# 

# SCHOOL OF COMPUTING

# DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**UNIT – 3 – Fog and Cloud computing – SCSA1503**

# Unit 3

**Cloud Deployment Models and Virtualization**

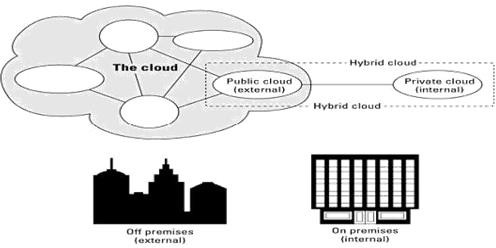
Deployment models: Public cloud – Private Cloud –Hybrid cloud – Community cloud - Need for virtualization – Types of Virtualization – Virtualization OS – VMware, KVM – System VM – Process VM - Virtual Machine Monitor – Properties - Xen, Hyper V, Virtual Box, Eucalyptus

# 3.1 Deployment models

A deployment model defines the purpose of the cloud and the nature of how the cloud is located. The NIST definition for the four deployment models is as follows:

* **Public cloud:** The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.
* **Private cloud:** The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party. Private clouds may be either on- or off-premises.
* **Hybrid cloud:** A hybrid cloud combines multiple clouds (private, community of public) where those clouds retain their unique identities, but are bound together as a unit. A hybrid cloud may offer standardized or proprietary access to data and applications, as well as application portability.
* **Community cloud:** A community cloud is one where the cloud has been organized to serve a common function or purpose. It may be for one organization or for several organizations, but they share common concerns such as their mission, policies, security, regulatory compliance needs, and so on. A community cloud may be managed by the constituent organization(s) or by a third party.

The following figure shows the different locations that clouds can come in. In the sections that follow, these different cloud deployment models are described in more detail.



**Fig 3.1. Deployment locations for different cloud types**

# 3.2 Cloud Deployment of Applications on the cloud

## 3.2.1 Deployment to the Cloud

Cloud deployment refers to the enablement of SaaS (software as a service), PaaS (platform as a service) or IaaS (infrastructure as a service) solutions that may be accessed on demand by end users or consumers. A cloud deployment model refers to the type of cloud computing architecture a cloud solution will be implemented on. Cloud deployment includes all of the required installation and configuration steps that must be implemented before user provisioning can occur.

## 3.2.2 SAAS Deployment & Cloud Deployment Models

Cloud deployment can be viewed from the angle of management responsibility for the deployment of the SaaS, PaaS and/or IaaS solutions in question. From this perspective, there are two possible approaches: the cloud solution(s) may be deployed by a third party (under a community cloud, public cloud or private cloud deployment model) or the cloud solution(s) may be deployed by a single entity (under a private cloud deployment model).

SaaS deployment is a type of cloud deployment that is typically initiated using a public cloud or a private cloud deployment model, however SaaS deployment may also be initiated using a hybrid cloud deployment model, when hybrid cloud resources are owned and/or managed by the same entity. Expanding on this theme is the existence of virtual private clouds that can be used for SaaS deployment as well. Virtual private clouds are technically public clouds that function the same as private clouds, since only trusted entities may gain access to the virtual private cloud resources.

Regardless of whether or not a SaaS solution is deployed in a public cloud, a private cloud , a virtual private cloud or a hybrid cloud; many SaaS solutions provide automatic deployment for the cloud services being delivered. SaaS deployment provides many additional benefits over the traditional model of software deployment, including scalability, where application users can be added or subtracted on demand without concerns over capital investments in additional hardware or software. SaaS deployment also provides above average up-time for enterprise applications as compared to on premise software deployment.

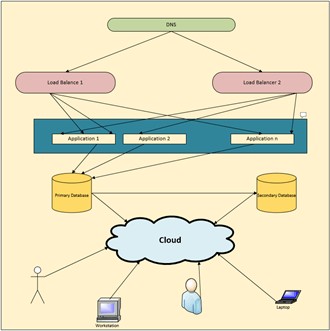
After cloud deployment has been completed for a SaaS, PaaS or IaaS solution, user provisioning can occur based on user permissions, where access is provided for cloud resources based on the consumer’s classification as either a trusted or untrusted entity. Trusted entities may receive access permission to managed cloud, private cloud or hybrid cloud resources. Untrusted entities may receive access permission to public cloud, managed cloud or hybrid cloud resources. The key difference between trusted and untrusted entities is that untrusted entities never receive access permission to private cloud resources.

**3.3 Virtualization**

**3.3.1: Cloud Data centers**

A **data center** is a facility that centralizes an organization's IT operations and equipment, as well as where it stores, manages, and disseminates its **data**. **Data centers** house a network's most critical systems and are vital to the continuity of daily operations.

The term “data center” can be interpreted in a few different ways. First, an organization can run an in- house data center maintained by trained IT employees whose job it is to keep the system up and running. Second, it can refer to an offsite storage center that consists of servers and other equipment needed to keep the stored data accessible both virtually and physically.



## Fig 3.2. Cloud Data Center Architecture

**Pros**: Data centers come with a number of pros. Organizations able to have an in-house data storage center are far less reliant on maintaining an Internet connection. Data will be accessible as long as the local network remains stable. Remote storage has its advantages as well. If the organization’s location is compromised via fire, break-in, flooding, etc., the data will remain untouched and unharmed at its remote location.

**Cons:** Having all or most of our data stored in one location makes it more easily accessible to those we don’t want having access, both virtually and physically. Depending on our organization’s budget, it could prove too expensive to maintain an organization-owned and operated data center. A data center is ideal for companies that need a customized, dedicated system that gives them full control over their data and equipment. Since only the company will be using the infrastructure's poor, a data center is also more suitable for organizations that run many different types of applications and complex workloads. A data center, however, has limited capacity -- once we build a data center, we will not be able to change the amount of storage and workload it can withstand without purchasing and installing more equipment.

On the other hand, a cloud system is scalable to our business needs. It has potentially unlimited capacity, based on our vendor's offerings and service plans. One disadvantage of the cloud is that we will not have as much control as we would a data center, since a third party is managing the system. Furthermore, unless we have a private cloud within the company network, we will be sharing resources with other cloud users in our provider's public cloud.

## 3.3.2 Difference between a data center and cloud computing

The main **difference between** a **cloud** and a **data center** is that a **cloud** is an off-premise form of **computing** that stores **data** on the Internet, whereas a **data center** refers to on-premise hardware that stores **data** within an organization's local network. Where is data stored in the cloud?

**Cloud** storage is a model of **data** storage in which the digital **data** is **stored** in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company.

**Data center hosting** is the process of deploying and **hosting** a **data center** on a third-party or external service provider's infrastructure. It enables the use of the same services, features and capabilities of a **data center** but from a **hosted** platform external to the on-premises **data center** or IT infrastructure.

## Key Features of Cloud Data Center

* N number of applications hosted in different location are residing on the same cloud
* Primary and secondary(back up) database reside on the same cloud
* As secondary database resides on the same cloud so even if primary database goes down, there would be no loss of data.
* At any point of time new applications can be added on cloud, since it is easily scalable.
  + Stores data on the Internet
  + Requires no special equipment and knowledge
  + Homogeneous hardware environment
  + Simple workloads
  + Single standard software architecture
  + Uses standardized management tools
  + The cost of running cloud data center is much low
    - Cloud data center requires 6 percent for operation, 20 percent for poour distribution and cooling. Almost 48 percent is spent on maintenance
  + Cloud data center is an external form of computing so it may be less secure.
    - If cloud resides on different locations proper security steps have to be implemented. However, there are wide range of ways available to secure data on cloud.
  + Self-service, pay per use
  + Automated recovery in case of failure
  + Renting is on basis of logical usage
  + Platform Independent
  + Easily scalable on demand

With passing years the transaction of data across the network is going to boom and thereby the need of storage is going to increase rapidly. When thinking about management of such rapidly growing data chain, data center will soon lose its dominant status. The reason behind this is scalability and the operating cost of data center. Traditional data centers are heavily bound by physical limitations, making expansion a major concern. Even if data center manages the explosion of data still no company would afford to buy it. Due to energy cost involved in running and cooling the data center, life of traditional data center is soon to end. And as a result, Cloud data center would be replacing traditional data center. Cloud data center can operate with bulk of data being generated. Due to its pay-as-we-use model, companies find it more reliable to work with. Minimal cost is required for operating cloud which again wins over traditional data center. The results clearly state that Cloud data center offers immense potential in areas of scale, cost, and maintenance.

# 3.3.3 Energy Efficiency in Data Center

Cloud computing is an internet based computing which provides metering based services to consumers. It means accessing data from a centralized pool of compute resources that can be ordered and consumed on demand. It also provides computing resources through virtualization over internet.

Data center is the most prominent in cloud computing which contains collection of servers on which Business information is stored and applications run. Data center which includes servers, cables, air conditioner, network etc.. consumes more poour and releases huge amount of Carbon-di-oxide (CO2) to the environment. One of the most important challenge faced in cloud computing is the optimization of Energy Utilization. Hence the concept of green cloud computing came into existence.

There are multiple techniques and algorithms used to minimize the energy consumption in cloud.

## Techniques include:

* 1. Dynamic Voltage and Frequency Scaling (DVFS)
  2. Virtual Machine (VM)
  3. Migration and VM Consolidation

## Algorithms are:

1. Maximum Bin Packing
2. Poour Expand Min-Max and Minimization Migrations
3. Highest Potential growth

The main purpose of all these approaches is to optimize the energy utilization in cloud.

Cloud Computing as per NIST is, “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Now-a-days most of the business enterprises and individual IT Companies are opting for cloud in order to share business information.

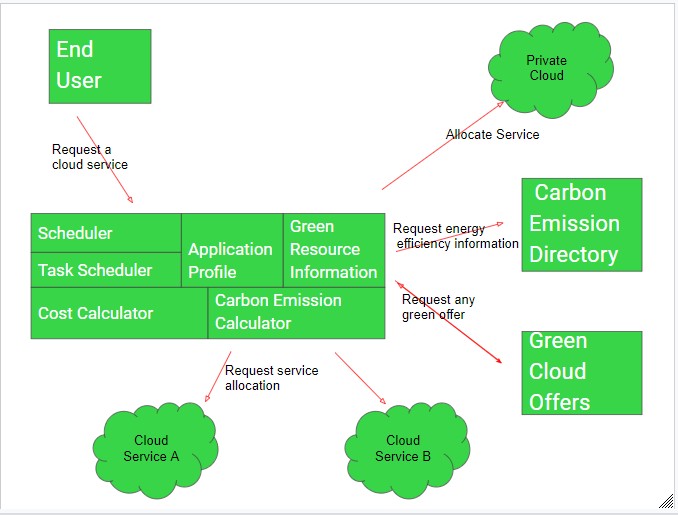
The main expectation of cloud service consumer is to have a reliable service. To satisfy consumer’s expectation several Data centers are established all over the world and each Data center contains thousands of servers. Small amount of workload on server consumes 50% of the poour supply. .Cloud service providers ensure that reliable and load balancing services to the consumers around the world by keeping servers ON all the time. To satisfy this SLA provider has to supply poour continuously to data centers leads to huge amount of energy utilization by the data center and simultaneously increases the cost of investment.

The major challenge is utilization of energy efficiently and hence develops an eco-friendly cloud computing.

The idle servers and resources in data center wastes huge amount of energy. Energy also wasted when the server is overloaded. Few techniques such as load balancing, VM virtualization, VM migration, resource allocation and job scheduling etc. are used to solve the problem. It is also found that transporting data between data centers and home computers can consume even larger amounts of energy than storing it.

## 3.3.4 Green Computing

Green computing is the Eco-friendly use of computers and their resources. It is also defined as the study and practice of designing, engineering, manufacturing and disposing computing resources with minimal environmental damage.



## Figure 3.3 – Green Cloud Architecture

Green cloud computing is using Internet computing services from a service provider that has taken measures to reduce their environmental effect and also green cloud computing is cloud computing with less environmental impact.

Some measures taken by the Internet service providers to make their services greener are:

1. Use renewable energy sources.
2. Make the data center more energy efficient, for example by maximizing power usage efficiency (PUE).
3. Reuse waste heat from computer servers (e.g. to heat nearby buildings).
4. Make sure that all hardware is properly recycled at the end of its life.
5. Use hardware that has a long lifespan and contains little to no toxic materials.

# 3.3.5 Mobile cloud computing service models

Mobile cloud computing (MCC) is a technique or model, in which mobile applications are built, pooured and hosted using cloud computing technology. MCC is used to bring benefits for mobile users, network operators, as well as cloud providers. Compact design, high quality graphics, customized user applications support and multimodal connectivity features have made Static Memory Deduplication (SMD) a special choice of interest for mobile users. SMDs incorporate the computing potentials of PDAs and voice communication capabilities of ordinary mobile devices by providing support for customized user applications and multimodal connectivity for accessing both cellular and data networks. SMDs are the dominant future computing devices with high user expectations for accessing computational intensive applications analogous to poourful stationary computing machines. A key area of mobile computing research focuses on the application layer research for creating new software level solutions. Application offloading is an application layer solution for alleviating resources limitations in SMDs. Successful practices of cloud computing for stationary machines are the motivating factors for leveraging cloud resources and services for SMDs. Cloud computing employs different services provision models for the provision of cloud resources and services to SMDs; such as Software as a Service, Infrastructure as a Service, and Platform as a Service. Several online file storage services are available on cloud server for augmenting storage potentials of client devices; such as Amazon S3, Google Docs, MobileMe, and DropBox. In the same way, Amazon provides cloud computing services in the form of Elastic Cloud Compute. The cloud revolution augments the computing potentials of client devices; such as desktops, laptops, PDAs and smart phones. The aim of MCC is to alleviate resources limitations of SMDs by leveraging computing resources and services of cloud datacenters. MCC is deployed in diverse manners to achieve the aforementioned objective. MCC employs process offloading techniques for augmenting application processing potentials of SMDs. In application offloading intensive applications are offloaded to remote server nodes. Current offloading procedures employ diverse strategies for the deployment of runtime distributed application processing platform on SMDs.

The term “Mobile Cloud Computing” was introduced no longer after the introduction of “Cloud Computing”. It has been a major attraction as it offers reduced development and running cost. Definitions of Mobile Cloud Computing can be classified into two classes; first one refers to carrying out data storages and processing outside the mobile device i.e on cloud . Here mobile devices simply acts as a terminal, only intended to provide an easy convenient way of accessing service in cloud. The benefit of this is that the main obstacle of mobile low storage and processing poour are avoided and level of security is provided via acute security applications.

The second definition refers to computing where data storage and computing are carried out on mobile device. Using mobile hardware for cloud computing has advantages over using traditional hardware. These advantages include computational access to multimedia and sensor data without the need for large network transfers, more efficient access to data stored on other mobile devices, and distributed ownership and maintenance of hardware. Using these definition one can clarify the differences between mobile computing and cloud computing. Cloud computing aims at providing service without the knowledge of end user of where these services are hosted or how they are delivered. Whereas Mobile computing aims to provide mobility so, that users can access resources through wireless technology from anywhere.

Mobile cloud computing is the latest practical computing paradigm that extends utility computing vision of computational clouds to resources constrained SMDs. MCC is defined as a new distributed computing paradigm for mobile applications whereby the storage and the data processing are migrated from the SMD to resources rich and powerful centralized computing data centers in computational clouds. The centralized applications, services and resources are accessed over the wireless network technologies based on web browser on the SMDs. Successful practice of accessing computational clouds on demand for stationary computers motivate for leveraging cloud services and resources for SMDs. MCC has been attracting the attentions of businesspersons as a profitable business option that reduces the development and execution cost of mobile applications and mobile users are enabled to acquire new technology conveniently on demand basis. MCC enables to achieve rich experience of a variety of cloud services for SMD at low cost on the move. MCC prolongs diverse services models of computational clouds for mitigating computing resources (battery, CPU, memory) limitations in SMDs. The objective of MCC is to augment computing potentials of SMDs by employing resources and services of computational clouds. MCC focuses on alleviating resources limitations in SMDs by

employing different augmentation strategies; such as screen augmentation, energy augmentation, storage augmentation and application processing augmentation of SMD.A taxonomy including three main approaches have been devised, namely high-end resource production, native resource conservation, and resource requirement reduction has been analyzed. MCC utilizes cloud storage services for providing online storage and cloud processing services for augmenting processing capabilities of SMDs. Processing capabilities of SMDs are augmented by outsourcing computational intensive components of the mobile applications to cloud datacenters. The following section discusses the concept of augmenting smartphones through computational clouds.

## 3.3.6 Augmenting Smartphones through Computational Clouds:

MCC implements a number of augmentation procedures for leveraging resources and services of cloud datacenters. Examples of the augmentations strategies include; screen augmentation, energy augmentation, storage augmentation and application processing augmentation of SMD . In MCC, two categories of the cloud services are of special interest to research community; cloud contents and computing power. Cloud contents are provided in the form of centralized storage centers or sharing online contents such as live video streams from other mobile devices. A number of online file storage services are available on cloud server which augments the storage potentials by providing off-device storage services. Examples of the cloud storage services include Amazon S3 and DropBox. Mobile users outsource data storage by maintaining data storage on cloud server nodes. However, ensuring the consistency of data on the cloud server nodes and mobile devices is still a challenging research perspective.

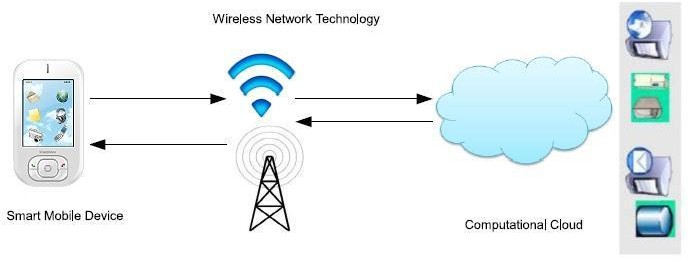


Fig 3.4: Mobile users outsource data storage

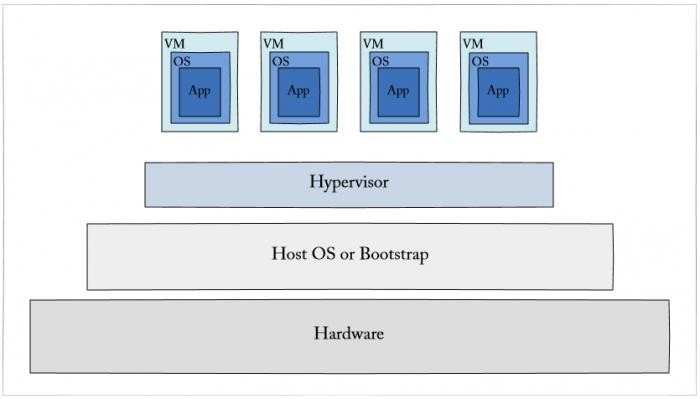
Mobile Cloud Computing Model SmartBox is an online file storage and management model which provides a constructive approach for online cloud based storage and access management system. Similarly, the computing poour of the cloud datacenters is utilized by outsourcing computational load to cloud server nodes. The mechanism of outsourcing computational task to remote server is called process offloading or cyber foraging. Smart mobile devices implement process offloading to utilize the computing poour of the cloud. The term cyber foraging is introduced to augment the computing potentials of wireless mobile devices by exploiting available stationary computers in the local environment. The mechanism of outsourcing computational load to remote surrogates in the close proximity is called cyber foraging . Researchers extend process offloading algorithms for Pervasive Computing, Grid Computing and Cluster Computing. In recent years, a number of cloud server based application offloading frameworks are introduced for outsourcing computational intensive components of the mobile applications partially or entirely to cloud datacenters. Mobile applications which are attributed with the features of runtime partitioning are called elastic mobile applications. Elastic applications are partitioned at runtime for the establishment of distributed processing platform.

# 3.4 Need for virtualization

Virtualization is the ability which allows sharing the physical instance of a single application or resource among multiple organizations or users. This technique is done by assigning a name logically to all those physical resources & provides a pointer to those physical resources based on demand.

Over an existing operating system & hardware, we generally create a virtual machine which and above it we run other operating systems or applications. This is called Hardware Virtualization. The virtual machine provides a separate environment that is logically distinct from its underlying hardware. Here, the system or the machine is the host & virtual machine is the guest machine. This virtual environment is managed by a firmware which is termed as a hypervisor.

Virtualization plays a significant role in cloud technology and its working mechanism. Usually, what happens in the cloud - the users not only share the data that are located in the cloud like an application but also share their infrastructures with the help of virtualization. Virtualization is used mainly to provide applications with standard versions for the cloud customers & with the release of the latest version of an application the providers can efficiently provide that application to the cloud and its users and it is possible using virtualization only. By the use of this virtualization concept, all servers & software other cloud providers require those are maintained by a third-party, and the cloud provider pays them on a monthly or yearly basis. In reality, most of the today's hypervisor make use of a combination of different types of hardware virtualization. Mainly virtualization means running multiple systems on a single machine but sharing all resources (hardware) & it helps to share IT resources to get benefit in the business field.



## Fig 3.5. Cloud Virtualization

## 3.4.1 Difference Between Virtualization and Cloud

1. Essentially there is a gap between these two terms, though cloud technology requires the concept of virtualization. Virtualization is a technology - it can also be treated as software that can manipulate hardware. Whereas cloud computing is a service which is the result of the manipulation.
2. Virtualization is the foundation element of cloud computing whereas Cloud technology is the delivery of shared resources as a service-on-demand via the internet.
3. Cloud is essentially made-up from the concept of virtualization.

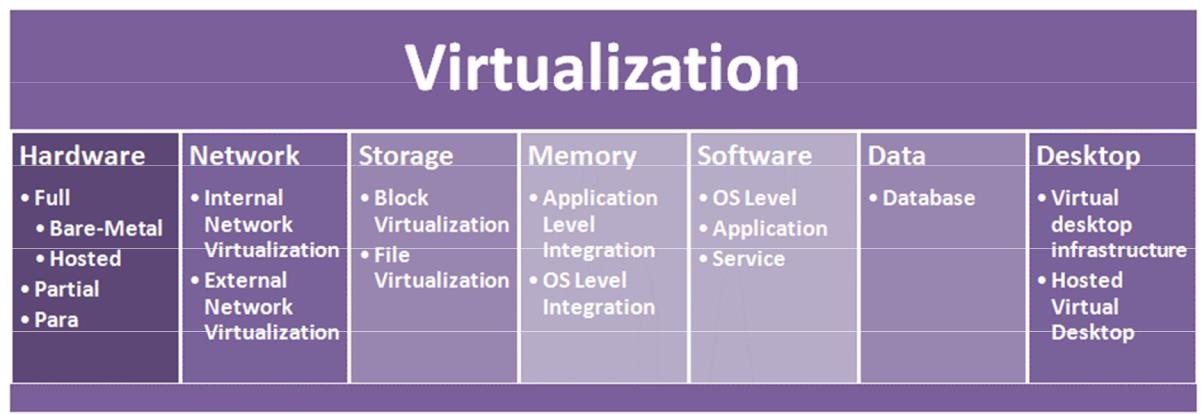
## 3.4.2 Advantages of Virtualization

* The number of servers gets reduced by the use of virtualization concept
* Improve the ability of technology
* The business continuity also raised due to the use of virtualization
* It creates a mixed virtual environment
* Increase efficiency for development & test environment
* Loours Total Cost of Ownership (TCO)

## 3.4.3 Features of Virtualization

1. Partitioning: Multiple virtual servers can run on a physical server at the same time
2. Encapsulation of data: All data on the virtual server including boot disks is encapsulated in a file format
3. Isolation: The Virtual server running on the physical server are safely separated & don't affect each other
4. Hardware Independence: When the virtual server runs, it can migrate to the different hardware platform

# 3.5 Types of Virtualization



**Fig 3.6: Virtualization types**

* + Seven Types of Virtualization
    - Hardware Virtualization.
    - Software Virtualization.
    - Network Virtualization.
    - Storage Virtualization
    - Memory Virtualization.
    - Data Virtualization.
    - Desktop Virtualization.

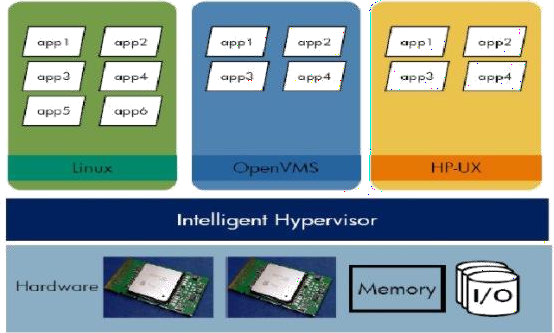
## Hardware Virtualization

* Hardware or platform virtualization means creation of virtual machine that act like **real computer**.
* Ex. Computer running Microsoft Windows 7 may host the virtual machine look like a Ubundu
* Hardware virtualization also knows as hardware-assisted virtualization or **server virtualization**.
* The basic idea of the technology is to combine many small physical servers into one large physical server, so that the processor can be used more effectively and efficiently.
* 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 advantages are increased processing poour as a result of **maximized hardware utilization and application uptime.**
* Hardware virtualization is further subdivided into the following types

**Full Virtualization** – Guest software does not require any modifications since the underlying hardware is fully simulated.

**Para Virtualization** – The hardware is not simulated and the guest software run their own isolated domains.

**Partial Virtualization** – The virtual machine simulates the hardware and becomes independent of it. The guest operating system may require modifications.



**Fig 3.7: Hardware Virtualization**

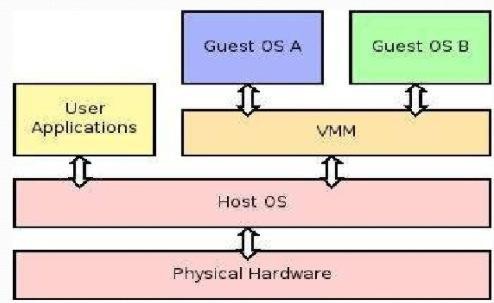
## Software Virtualization

* The ability to computer to run and create **one or more virtual environments**.
* It is used to enable a **computer system** in order to allow a guest OS to run.
* Ex. Linux to run as a guest that is natively running a Microsoft Windows OS
* Subtypes:

**Operating System Virtualization** – Hosting multiple OS on the native

**Application Virtualization** – Hosting individual applications in a virtual environment separate from the native OS

**Service Virtualization** – Hosting specific processes and services related to a particular application

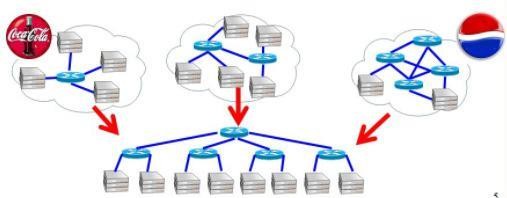


**Fig 3.8: Software Virtualization**

## Network Virtualization

* It refers to the **management and monitoring of a computer network** as a single managerial entity from a single software-based administrator’s console.
* **Multiple sub-networks** can be created on the same physical network, which may or may not is authorized to communicate with each other.
* It allows **network optimization** of data transfer rates, scalability, reliability, flexibility, and security
* Subtypes:

**Internal network**: Enables a single system to function like a network O **External network**: Combine many networks, or parts of networks into a virtual unit.



**Fig 3.9: Network Virtualization**

## Storage Virtualization

* **Multiple physical storage devices** are grouped together, which look like a single storage device.
* Ex. **Partitioning our hard drive** into multiple partitions

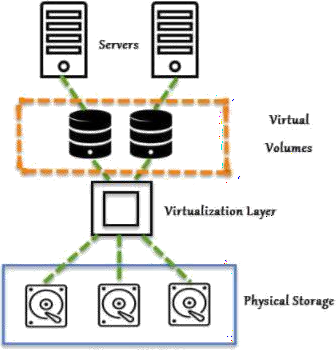
## Advantages

* + Improved storage management in a heterogeneous IT environment
  + Easy updates, better availability
  + Reduced downtime
  + Better storage utilization
  + Automated management

## Two types

**Block-** Multiple storage devices are consolidated into one

**File-** Storage system grants access to files that are stored over multiple hosts



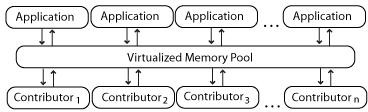
**Fig 3.10: Storage Virtualization**

## Memory Virtualization

* The way to **decouple memory from the server** to provide a shared, distributed or networked function.
* It enhances performance by providing **greater memory capacity** without any addition to the main memory.

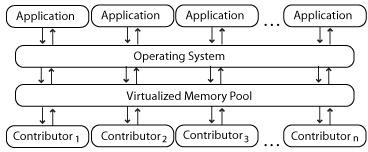
## Implementations

**Application-level integration –** Applications access the memory pool directly

a

**Fig 3.11: Application level integration**

**Operating System Level Integration –** Access to the memory pool is provided through an operating system.



**Fig 3.12: Operating system level integration**

## Data Virtualization

* Without any technical details, we can **easily manipulate data** and know how it is formatted or where it is physically located.
* It decreases the data errors and workload
* The data is presented as an abstract layer **completely independent of data structure and database systems**
* The user’s desktop is stored on a remote server, allowing **the user to access his/her desktop from any device or location**.
* It provides the **work convenience and security**
* It provides a lot of flexibility for employees to **work from home or on the go**
* Since the **data transfer takes place over secure protocols**, any risk of data theft is minimized



* **Fig 3.13: Data virtualization**

# 3.6 Operating System Virtualization:

Operating system virtualization refers to the use of software to allow system hardware to run multiple instances of different operating systems concurrently, allowing we to run different applications requiring different operating systems on one computer system. The operating systems do not interfere with each other or the various applications. Not to be confused with operating system-level virtualization, which is a type of server virtualization.

# 3.6.1 VMWare

VMware is a virtualization and cloud computing software provider based in Palo Alto, Calif. Founded in 1998, VMware is a subsidiary of Dell Technologies. EMC Corporation originally acquired VMware in 2004; EMC was later acquired by Dell Technologies in 2016. VMware bases its virtualization technologies on its bare-metal hypervisor ESX/ESXi in x86 architecture.With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server. Each VM can run its own operating system (OS), which means multiple OSes can run on one physical server. All the VMs on the same physical server share resources, such as networking and RAM. In 2019, VMware added support to its hypervisor to run containerized workloads in a Kubernetes cluster in a similar way. These types of workloads can be managed by the infrastructure team in the same way as virtual machines and the DevOps teams can deploy containers as they oure used to.

Diane Greene, Scott Devine, Mendel Rosenblum, Edward Wang and Edouard Bugnion founded VMware, which launched its first product -- VMware Workstation -- in 1999. The company released its second product, VMware ESX in 2001.VMware products include virtualization, networking and security management tools, software-defined data center software and storage software.VMware vSphere is VMware's suite of virtualization products. VMware vSphere, known as VMware Infrastructure prior to 2009, includes the following:

* ESXi
* vCenter Server
* vSphere Client
* vMotion

As of April 2018, the most current version is vSphere 6.7, which is available in three editions: Standard, Enterprise Plus and Platinum. There are also two three-server kits targeted toward small and medium- sized businesses named vSphere Essentials and Essentials Plus.With **VMware Cloud on AWS**, customers can run a cluster of vSphere hosts with vSAN and NSX in an Amazon data center and run their workloads there while in the meantime manage them with their well-known VMware tools and skills.

## 3.6.2 Networking and security

**VMware NSX** is a virtual networking and security software offering created when VMware acquired Nicera in 2012. NSX allows an admin to virtualize network components, enabling them to develop, deploy and configure virtual networks and switches through software rather than hardware. A software layer sits on top of the hypervisor to allow an administrator to divide a physical network into multiple virtual networks.With the latest release of the product, NSX-T Data Center, network virtualization can be added to both ESXi and KVM as hypervisors, as well as to bare-metal servers. Also containerized workloads in a Kubernetes cluster can be virtualized and protected. NSX-T Data Center also offers Network Function Virtualization, with which functions such as a firewall, load balancer and VPN, can be run in the virtualization software stack.

**VMware vRealize Network Insight** is a network operations management tool that enables an admin to plan microsegmentation and check on the health of VMware NSX. VRealize Network Insight relies on technology from VMware's acquisition of Arkin in 2016. VRealize Network Insight collects information from the NSX Manager. It also displays errors in its user interface, which helps troubleshoot an NSX environment.

## Software Defined Data Center ( SDDC ) platform:

**VMware Cloud Foundation** is an integrated software stack that bundles vSphere, VMware vSAN and VMware NSX into a single platform through the SDDC Manager. An admin can deploy the bundle on premises as a private cloud or run it as a service within a public cloud. An administrator can provision an application immediately without having to wait for network or storage.

## Storage and availability

**VMware vSAN** is a software-based storage feature that is built into the ESXi hypervisor and integrated with vSphere; it pools disk space from multiple ESXi hosts and provisions it via smart policies, such as protection limits, thin provisioning and erasure coding. It integrates with vSphere High Availability to offer increased compute and storage availability.

**VMware Site Recovery Manager (SRM)** is a disaster recovery management product that allows an administrator to create recovery plans that are automatically executed in case of a failure. Site Recovery Manager allows admins to automatically orchestrate the failover and failback of VMs. SRM also integrates with NSX to preserve network and security policies on migrated VMs.

**VMware vCloud NFV** is a network functions virtualization platform that enables a service provider to run network functions as virtualized applications from different vendors. NFV provides the same benefits of virtualization and cloud to a communications service provider that previously relied on hardware.

## Cloud management platform

The **vRealize Suite** is a group of software that allows a user to create and manage hybrid clouds. The vRealize Suite includes vRealize Operations for monitoring, vRealize Log Insight for centralized logging, vRealize Automation for data center automation and vRealize Business for Cloud for cost management.

With this bundle, an administrator can deploy and manage VMs on multiple hypervisors or cloud platforms from a single management console. Released in 2019, VMware Tanzu allows customers to build containerized apps, run enterprise Kubernetes and manage Kubernetes for developers and IT.

## Virtual desktop infrastructure

**VMware Horizon** allows organizations to run Windows desktops in the data center or in VMware Cloud on AWS. This removes the need to place and manage full desktops on the workplace and centralizes management and security for the user's environment. It integrates with the VMware products App Volumes and Dynamic Environment Manager for application delivery and Windows desktop management.

## Digital workspace and enterprise mobility management

Workspace ONE allows an administrator to control mobile devices and cloud-hosted virtual desktops and applications from a single management platform deployed either in the cloud or on premises. The Workspace ONE suite includes VMware AirWatch, Horizon Air and Identity Manager. Identity Manager is an identity-as-a-service product that offers single sign-on (SSO) capabilities for web, cloud and mobile applications. Identity Manager gives SSO access to any application from any device, based on the policies created.VMware AirWatch is an enterprise mobility management (EMM) software platform that enables an administrator to deploy and manage mobile devices, applications and data.

## Personal desktop

VMware Workstation is the first product ever released by the software company. It enables users to create and run VMs directly on a single Windows or Linux desktop or laptop. Those VMs run simultaneously with the physical machine. Each VM runs its own OS such as Windows or Linux. This enables users to run Windows on a Linux machine or vice versa simultaneously with the natively installed OS.VMware Fusion is software like VMware Workstation that virtualizes a Windows or Linux OS on Mac computers.

## Benefits of VMware

* Security based on a zero-trust model, along with better security than container systems like Kubernetes;
* Better provisioning of applications and resources;
* Simplified Data Center Management
* Increased efficiency and agility of data center systems.

## Drawbacks of VMware

* High licensing fees;
* Better Hyper-V and Xen hypervisor alternatives, according to some;
* Lack of support and several bugs when used alongside oracle products; and
* Hardware compatibility issues as not everything works well with VMware.

# 3.7 KVM

Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux®. Specifically, KVM lets we turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs). KVM is part of Linux. If we’ve got Linux 2.6.20 or neour, we’ve got KVM. KVM was first announced in 2006 and merged into the mainline Linux kernel version a year later. Because KVM is part of existing Linux code, it immediately benefits from every new Linux feature, fix, and advancement without additional engineering.

## 3.7.1 Working of KVM

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.

## Implementing KVM

We need to have to run a version of Linux that was released after 2007 and it needs to be installed on X86 hardware that supports virtualization capabilities. If both of those boxes are checked, then all we have to do is load 2 existing modules (a host kernel module and a processor-specific module), an emulator, and any drivers that will help we run additional systems.

But implementing KVM on a supported Linux distribution—like Red Hat Enterprise Linux—expands KVM's capabilities, letting we swap resources among guests, share common libraries, optimize system performance, and a lot more.

## 3.7.3 Migrating to a KVM-based virtual infrastructure

Building a virtual infrastructure on a platform we’re contractually tied to may limit our access to the source code. That means our IT developments are probably going to be more workarounds than innovations, and the next contract could keep we from investing in clouds, containers, and automation. Migrating to a KVM-based virtualization platform means being able to inspect, modify, and enhance the source code behind our hypervisor. And there’s no enterprise-license agreement because there’s no source code to protect.

## 3.7.4 KVM features

KVM is part of Linux. Linux is part of KVM. Everything Linux has, KVM has too. But there are specific features that make KVM an enterprise’s preferred hypervisor.

**Security**

KVM uses a combination of security-enhanced Linux (SELinux) and secure virtualization (sVirt) for enhanced VM security and isolation. SELinux establishes security boundaries around VMs. sVirt extends SELinux’s capabilities, allowing Mandatory Access Control (MAC) security to be applied to guest VMs and preventing manual labeling errors.

**Storage**

KVM is able to use any storage supported by Linux, including some local disks and network-attached storage (NAS). Multipath I/O may be used to improve storage and provide redundancy. KVM also supports shared file systems so VM images may be shared by multiple hosts. Disk images support thin provisioning, allocating storage on demand rather than all up front.

## Hardware Support:

KVM can use a wide variety of certified Linux-supported hardware platforms. Because hardware vendors regularly contribute to kernel development, the latest hardware features are often rapidly adopted in the Linux kernel.

## Memory Management:

KVM inherits the memory management features of Linux, including non-uniform memory access and kernel same-page merging. The memory of a VM can be swapped, backed by large volumes for better performance, and shared or backed by a disk file.

## Live Migration

KVM supports live migration, which is the ability to move a running VM between physical hosts with no service interruption. The VM remains powered on, network connections remain active, and applications continue to run while the VM is relocated. KVM also saves a VM's current state so it can be stored and resumed later.

## Performance and Scalability

KVM inherits the performance of Linux, scaling to match demand load if the number of guest machines and requests increases. KVM allows the most demanding application workloads to be virtualized and is the basis for many enterprise virtualization setups, such as datacenters and private clouds

## Scheduling and Resource Control:

In the KVM model, a VM is a linux process, scheduled and managed by the kernel. The Linux scheduler allows fine-grained control of the resources allocated to a Linux process and guarantees a quality of service for a particular process. In KVM, this includes the completely fair scheduler, control groups, network name spaces, and real-time extensions.

## Lower Latency and higher prioritization

The Linux kernel features real-time extensions that allow VM-based apps to run at loour latency with better prioritization(compared to bare metal). The kernel also divides processes that require long computing times into smaller components, which are then scheduled and processed accordingly.

## Managing KVM

It’s possible to manually manage a handful of VM fired up on a single workstation without a management tool. Large enterprises use virtualization management software that interfaces with virtual environments and the underlying physical hardware to simplify resource administration, enhance data analyses, and streamline operations. Red Hat created Red Hat Virtualization for exactly this purpose.

## KVM and Red Hat

We believe in KVM so much that it’s the sole hypervisor for all of our virtualization products, and we’re continually improving the kernel code with contributions to the KVM community. But since

KVM is part of Linux, it’s already included in Red Hat Enterprise Linux. Red Hat has 2 versions of KVM. The KVM that ships with Red Hat Enterprise Linux has all of the hypervisor functionality with basic management capabilities, allowing customers to run up to 4 isolated virtual machines on a single host. Red Hat Virtualization contains an advanced version of KVM that enables enterprise management of unlimited guest machines. It’s ideal for use in datacenter virtualization, technical workstations, private clouds, and in development or production.

# 3.8 System VM and Process VM

## Two categories of virtual machines

Virtual machines are separated in two major categories, based on their use and degree of correspondence to any real machine. A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS). In contrast, a process virtual machine is designed to run a single program, which means that it supports a single process. An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine — it cannot break out of its virtual world.

# 3.8.1 System Virtual Machines

System virtual machines (sometimes called hardware virtual machines) allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. The software layer providing the virtualization is called a virtual machine monitor or hypervisor. A hypervisor can run on bare hardware (Type 1 or native VM) or on top of an operating system (Type 2 or hosted VM).

## Main advantages of system VMs

* + Multiple OS environments can co-exist on the same computer, in strong isolation from each other;
  + The virtual machine can provide an instruction set architecture (ISA) that is somewhat different from that of the real machine.

## Main disadvantages of system VMs

* + There's still an overhead of the virtualization solution which is used to run and manage a VM, so performance of a VM will be somewhat slower compared to a physical system with comparable configuration
  + Virtualization means decoupling from physical hardware available to the host PC, this usually means access to devices needs to go through the virtualization solution and this may not always be possible

Multiple VMs each running their own operating system (called guest operating system) are frequently used in server consolidation, where different services that used to run on individual machines in order to avoid interference are instead run in separate VMs on the same physical machine. This use is frequently called quality-of-service isolation (QoS isolation).

# 3.8.2 Process Virtual Machines

A process VM, sometimes called an application virtual machine, runs as a normal application inside an OS and supports a single process. It is created when that process is started and destroyed when it exits. Its purpose is to provide a platform-independent programming environment that abstracts away details of the underlying hardware or operating system, and allows a program to execute in the same way on any platform.

A process VM provides a high-level abstraction — that of a high-level programming language (compared to the low-level ISA abstraction of the system VM). Process VMs are implemented using an interpreter; performance comparable to compiled programming languages is achieved by the use of just-in-time compilation. This type of VM has become popular with the Java programming language, which is implemented using the Java virtual machine. Another example is the .NET Framework, which runs on a VM called the Common Language Runtime.

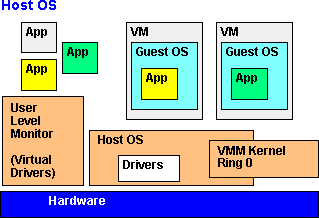
# 3.9 Virtual Machine Monitor

A Virtual Machine Monitor (VMM) is a software program that enables the creation, management and governance of virtual machines (VM) and manages the operation of a virtualized environment on top of a physical host machine. VMM is also known as Virtual Machine Manager and Hypervisor. VMM is the primary software behind virtualization environments and implementations. When installed over a host machine, VMM facilitates the creation of VMs, each with separate operating systems (OS) and applications. VMM manages the backend operation of these VMs by allocating the necessary computing, memory, storage and other input/output (I/O) resources. VMM also provides a centralized interface for managing the entire operation, status and availability of VMs that are installed over a single host or spread across different and interconnected hosts.

The software that creates a virtual machine (VM) environment in a computer In a regular, non-virtual computer, the operating system is the master control program, which manages the execution of all applications and acts as an interface between the apps and the hardware. The OS has the highest privilege level in the machine, known as "ring 0"

In a VM environment, the VM monitor (VMM) becomes the master control program with the highest privilege level, and the VMM manages one or more "guest operating systems." Each guest OS manages its own applications in a separate "virtual machine" (VM) in the computer, sometimes called a "guest OS stack."

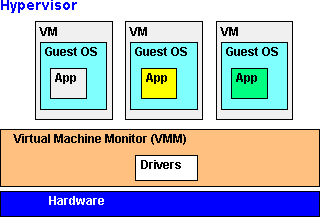
The VM monitor (VMM) is an interface between the guest OS and the hardware. It intercepts calls to the peripheral devices and memory tables from each guest OS and intercedes on its behalf. In reverse, when a disk or SSD write creates an interrupt, the VM monitor injects that interrupt into the appropriate guest OS. Following are the major monitor types.



* **Fig 3.14: Host OS monitor**

**Host OS**

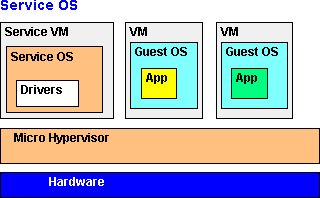
This VM monitor (VMM) is installed in an existing, running computer. The VMM kernel runs alongside the host OS, and calls for I/O are redirected to virtual drivers that call the native API of the host OS. Examples of OS-hosted VMMs are VMware Workstation, VMware Server, Parallels Workstation and Parallels Desktop for Mac.



* **Fig 3.15: VM monitor**

**Hypervisor**

The hypervisor monitor provides the most control, flexibility and performance, because it is not subject to limitations of a host OS. The hypervisor relies on its own software drivers for the hardware; however, they may limit portability to another platform. Examples of this method are VMware ESX and IBM's mainframe z/VM.



* **Fig 3.16: Hypervisor**

**Service OS**

This method combines the robustness of the hypervisor with the flexibility of the host model. In order to take advantage of the drivers in a popular OS, the Service OS runs as a component of the hypervisor in a separate VM. Xen, XenServer and Hyper-V are examples of the service VM approach. The VMM is in charge of running the virtual machines.

## There are two main types of VMM:

Type 1: Native

Type 2: Hosted

**Type 1**: Native Hypervisors run directly on the host machine, and share out resources (such as memory and devices) between guest machines.

e.g. XEN, Oracle VM Server

**Type 2:** Hosted Hypervisors run as an application inside an operating system, and support virtual machines running as individual processes.

e.g. VirtualBox, Parallels Desktop, QEMU

## Properties of a Virtual Machine

1.Efficiency: The majority of guest instructions are executed directly on the host machine. 2.Resource Control: The virtual machine monitor must remain in control of all machine resources.

3.Equivalence: The virtual machine must behave in a way that is indistinguishable from if it was running as a physical machine.

## Efficiency

“All innocuous instructions are executed by the hardware directly, with no intervention at all on the part of the control program.”

Normal guest machine instructions should be executed directly on the processor. System instructions need to be emulated by the VMM.

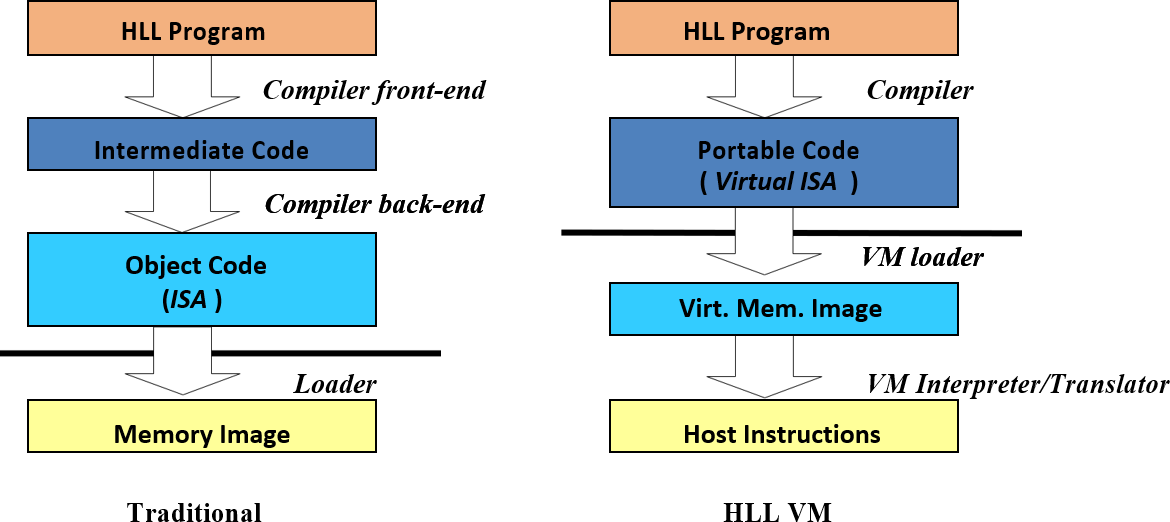
## Resource Control

“It must be impossible for that arbitrary program to affect the system resources, i.e. memory, available to it; the allocator of the control program is to be invoked upon any attempt.” The virtual machine should not be able to affect the host machine in any adverse way. The host machine should remain in control of all physical resources, sharing them out to guest machines.

## Equivalence

“Any program K executing with a control program resident, with two possible exceptions, performs in a manner indistinguishable from the case when the control program did not exist and K had whatever freedom of access to privileged instructions that the programmer had intended.” A formal way of saying that the operating system running on a virtual machine should believe it is running on a physical machine, i.e. the behaviour of the virtual machine (from the guest OS’ point of view) is identical to that of the corresponding physical machine.The two exceptions mentioned are: temporal latency (some instruction sequences will take longer to run) and resource availability (physical machine resources are shared between virtual machines)

# High Level Language Virtual Machines(HLL VM)



**Fig 3.17: Traditional vs HLL VM**

**Two major examples**– Java VM

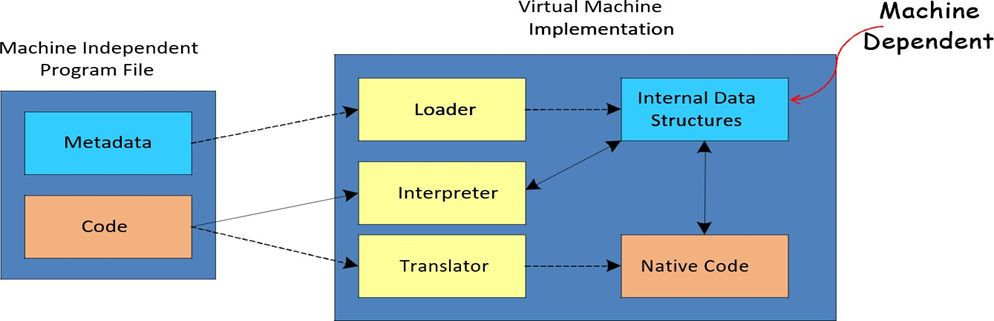
* Microsoft Common Language Infrastructure (CLI)

## HLL VMS:

Compiler forms program files (e.g. class files)

–Standard format

Program files contain both code and metadata–



* **Fig 3.18: Traditional vs HLL VM**

|  |  |
| --- | --- |
| Java Virtual Machine Architecture & CLI | – Analogous to an ISA |
| Java Virtual Machine Implementation & CLR (Common Language Runtime) | – Analogous to a computer implementation |
| Java bytecodes & Microsoft Intermediate Language (MSIL), CIL, IL | -The instruction part of the ISA |
| Java Platform & .NET framework | – ISA + Libraries; a higher level ABI |

## Characteristics of HLL VMs

•Security

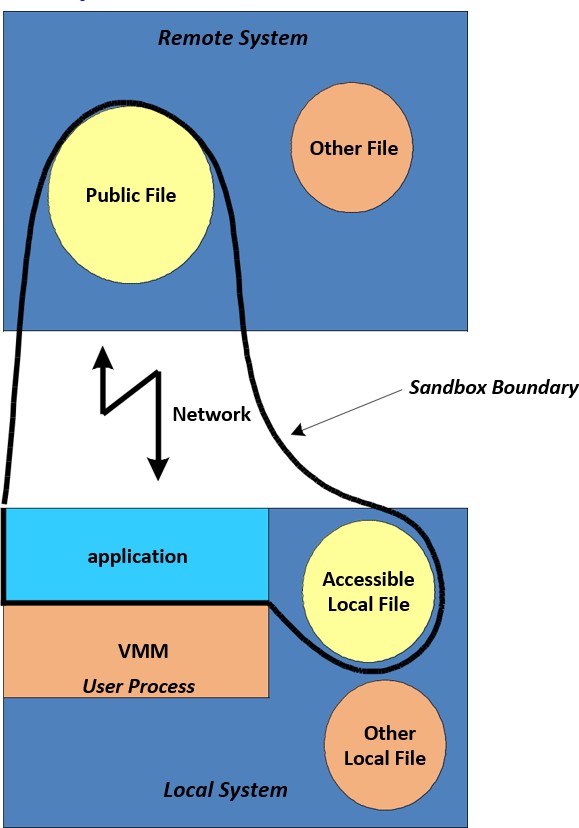
•Robustness

•Networking

•Performance

## Security

* A key aspect of modern network-oriented VMs
* Must protect:
* Local files and resources
* Runtime from user process
* The program runs in a sandbox at the host machine. It is managed by the VM runtime.
* The ability to load an untrusted application and run it in a managed secure fashion is a very big challenge!



* **Fig 3.19: HLL VM**

## Robustness: Object Orientation

* **Objects**
* Data carrying entities
* Dynamically allocated
* Must be accessed via pointers or references

## Methods

* Procedures that operate on objects

## Class

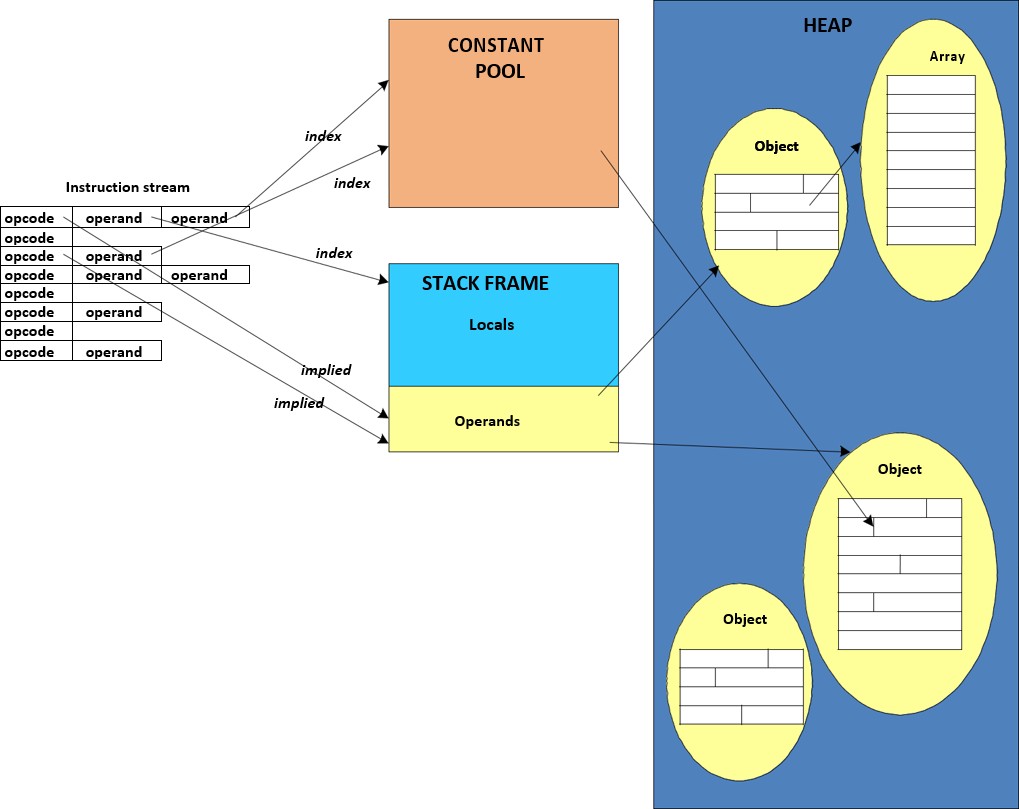
* A type of object and its associated methods
* Object created at runtime is an instance of the class
* Data associated with a class may be dynamic or static

OO programming paradigm has become the model of choice for modern HLL VMs. Both Java and CLI are designed to support OO software.

## Networking:

•The application must use the available bandwidth (scarce) efficiently

* Application loaded incrementally dynamic linking
* Improves program startup-time



## Fig:3.20 Memory Hierarchy in JVM

**JVM: Bytcode Emulation**

* Interpretation
* Simple, fast startup, but slow

•Just-In-Time (JIT) Compilation

* Compile each method when first touched
* Simple, static optimizations

•Hot-Spot Compilation

* Find frequently executed code
* Apply more aggressive optimizations on that code
* Typically phased with interpretation or JIT
* Dynamic Compilation
* Based on Hot-Spot compilation
* Use runtime information to optimize

# 3.10. Hypervisor

Software that controls the layer between the hardware operating systems. It allows multiple operating systems to run on the same physical hardware. There are two types of hypervisors:

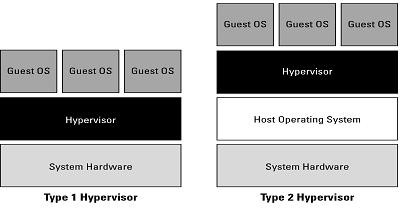
* Bare metal, which allows the hypervisor to run directly on the hardware
* Hosted architecture, in which the hypervisor runs on top of an existing operating system

A low-level program is required to provide system resource access to virtual machines, and this program is referred to as the hypervisor or Virtual Machine Monitor (VMM). A hypervisor running on bare metal is a Type 1 VM or native VM. Examples of Type 1 Virtual Machine Monitors are LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogix VLX, VMware ESX and ESXi, and Wind River VxWorks, among others. The operating system loaded into a virtual machine is referred to as the guest operating system, and there is no constraint on running the same guest on multiple VMs on a physical system. Type 1 VMs have no host operating system because they are installed on a bare system.

An operating system running on a Type 1 VM is a full virtualization because it is a complete simulation of the hardware that it is running on. Not all CPUs support virtual machines, and many that do require that we enable this support in the BIOS. For example, AMD-V processors (code named Pacifica) and Intel VT-x (code named Vanderpool) oure the first of these vendor's 64-bit offerings that added this type of support.

Some hypervisors are installed over an operating system and are referred to as Type 2 or hosted VM. Examples of Type 2 Virtual Machine Monitors are Containers, KVM, Microsoft Hyper V, Parallels Desktop for Mac, Wind River Simics, VMWare Fusion, Virtual Server 2005 R2, Xen, Windows Virtual PC, and VMware Workstation 6.0 and Server, among others. This is a very rich product category. Type 2 virtual machines are installed over a host operating system; for Microsoft Hyper-V, that operating system would be Windows Server. In the section that follows, the Xen hypervisor (which runs on top of a Linux host OS) is more fully described. Xen is used by Amazon Web Services to provide Amazon Machine Instances (AMIs). On a Type 2 VM, a software interface is created that emulates the devices with which a system would normally interact. This abstraction is meant to place many I/O operations outside the virtual environment, which makes it both programmatically easier and more efficient to execute device I/O than it would be inside a virtual environment. This type of virtualization is sometimes referred to as paravirtualization, and it is found in hypervisors such as Microsoft's Hyper-V and Xen. It is the host operating system that is performing the I/O through a para-API.

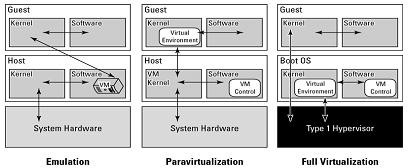
## 3.10.1 VMware's vSphere cloud computing infrastructure model



**Fig 3.21: Hypervisor**

**3.10.2 Type 1 and Type 2 hypervisors.**

The above figure shows the difference between emulation, para virtualization, and full virtualization. In emulation, the virtual machine simulates hardware, so it can be independent of the underlying system hardware. A guest operating system using emulation does not need to be modified in any way. Para virtualization requires that the host operating system provide a virtual machine interface for the guest operating system and that the guest access hardware through that host VM. An operating system running as a guest on a paravirtualizationsystem must be ported to work with the host interface. Finally, in a full virtualization scheme, the VM is installed as a Type 1 Hypervisor directly onto the hardware. All operating systems in full virtualization communicate directly with the VM hypervisor, so guest operating systems do not require any modification. Guest operating systems in full virtualization systems are generally faster than other virtualization schemes. The Virtual Machine Interface (VMI) open standard [(http://vmi](http://vmi/) ncsa.uiuc.edu/) that VMware has proposed is an example of a paravirtualization API. The latest version of VMI is 2.1, and it ships as a default installation with many versions of the Linux operating system. Wikipedia maintains a page called “Comparison of platform virtual machines” <http://en.wikipedia.org/wiki/Comparison>of platform virtual machines. The page contains a table of features of the most common Virtual Machine Managers. Mostly all are familiar with process or application virtual machines. Most folks run the Java Virtual Machine or Microsoft's .NET Framework VM (called the Common Language Runtime or CLR) on their computers. A process virtual machine instantiates when a command begins a process, the VM is created by an interpreter, the VM then executes the process, and finally the VM exits the system and is destroyed. During the time the VM exists, it runs as a high-level abstraction.



**Fig 3.22: types of virtualization**

## 3.10.3 Emulation, paravirtualization, and full virtualization types

Applications running inside an application virtual machine are generally slow, but these programs are very popular because they provide portability, offer rich programming languages, come with many advanced features, and allow platform independence for their programs. Although many cloud computing applications provide process virtual machine applications, this

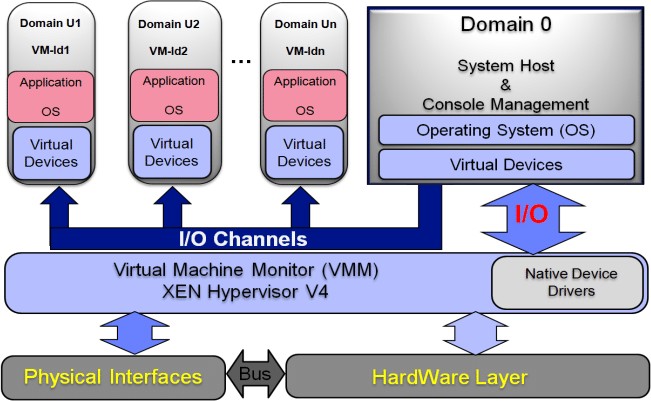
type of abstraction isn't really suitable for building a large or high-performing cloud network, with one exception. The exception is the process VMs that enable a class of parallel cluster computing applications. These applications are high-performance systems where the virtual machine is operating one process per cluster node, and the system maintains the necessary intra-application communications over the network interconnect. Examples of this type of system are the Parallel Virtual Machine (PVM; see <http://www.csm.ornl.gov/pvm/pvm> home.html) and the Message Passing Interface (MPI; see [http://www](http://www/) mpi-forum.org/).

Some people do not consider these application VMs to be true virtual machines, noting that these applications can still access the host operating system services on the specific system on which they are running. The emphasis on using these process VMs is in creating a high-performance networked supercomputer often out of heterogeneous systems, rather than on creating a ubiquitous utility resource that characterizes a cloud network.

Some operating systems such as Sun Solaris and IBM AIX 6.1 support a feature known as operating system virtualization. This type of virtualization creates virtual servers at the operating system or kernel level. Each virtual server is running in its own virtual environment (VE) as a virtual private server (VPS). Different operating systems use different names to describe these machine instances, each of which can support its own guest OS. However, unlike true virtual machines, VPS must all be running the same OS and the same version of that OS. Sun Solaris 10 uses VPS to create what is called Solaris Zones. With IBM AIX, the VPS is called a System Workload Partition (WPAR). This type of virtualization allows for a dense collection of virtual machines with relatively low overhead. Operating system virtualization provides many of the benefits of virtualization previously noted in this section.

# 3.11 Xen Hypervisor

Xen Hypervisor Xen is a type-1 hypervisor, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently. It was developed by

the University of Cambridge. Now being developed by the Linux Foundation with support from Intel.

**Fig 3.23: Xen**

Xen is a hypervisor that enables the simultaneous creation, execution and management of multiple virtual machines on one physical computer.

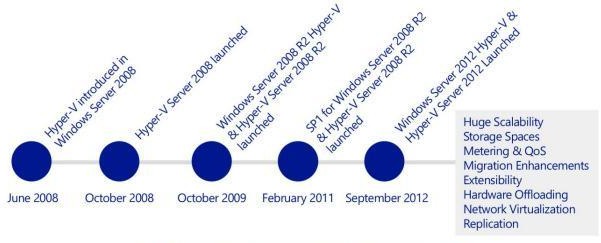
* + Xen was developed by XenSource, which was purchased by Citrix Systems in 2007.
  + Xen was first released in 2003.
  + It is an open source hypervisor.
  + It also comes in an enterprise version.
  + Because it's a type-1 hypervisor, Xen controls, monitors and manages the hardware, peripheral and I/O resources directly.
  + Guest virtual machines request Xen to provision any resource and must install Xen virtual device drivers to access hardware components.
  + Xen supports multiple instances of the same or different operating systems with native support for most operating systems, including Windows and Linux.
* Moreover, Xen can be used on x86, IA-32 and ARM processor architecture.

# 3.12 Hyper V

Microsoft **Hyper-V**, formerly known as **Windows Server Virtualization**, is a native hypervisor; it can create virtual machines on x86-64 systems

running Windows. Starting with Windows 8, Hyper-V supersedes Windows Virtual PC as the hardware virtualization component of the client editions of Windows NT. A server computer running Hyper-V can be configured to expose individual virtual machines to one or more networks.

Hyper-V was first released alongside Windows Server 2008, and has been available without charge for all the Windows Server and some client operating systems since.



**Fig 3.24: Hyper V**

There are two manifestations of the Hyper-V technology:

**Hyper-V** is the hypervisor-based virtualization role of **Windows Server**.

**Microsoft Hyper-V Server** is the hypervisor-based server virtualization product that allows customers to consolidate workloads onto a single physical server. This is available as a free download.With the launch of Windows Server 2008 R2 Hyper-V, in October 2009, Microsoft introduced a number of compelling capabilities to help organizations reduce costs, whilst increasing agility and flexibility. Key features introduced included:

**Live Migration** – Enabling the movement of virtual machines (VMs) with no interruption or downtime

**Cluster Shared Volumes** – Highly scalable and flexible use of shared storage (SAN) for VMs

**Processor Compatibility** – Increase the Flexibility for Live Migration across hosts with differing CPU architectures

**Hot Add Storage** – Flexibly add or remove storage to and from VMs

**Improved Virtual Networking Performance** – Support for Jumbo Frames and Virtual Machine Queue (VMq)

With the addition of Service Pack 1 (SP1) for Hyper-V, in October 2011, Microsoft introduced 2 new, key capabilities to help organizations realize even greater value from the platform:

**Dynamic Memory** – More efficient use of memory while maintaining consistent workload performance and scalability.

**RemoteFX**– Provides the richest virtualized Windows 7 experience for Virtual Desktop Infrastructure (VDI) deployments.

## 3.12.1 Windows Server 2012 Hyper V and Windows Server 2012 R2

Fast forward to September 2012, and the launch of Windows Server 2012. This brought an incredible number of new and an enhanced Hyper-V capabilities. These capabilities, many of which we’ll discuss in this paper, ranged from enhancements around scalability, new storage and networking features, significant enhancements to the Live Migration capabilities, deeper integration with hardware, and an in-box VM replication capability, to name but a few. These improvements, new features and enhancements can be grouped into 4 key areas, and it’s these key areas we’ll focus on throughout this whitepaper, looking at both Windows Server 2012 and R2, and how it compares and contrasts with vSphere 5.5. The 4 key areas are:

**Scalability, Performance & Density** – customers are looking to run bigger, more poourful virtual machines, to handle the demands of their biggest workloads. In addition, as hardware scale grows, customers wish to take advantage of the largest physical systems to drive the highest levels of density, and reduce overall costs.

**Security &Multitenancy**- Virtualized data centers are becoming more popular and practical every day. IT organizations and hosting providers have begun offering infrastructure as a service (IaaS), which provides more flexible, virtualized infrastructures to customers— “server instances on-demand.” Because of this trend, IT organizations and hosting providers must offer customers enhanced security and isolation from one another, and in some cases, encrypted to meet compliance demands.

**Flexible Infrastructure** – In a modern datacenter, customers are looking to be agile, in order to respond to changing business demands quickly, and efficiently. Being able to move workloads flexibly around the infrastructure is of incredible importance, and in addition, customers want to be able to choose where best to deploy their workloads based on the needs of that workload specifically.

**High Availability & Resiliency** – As customers’ confidence in virtualization grows, and they virtualize their more mission-critical workloads, the importance of keeping those workloads continuously available grows significantly. Having capabilities built into the platform that not only help keep those workloads highly available, but also, in the event of a disaster, quick to restore in another geographical location, is of immense importance when choosing a platform for today’s modern datacenter.

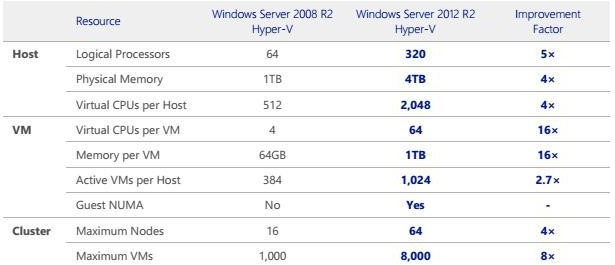
## 3.12.2 Need for Hyper-V

Virtualization technologies help customers’ loour costs and deliver greater agility and economies of scale. Either as a stand-alone product or an integrated part of Windows Server, Hyper-V is a leading virtualization platform for today and the transformational opportunity with cloud computing. With Hyper-V, it is now easier than ever for organizations to take advantage of the cost savings of virtualization, and make the optimum use of server hardware investments by consolidating multiple server roles as separate virtual machines that are running on a single physical machine. Customers can use Hyper-V to efficiently run multiple operating systems, Windows, Linux, and others, in parallel, on a single server. Windows Server 2012 R2 extends this with more features, greater scalability and further inbuilt reliability mechanisms. In the data center, on the desktop, and now in the cloud, the Microsoft virtualization platform, which is led by Hyper-V and surrounding System Center management tools, simply makes more sense and offers better value for money when compared to the competition.

## Enhanced Storage Capabilities

Windows Server 2012 and subsequently, 2012 R2 Hyper-V also introduce a number of enhanced storage capabilities to support the most intensive, mission-critical of workloads. These capabilities include:

**Virtual Fiber Channel** – Enables virtual machines to integrate directly into Fiber Channel Storage Area Networks (SAN), unlocking scenarios such as fiber channel-based Hyper-V Guest Clusters.



**Fig 3.25 Hyper V comparision**

**Support for 4-KB Disk Sectors in Hyper-V Virtual Disks.** Support for 4,000-byte (4-KB) disk sectors lets customers take advantage of the emerging innovation in storage hardware that provides increased capacity and reliability.

**New in R2 - Storage Spaces with Tiering-** Storage Spaces enables we to virtualize storage by grouping industry-standard disks into storage pools, and then create virtual disks called storage spaces from the available capacity in the storage pools. These pools now support a mix of HDD and SSD, providing a tiered pool, where hot data will reside on SSD and cold data on HDD. Fully supported as a repository for Hyper-V VMs.

**Data Deduplication -** Windows Server 2012 R2 also provides an inbox deduplication capabilities which utilizes sub-file variable-size chunking and compression to considerably reduce storage consumption for files and folders hosted on deduplicated Windows Server volumes. With Windows Server 2012 R2, support has been added for VDI deployments. Deduplication rates for VDI deployments can range as high as 95% savings and that includes VDI deployments that utilize differencing disks for rapid provisioning.

**New Virtual Hard Disk Format.** This new format, called VHDX, is designed to better handle current and future workloads and addresses the technological demands of an enterprise’s evolving needs by increasing storage capacity, protecting data, improving quality performance on 4-KB disks, and providing additional operation-enhancing features. The maximum size of a VHDX file is 64TB.

**Offloaded Data Transfer (ODX).** With Offloaded Data Transfer support, the Hyper-V host CPUs can concentrate on the processing needs of the application and offload storage-related tasks to the SAN, increasing performance.

**Online Checkpoint Merge**. With the online checkpoint merge capability, customers who have taken checkpoints (snapshots), for a running virtual machine, no longer have to poour down the virtual machine in order to merge the checkpoint back into the original virtual disk file, ensuring virtual machine uptime is increased and the administrator gains increased flexibility.

**New in R2 - Online Virtual Disk Resize**. With the online virtual disk resize, administrators can grow and shrink virtual disks that are attached to a VM’s virtual SCSI controller, providing an administrator with greater flexibility to respond to changing business needs.

## Enhanced Networking Performance

Windows Server 2012 R2 Hyper-V also includes a number of performance enhancements within the networking stack to help customers virtualize their most intensive network workloads. These capabilities include:

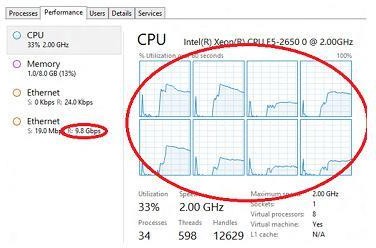
**Dynamic Virtual Machine Queue** – DVMQ dynamically distributes incoming VM network traffic processing to host processors (based on processor usage and network load). In times of heavy network load, Dynamic VMQ automatically recruits more processors. In times of light network load, Dynamic VMQ relinquishes those same processors

**IPsec Task Offload** - IPsec Task Offload in Windows Server 2012 R2 leverages the hardware capabilities of server NICs to offload IPsec processing. This reduces the CPU overhead of IPsec encryption and decryption significantly. In Windows Server 2012 R2, IPsec Task Offload is extended to Virtual Machines as well. Customers using VMs who want to protect their network traffic with IPsec can take advantage of the IPsec hardware offload capability available in server NICs, thus freeing up CPU cycles to perform more application level work and leaving the per packet encryption/decryption to hardware.

**SR-IOV** - When it comes to virtual networking, a primary goal is native I/O throughput. Windows Server 2012 R2 provides the ability to assign SR-IOV functionality from physical devices directly into virtual machines. This gives VMs the ability to bypass the software- based Hyper-V Virtual Network Switch, and more directly address the NIC. As a result, CPU overhead and latency is reduced, with a corresponding rise in throughput. This is all available, without sacrificing key Hyper-V features such as virtual machine Live Migration.

**New in R2 – Virtual Receive Side Scaling** - Prior to 10GbE networking, one modern processor was usually more than enough to handle the networking workload of a VM. With the introduction of 10GbE NICs, the amount of data being sent to and received from a VM exceeded what a single processor could effectively handle. In the physical host, this challenge had a solution, namely, Receive Side Scaling (RSS). RSS spreads traffic from the network

interface card (NIC), based on TCP flows, and to multiple processors for simultaneous processing of TCP flows. With Windows Server 2012 R2 however, similar to how RSS distributes networking traffic to multiple cores in physical machines, vRSS spreads networking traffic to multiple VPs in each VM by enabling RSS inside the VM. With vRSS enabled, a VM is able to process traffic on multiple VPs simultaneously and increase the amount of throughput it is able to handle.



**Fig 3.26: CPU utilization**

## Enhanced Resource Management

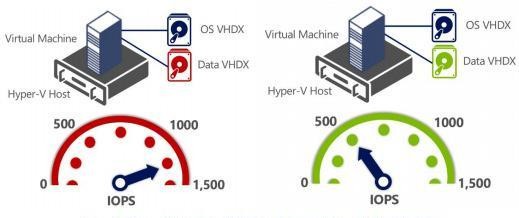
Windows Server 2012 R2 Hyper-V also includes a number of enhanced resource management capabilities that help customers to optimize the utilization of the virtualized infrastructure to drive higher levels of performance. These capabilities include:

**Dynamic Memory Improvements -** These improvements dramatically increase virtual machine consolidation ratios and improve reliability for restart operations that can lead to loour costs, especially in environments, such as VDI, that have many idle or low-load virtual machines. Administrators can now more flexibly manage memory through the use of aStartup, Minimum and Maximum configuration option, along with the ability to adjust the memory values whilst the VM is running, increasing flexibility for the administrator. Windows Server 2012 R2 Hyper-V also includes a capability known as Smart Paging, which provides a more reliable and robust solution for VM restarts when memory is under contention.

**Resource Metering -** In Windows Server 2012 R2 Hyper-V, Resource Metering, helps we track historical data on the use of virtual machines and gain insight into the resource use of specific servers. We can use this data to perform capacity planning, to monitor consumption by different business units or customers, or to capture data needed to help redistribute the costs of running a workload. Resource Metering captures metrics across CPU, Memory, Disk and Network.

**Network Quality of Service -** QoS provides the ability to programmatically adhere to a service level agreement (SLA) by specifying the minimum bandwidth that is available to a virtual machine or a port. It prevents latency issues by allocating maximum bandwidth use for a virtual machine or port.

**New in R2 – Storage Quality of Service –** Storage QoS provides storage performance isolation in a multitenant environment and mechanisms to notify we when the storage I/O performance does not meet the defined threshold to efficiently run our virtual machine workloads.



**Fig 3.27: IOPS of a Virtual machine**



**Fig 3.28:Hyper V comparison**

# 3.11 Virtual Box

Oracle VM VirtualBox is cross platform virtualization software that allows we to extend our existing computer to run multiple operating systems at the same time. Designed for IT professionals and developers, Oracle VM VirtualBox runs on Windows, Mac OS X, Linux and Oracle Solaris systems and is ideal for testing, developing, demonstrating and deploying solutions across multiple platforms on one machine.

## Key Benefits

* Run almost any type of application on our existing machine
* Quickly and easily try out new platforms
* Create a multiplatform test and development environment
* Build a multi1tier demonstration system on a single portable machine
* Extend the lifetime and usefulness of existing computers
* Run legacy platforms and applications on modern hardware
* Easily create isolated environments

## Key Features

* Available for Windows, Mac OS X, Linux and Oracle Solaris host operating systems
* Supports a wide range of guest platforms
* Easy to use graphical user interface
* Poourful, scriptable command line interface
* Import and export virtual machines using OVF/OVA standards
* Shared folders between guest and host
* Seamless, resizable, and full screen window display modes
* Video and 3D (OpenGL, DirectX) acceleration
* Virtual webcam
* Multiple virtual screen support
* Poourful and flexible networking options
* USB 1.1/2.0/3.0 and serial ports
* SAS, SATA, SCSI and IDE storage controllers
* Built-in iSCSI initiator
* Built-in Remote Display Server
* Multi-generational branched snapshots
* Linked and full clones
* Controllable copy and paste
* Screen-recording facility
* Disk image encryption
* HiDPI support
* Drag and drop support

## 3.11.1 Oracle VM VirtualBox Manager Screen



**Easy to Use, Fast and Powerful, Great Platform Coverage**

Designed for use on systems ranging from ultrabooks to high end server class hardware, Oracle VM Virtual Box is lightweight and easy to install and use. Yet under the simple exterior lies an extremely fast and poourful virtualization engine. With a formidable reputation for speed and agility, Oracle VM Virtual Box contains innovative features to deliver tangible business benefits: significant performance improvements; a more poourful virtualization system and a wider range of supported guest operating system platforms.

## Easy to Use

Improved Virtual Box Manager with further features – The Oracle VM Virtual Box Manager now supports hot-plug for SATA virtual disks and the option to customize status bar, menu bar and guest-content scaling for each virtual machine deployed;

New Introduced Headless and Detachable start options – The Oracle VM Virtual Box Manager now supports to start virtual machine in the background with a separate frontend process that can be closed while the virtual machine continues to work;

Easy to use Wizards – Wizards help with the creation of new virtual machines. Preconfigured settings are used based on the type of guest OS;

Easy import and export of appliances – Virtual machines can be created, configured and then shared by exporting and importing virtual appliances using industry-standard formats such as .ova; Improved Huge Range of Guest Platforms – including the very latest Windows 10, Windows Server 2012 R2 and leading edge Linux platforms too.

Improved Virtual Box Guest Additions – Installed inside the guest virtual machine, the Guest Additions provide a more natural user experience. For example, guest windows can be easily resized to arbitrary resolutions, made full-screen or even operate in seamless mode. And data can be copy and pasted to and from, and between, concurrently running machines and the host platform. This functionality is now controllable as bi-directional, uni-directional, or disabled;

Shared Folders – Share our host platform’s filesystem with the guest to facilitate real cross- platform computing;

Multi-touch support – Hosts supporting multi-touch interfaces can now also deliver this to their guests too;

Flexible Networking options – Oracle VM Virtual Box offers a rich range of networking models from easy-to-use NAT networking, to fully functional Bridged networking, and specialist Internal and Host-only networking too. The new “NAT Network” mode allows multiple guests to run on the same internal network, seeing each other, and also the outside world via a new NAT service;

IPv6 – IPv6 is now offered as an option in most networking modes alongside IPv4;

Virtual Media Manager – Oracle VM Virtual Box supports the widest range of virtual disk formats from its own native .vdi format to those offered by Microsoft (.vhd), VMware

(.vmdk), and Parallels (.vdd). The Virtual Media Manager tool now allows conversions between formats using an easy to use graphical user interface;

Video Capture – A built-in recording mechanism of the guest’s screen contents. Easy to start and stop, recording one or more virtual screens to the standard webm format.

## 3.11.2 Performance

Improved Latest Intel and AMD hardware support – Harnessing the latest in chip-level support for virtualization, Oracle VM Virtual Box supports even the most recent AMD and Intel processors bringing faster execution times for everything from Windows to Linux and Oracle Solaris guests. But Virtual Box will also run on older hardware without VT support;

Improved Instruction Set extended – More instruction set extensions available to the guest when running with hardware-assisted virtualization; this include also AES-NI that improve the speed of applications performing encryption and decryption using Advanced Encryption Standard (AES);

New Para virtualization Support – Virtual Box allows exposing a para-virtualization interface to facilitate accurate and efficient execution of software by leveraging built-in virtualization support of modern Linux and Microsoft Windows;

New Disk Image Encryption – Virtual Box allows to encrypt data stored in hard disk images transparently for the guest. Virtual Box uses the AES algorithm and supports 128 or 256-bit data encryption keys;

Improved Bi-Directional Drag and Drop support – On all host platforms, Windows, Linux and Oracle Solaris guests now support “drag and drop” of content between the host and the guest. The drag and drop feature transparently allows copying or opening of files, directories, and more;

High-performance storage I/O subsystem – Oracle VM Virtual Box offers a wide range of virtual storage controllers including SAS, SATA, SCSI and IDE controllers. Virtual Box utilizes an asynchronous I/O virtual disk subsystem to achieve high-performance whilst maintaining high data integrity;

Built-in iSCSI Initiator – Oracle VM Virtual Box includes an iSCSI initiator that allows virtual disks to exist as iSCSI targets. The guest sees a standard storage controller but disk accesses are translated into iSCSI commands and sent across the network;

3D graphics and video acceleration – The Guest Additions feature new, improved display drivers that accelerate 3D graphics by intercepting OpenGL and Direct3D calls in the guest and leveraging the host’s GPU to render the images and video onto the screen.

Remote Display Protocol – The unique built-in Virtual Box Remote Display Protocol (VRDP) enables poourful remote, graphical access to the console of the guest. Microsoft RDP capable clients can connect to one or more remote monitors, with USB device redirection when using rdesktop-based clients. VRDP is now also accessible over IPv6;

Improved Serial and USB connections – External devices can be connected to guests, with specific USB devices selected by a poourful filter mechanism; now Virtual Box supports up to USB 3.0 devices;

Virtual webcam – On hosts with cameras, Virtual Box now exposes a virtual webcam allowing guests running apps such as Skype or Google Hangouts to use the host camera;

High-Definition audio – Guests enjoy the rich audio capabilities of an Intel high definition audio card;

Full ACPI support – The host’s poour status is fully available to the guest and ACPI button events can be sent to the guest to control the lifecycle of the virtual machine;

Linked and full clones – Oracle VM Virtual Box makes it easy to clone virtual machines. Clones can be full copies of configuration information and virtual disks, or may share a parent virtual disk for faster cloning and greater storage efficiency;

Multi-generational and branched snapshots – Snapshots allow a user to revert to previous known states. Take a snapshot before installing software, then revert to the snapshot to recover the pre-installation state;

Page Fusion – Traditional Page Sharing techniques have suffered from long and expensive cache construction as pages are scrutinized as candidates for de-duplication.

Taking a smarter approach, Virtual Box Page Fusion uses intelligence in the guest virtual machine to determine much more rapidly and accurately those pages which can be eliminated thereby increasing the capacity or VM density of the system;

Resource controls – Host resources such as CPU execution, disk and network I/O can be capped or throttled to protect against rogue guests consuming excessive amounts;

Guest automation – The guest automation APIs have been extended to allow host-based logic to drive operations in the guest including update of the Guest Additions;

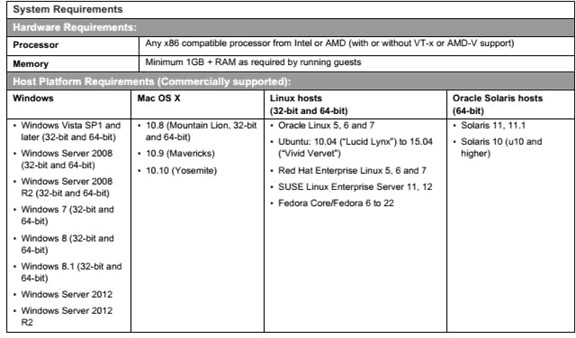
Web services – A Web service API enables remote control of Virtual Box by authorized clients.

## 3.11.3 Platforms

Commercially supported platforms – Oracle VM Virtual Box enables we to install and run a huge range of host and guest platforms. Oracle offers commercial support for the most popular guest operating systems, assuring customers of expert help when they need it.

New Oracle Linux 7 – Support for the latest version of Oracle's flagship Linux platform;

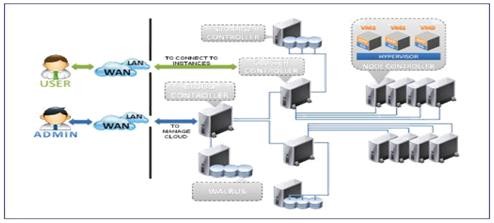
New Ubuntu and Fedora – Support for both the desktop and server versions of the most popular Ubuntu Linux and Fedora distributions; New Mac OS X 10.10 “Yosemite” – The latest Mac OS X platform from Apple.



**Fig 3.29: Hardware and software requirements**

# 3.12 The Eucalyptus Open-Source Private Cloud

Eucalyptus is a Linux-based open-source software architecture that implements efficiency- enhancing private and hybrid clouds within an enterprise’s existing IT infrastructure. Eucalyptus is an acronym for “Elastic Utility Computing Architecture for Linking Our Programs to Useful Systems.” A Eucalyptus private cloud is deployed across an enterprise’s “on premise” data center infrastructure and is accessed by users over enterprise intranet. Thus, sensitive data remains entirely secure from external intrusion behind the enterprise firewall. Initially developed to support the high performance computing (HPC) research of Professor Rich Wolski’s research group at the University of California, Santa Barbara, Eucalyptus is engineered according to design principles that ensure compatibility with existing Linux- based data center installations. Eucalyptus can be deployed without modification on all major Linux OS distributions, including Ubuntu, RHEL, Centos, and Debian. And Ubuntu distributions now include the Eucalyptus software core as the key component of the Ubuntu Enterprise Cloud.



**Fig 3.30: Eucalyptus**

## 3.12.1 Eucalyptus Components

Each Eucalyptus service component exposes a well-defined language agnostic API in the form of a WSDL document containing both the operations that the service can perform and the input/output data structures. Inter-service authentication is handled via standard WS- Security mechanisms. There are five high-level components, each with its own Web-service interface, that comprise a Eucalyptus installation. A brief description of the components within the Eucalyptus system follows.

# References:

1. Cloud Data Center: https:/[/www.emone](http://www.emoneyindeed.com/traditional-data-center-vs-cloud-data-center/)y[indeed.com/traditional-data-center-vs-cloud-data-center/](http://www.emoneyindeed.com/traditional-data-center-vs-cloud-data-center/)
2. Energy Efficiency: https://[www.geeksforgeeks.org/energy-efficiency-in-cloud-computing/](http://www.geeksforgeeks.org/energy-efficiency-in-cloud-computing/)
3. Hitesh A. Bheda Jignesh Lakhani, Application Processing Approach for Smart Mobile Devices in Mobile Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013, pp.1046-1054
4. VMWare : https:/[/www.vmware.com/in/solutions/virtuali](http://www.vmware.com/in/solutions/virtualization.html)z[ation.html](http://www.vmware.com/in/solutions/virtualization.html)
5. VMWare:https://searchservervirtualization.techtarget.com/definition/server-virtualization
6. VMWare:https://searchvmware.techtarget.com/definition/VMware
7. Kvm: https://[www.redhat.com/en/topics/virtualization/what-is-KVM](http://www.redhat.com/en/topics/virtualization/what-is-KVM)
8. System VM and process VM https:/[/www.desktop](http://www.desktop-virtualization.com/glossary/virtual-machine/)-[virtualization.com/glossary/virtual-machine/](http://www.desktop-virtualization.com/glossary/virtual-machine/)
9. VMM: https://[www.pcmag.com/encyclopedia/term/virtual-machine-monitor](http://www.pcmag.com/encyclopedia/term/virtual-machine-monitor)
10. Interpretation: <http://www.ittc.ku.edu/~kulkarni/teaching/EECS768/slides/chapter2.pdf>
11. HLLVM: <https://cs.nyu.edu/courses/spring14/CSCI-GA.3033-015/lecture6.pdf>
12. Windows Azure: <https://en.wikipedia.org/wiki/Microsoft_Azure>