, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Cloud infrastructure involves the hardware and software components required for the proper deployment of a cloud computing model. Cloud computing can also be thought of as utility computing or on-demand computing.

Cloud computing relies heavily on virtualization and automation technologies. Virtualization lets IT organizations create virtual instances of servers, storage and other resources that let multiple VMs or cloud environments run on a single physical server using software known as a hypervisor. This simplifies the abstraction and provisioning of cloud resources into logical entities, letting users easily request and use these resources. Automation and accompanying orchestration capabilities provide users with a high degree of self-service to provision resources, connect services and deploy workloads without direct intervention from the cloud provider's IT staff

Types of service models:

1. Infrastructure as a service (IaaS). IaaS providers, such as Amazon Web Services (AWS), supply a virtual server instance and storage, as well as application programming interfaces (APIs) that let users migrate workloads to a virtual machine (VM). Users have an allocated storage capacity and can start, stop, access and configure the VM and storage as desired. IaaS providers offer small, medium, large, extra-large and memory- or compute-optimized instances, in addition to enabling customization of instances for various workload needs. The IaaS cloud model is closest to a remote data center for business users.
2. Platform as a service (PaaS). In the PaaS model, cloud providers host development tools on their infrastructures. Users access these tools over the internet using APIs, web portals or gateway software. PaaS is used for general software development and many PaaS providers host the software after it's developed. Examples of PaaS products include Salesforce Lightning, AWS Elastic Beanstalk and Google App Engine.
3. Software as a service (SaaS). SaaS is a distribution model that delivers software applications over the internet; these applications are often called *web services*. Users can access SaaS applications and services from any location using a computer or mobile device that has internet access. In the SaaS model, users gain access to application software and databases. An example of a SaaS application is Microsoft 365 for productivity and email services.
4. Function as a service (FaaS). FaaS, also known as *serverless computing*, lets users run code in the cloud without having to worry about the underlying infrastructure. Users can create and deploy functions that respond to events or triggers. FaaS abstracts server and infrastructure management, letting developers concentrate solely on code creation.

Deployment Model types:

Private cloud

A business's data center delivers private cloud services to internal users. With a private cloud, an organization builds and maintains its own underlying cloud infrastructure. This model offers the versatility and convenience of the cloud, while preserving the management, control and security common to local data centers. Internal users might be billed for services through IT chargeback. Examples of private cloud technologies and vendors include VMware and OpenStack.

Public cloud

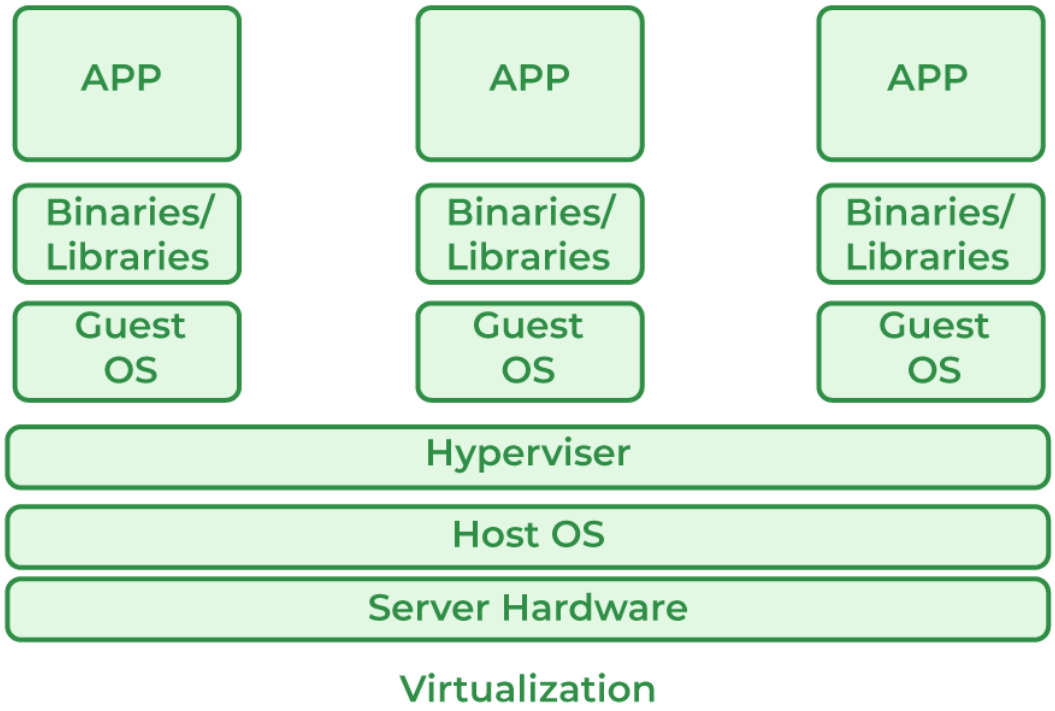
In the public cloud model, a third-party cloud service provider (CSP) delivers the cloud service over the internet. Public cloud services are sold on demand, typically by the minute or hour, though long-term commitments are available for many services. Customers only pay for the central processing unit cycles, storage or bandwidth they consume. Examples of public CSPs include AWS, Google Cloud Platform (GCP), IBM, Microsoft Azure, Oracle and Tencent Cloud.

Hybrid cloud

A hybrid cloud is a combination of public cloud services and an on-premises private cloud, with orchestration and automation between the two. Companies can run mission-critical workloads or sensitive applications on the private cloud and use the public cloud to handle workload bursts or spikes in demand. The goal of a hybrid cloud is to create a unified, automated, scalable environment that takes advantage of all that a public cloud infrastructure can provide, while still maintaining control over mission-critical data.

Virtualization in Cloud Computing:

In cloud computing, Virtualization facilitates the creation of virtual machines and ensures the smooth functioning of multiple operating systems. It also helps create a virtual ecosystem for server operating systems and multiple storage devices, and it runs multiple operating systems.Cloud Computing is identified as an application or service that involves a virtual ecosystem. Such an ecosystem could be of public or private nature. With Virtualization, the need to have a physical infrastructure is reduced. The terms Cloud Computing and Virtualization are now being used interchangeably, and they are being unified quickly.Virtualization and Cloud Computing work hand in hand to ensure that you will get advanced and sophisticated levels of computing. It ensures that applications can be shared across multiple network threads of different enterprise and active users.Cloud Computing delivers scalability, efficiency, and economic value. It offers streamlined workload management systems.In simpler words, Cloud Computing in collaboration with Virtualization ensures that the modern-day enterprise gets a more cost-efficient way to run multiple operating systems using one dedicated resource.



Characteristics of Virtualization

Distribution of resources: Virtualization and Cloud Computing technology ensure end-users develop a unique computing environment. It is achieved through the creation of one host machine. Through this host machine, the end-user can restrict the number of active users. By doing so, it facilitates easy of control. They can also be used to bring down power consumption.

Accessibility of server resources: Virtualization delivers several unique features that ensure no need for physical servers. Such features ensure a boost to uptime, and there is less fault tolerance and availability of resources.

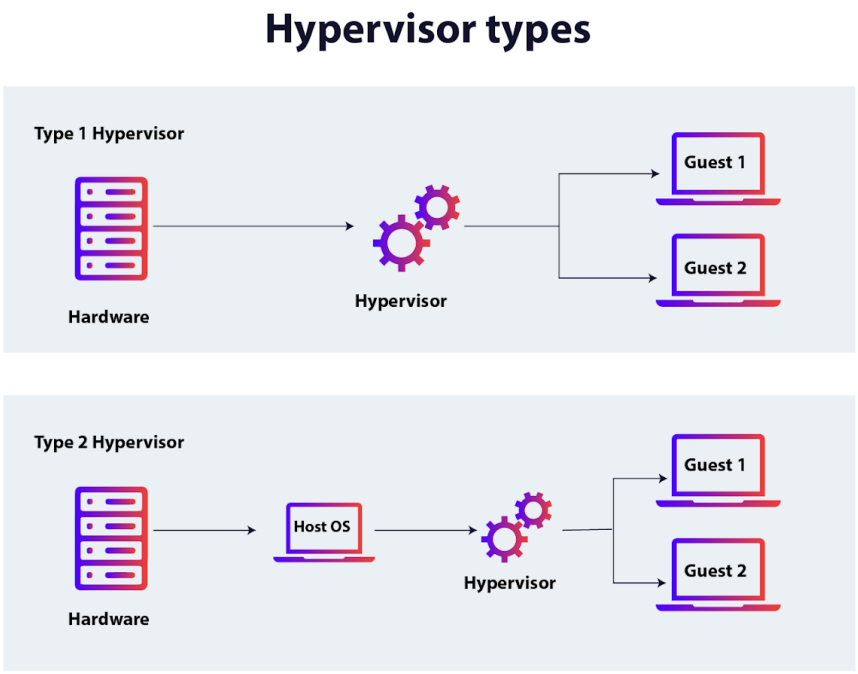
Resource Isolation: Virtualization provides isolated virtual machines. Each virtual machine can have many guest users, and guest users could be either operating systems, devices, or applications.The virtual machine provides such guest users with an isolated virtual environment. This ensures that the sensitive information remains protected, and, at the same time, guest users remain inter-connected with one another.

Security and authenticity: The virtualization systems ensure continuous uptime of systems, and it does automatic load balancing and ensures there is less disruption of services.

Aggregation: Aggregation in Virtualization is achieved through cluster management software. This software ensures that the homogenous sets of computers or networks are connected and act as one unified resource.

Hypervisor:

A hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware. The program which provides partitioning, isolation, or abstraction is called a virtualization hypervisor. The 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).



Types of Hypervisor –

TYPE-1 Hypervisor:

The hypervisor runs directly on the underlying host system. It is also known as a “Native Hypervisor” or “Bare metal hypervisor”. It does not require any base server operating

system. It has direct access to hardware resources. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer, and Microsoft Hyper-V hypervisor.

Pros & Cons of Type-1 Hypervisor:

Pros: Such kinds of hypervisors are very efficient because they have direct access to the physical hardware resources(like Cpu, Memory, Network, and Physical storage). This causes the empowerment of the security because there is nothing any kind of the third party resource so that attacker couldn't compromise with anything.

Cons: One problem with Type-1 hypervisors is that they usually need a dedicated separate machine to perform their operation and to instruct different VMs and control the host hardware resources.

TYPE-2 Hypervisor:

A Host operating system runs on the underlying host system. It is also known as 'Hosted Hypervisor". Such kind of hypervisors doesn't run directly over the underlying hardware rather they run as an application in a Host system(physical machine). Basically, the software is installed on an operating system. Hypervisor asks the operating system to make hardware calls. An example of a Type 2 hypervisor includes VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs. The type-2 hypervisor is very useful for engineers, and security analysts (for checking malware, or malicious source code and newly developed applications).

Pros & Cons of Type-2 Hypervisor:

Pros: Such kind of hypervisors allows quick and easy access to a guest Operating System alongside the host machine running. These hypervisors usually come with additional useful features for guest machines. Such tools enhance the coordination between the host machine and the guest machine.

Cons: Here there is no direct access to the physical hardware resources so the efficiency of these hypervisors lags in performance as compared to the type-1 hypervisors, and potential security risks are also there an attacker can compromise the security weakness if there is access to the host operating system so he can also access the guest operating system.