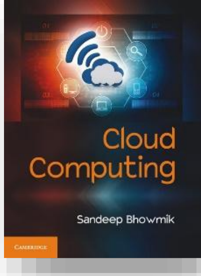
Cloud Computing

Sandeep Bhowmik

Chapter 7

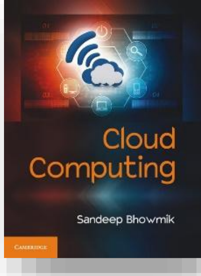
Resource Virtualization

Cambridge University Press



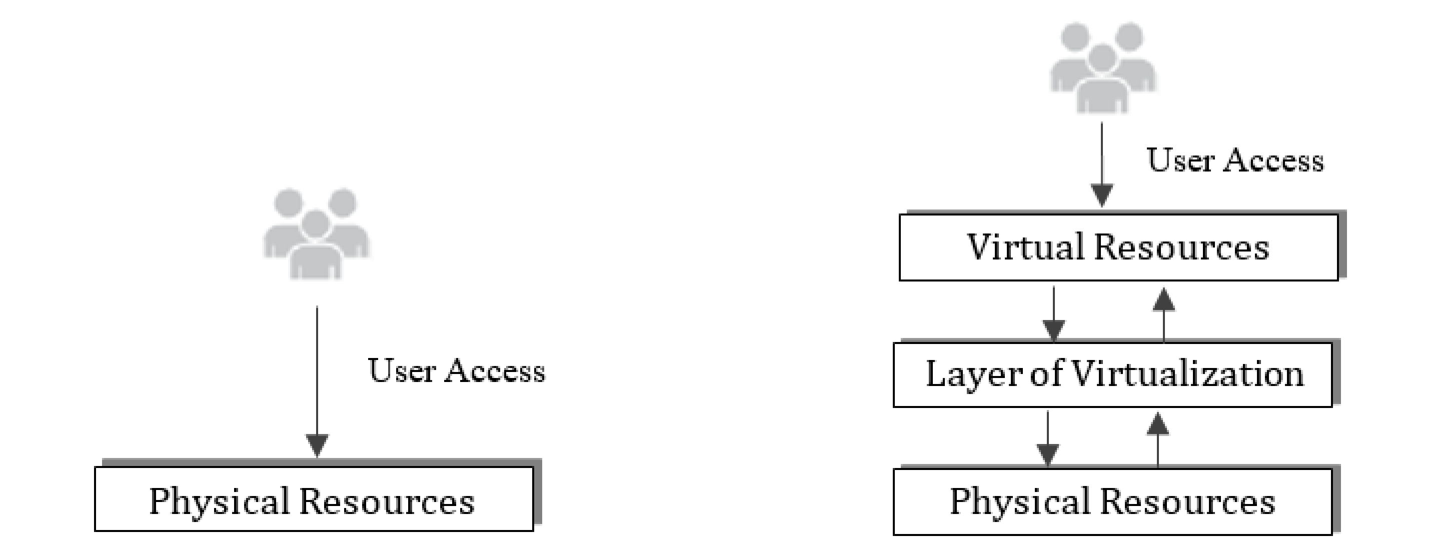
What Is Virtualization

- Virtualization refers to the representation of physical computing resources in simulated form made through software.
- This special layer of software (installed over active physical machines) is referred as layer of virtualization.
- Virtualization decouples the physical computing resources from direct access of users.



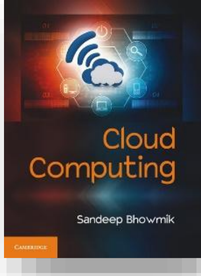
What Is Virtualization

- Users' interaction with computer in traditional and virtualized computing environment -



Traditional Computing Environment

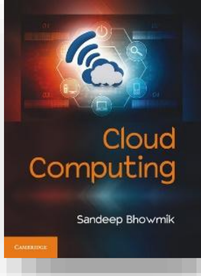
Virtualized Computing Environment



Virtualizing Physical Computing Resources

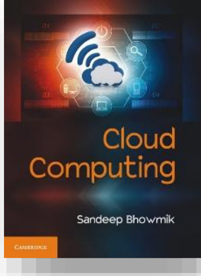
- Any kind of computing resources can be virtualized.
  - Processor
  - Memory
  - Storage
  - Network devices (like switch, router etc.)
  - Communication links
  - Peripheral devices (like keyboard, mouse, printer etc.)

- Virtualization decouples the physical computing resources from direct access of users.

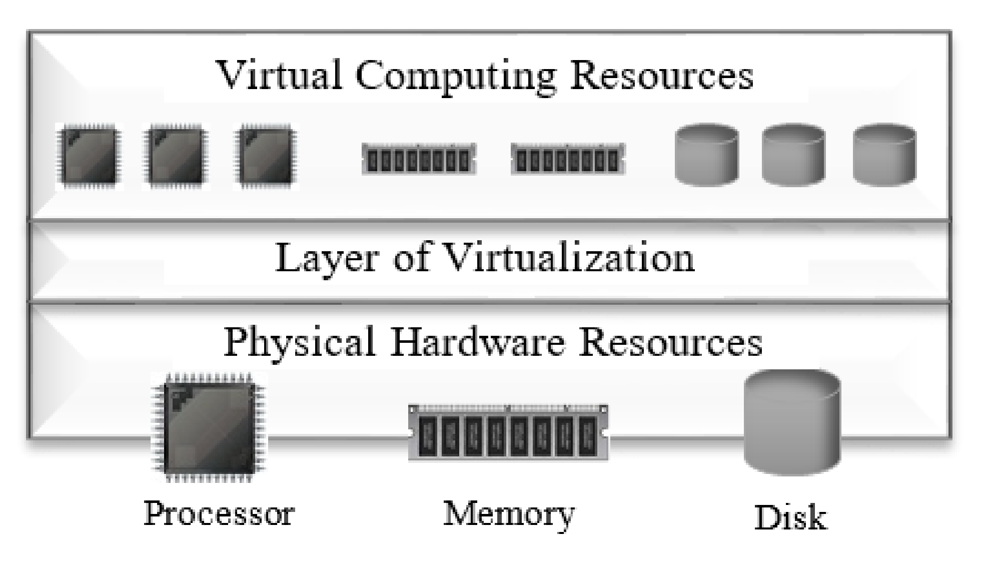


What Is Virtualization

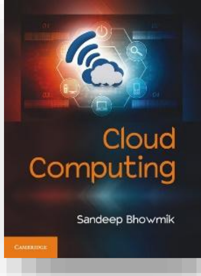
- A virtualized component can be operational when a physical resource empowers it from backend.
- The layer of virtualization transforms the physical computing devices into virtual form and presents them before user.
- The simulated devices produced through virtualization may or may not resemble the actual physical components in
    - Quality
    - Architecture
    - Quantity



What Is Virtualization

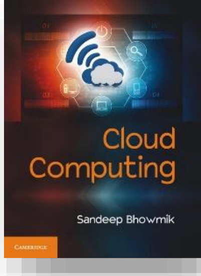


Virtualized computing environment comprising of processor, memory and storage disk.



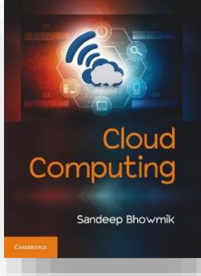
What Is Virtualization

- The software for virtualization consists of a set of control programs.
- It offers all the physical computing resources in custom made simulated (virtual) form.
- Virtual computers can be built using virtual computing resources produced by virtualization.



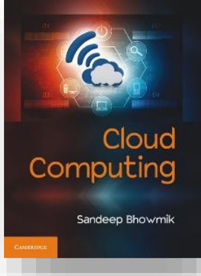
Understanding Abstraction

- The theory of virtualization is rooted around the idea of providing logical access to physical resources.
- Virtualization creates a layer of abstraction and masks physical resources from external access.
- Abstraction is the process of hiding the complex and non-essential characteristics of a system.
- Virtualization can be defined as the abstraction of different computing resources like processor, memory, storage, network.

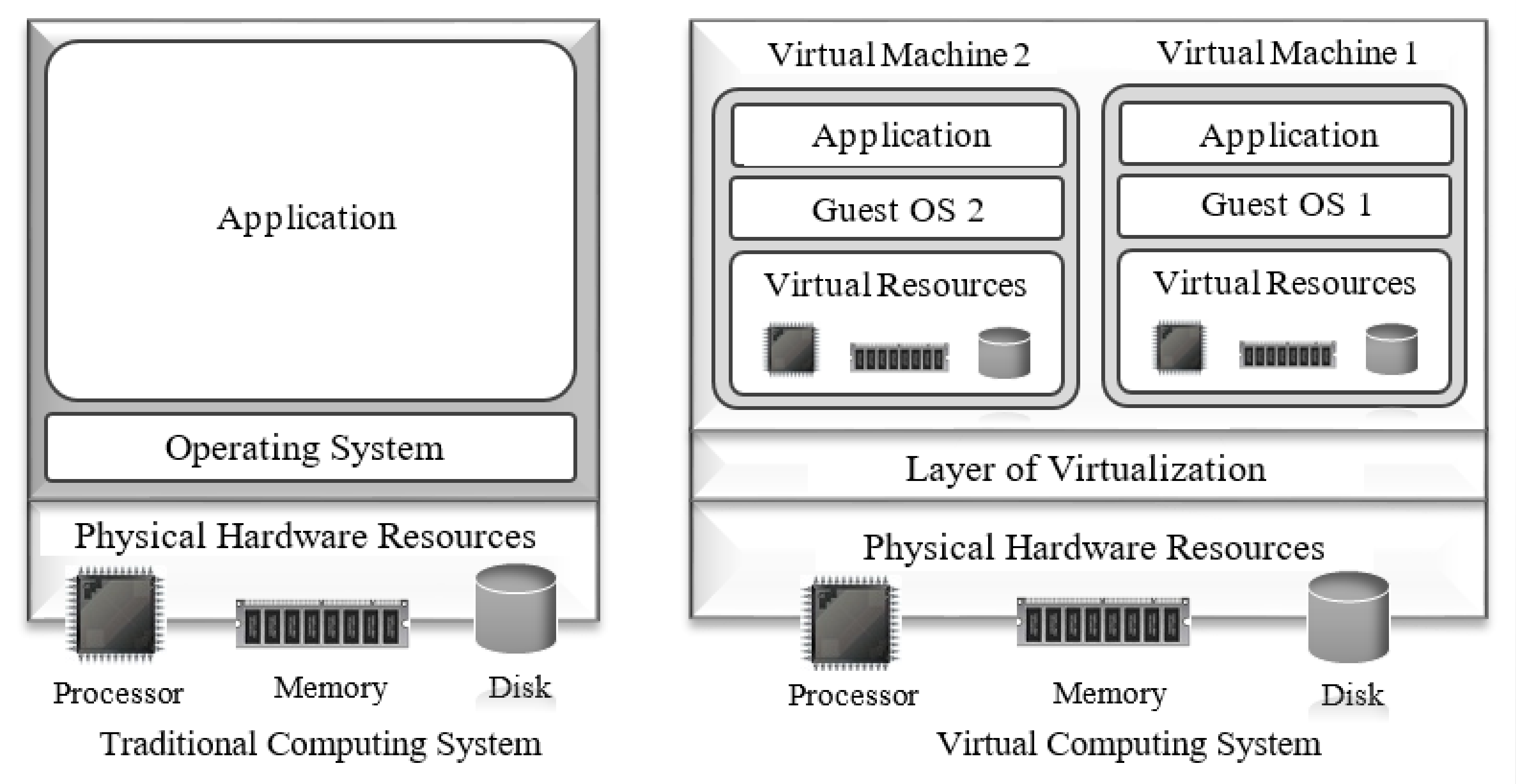


Machine or Server Level Virtualization

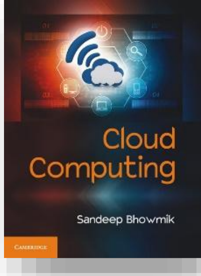
- It is the concept of creating virtual machine (that is, virtual computer) on actual physical machine.
- The parent system on which the virtual machines run is called the *host system*.
- The virtual machines are themselves referred as guest *systems*.
- Virtualized physical server can host multiple virtual machines, each one having different OS.



Machine or Server Level Virtualization



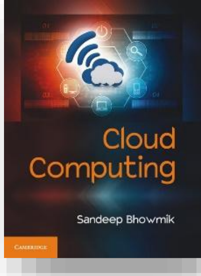
Conventional computing system vs. virtualized computing system.



Machine or Server Level Virtualization

- Comparison between non-virtualized and virtualized machine environment.

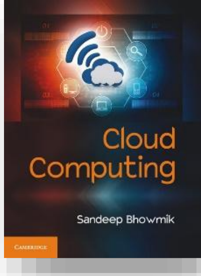
Non-Virtualized Machine Environment	Virtualized Machine Environment
At a moment, one single OS can run on a physical machine.	Multiple OS can run simultaneously on one physical machine.
Application and hardware system remain tightly coupled.	Virtual Machines isolates applications from the underlying hardware.
Resources utilization rate is low in most of the times.	Resource utilization improves as multiple VMs share same set of physical resources.



Machine or Server Level Virtualization

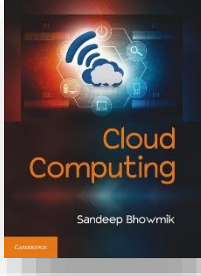
- Comparison between non-virtualized and virtualized machine environment (contd.).

Non-Virtualized Machine Environment	Virtualized Machine Environment
Increases cost of business due to low resource utilization.	Cost effective if planned properly.
Inflexible approach.	Provides lot of flexibility to system designers.



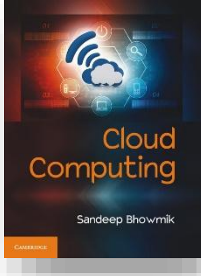
The Layer of Virtualization

- Virtual machines are created over the virtualization layer.
- This layer provides the system resources' access to the virtual machines.
- This software layer is referred as the *Hypervisor* or *Virtual Machine Monitor (VMM)*.
- The hypervisor abstracts the underlying software and/or hardware environments and represents virtual system resources to its users.



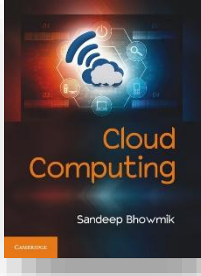
Machine Virtualization Techniques

- There are two different techniques of server or machine virtualization -
  - Hosted approach
  - Bare metal approach.
- The techniques differ depending on the type of hypervisor used.

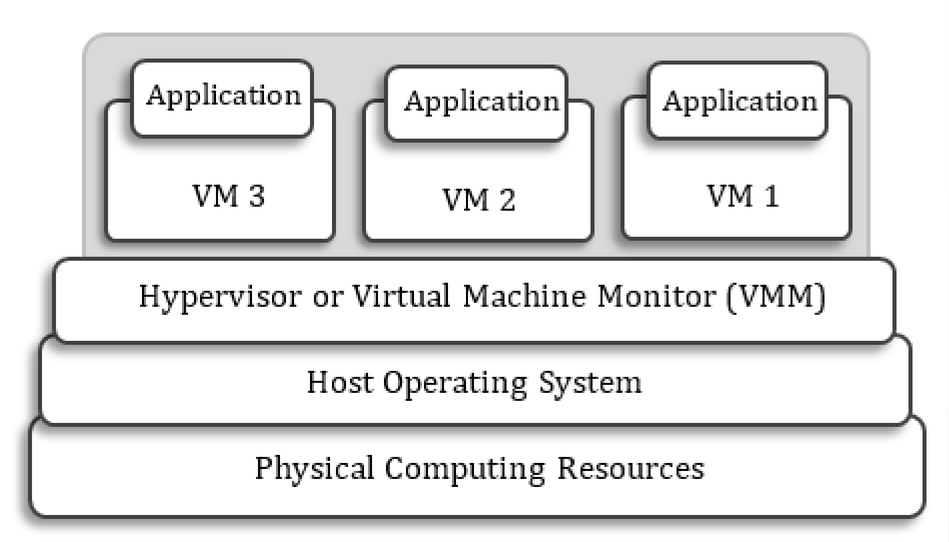


Hosted Approach

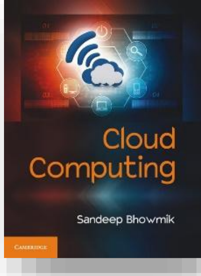
- In this approach, an operating system is first installed on the physical machine to activate it.
- This OS installed over the host machine is referred as *host operating system*.
- The hypervisor is then installed over this host OS.
- This type of hypervisor is referred to as *Type 2 hypervisor* or *Hosted hypervisor*.



Hosted Approach


Application
Application
Application
VM 3
VM 2
VM 1
Hypervisor or Virtual Machine Monitor (VMM)
Host Operating System
Physical Computing Resources

A model of hosted machine virtualization approach.

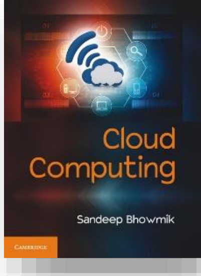


Hosted Approach

- **Benefits**

- In this approach the host OS supplies the hardware drivers for the underlying physical resources.

- This eases the installation and configuration of the hypervisor. It makes the type-2 hypervisors compatible for a wide variety of hardware platform.

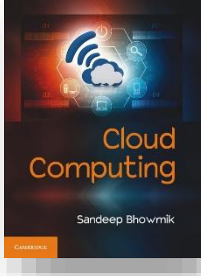


Hosted Approach

- **Drawbacks**

- A hosted hypervisor does not have direct access to the hardware resources. This may degrade the performance of the virtual machines.

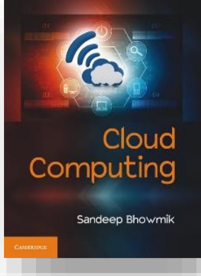
- Since the underlying host OS controls the scheduling of jobs, it becomes unrealistic to run a real-time OS inside a VM using hosted virtualization.



Hosted Approach

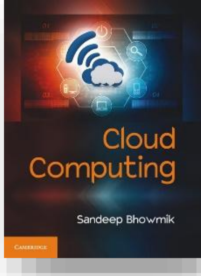
- **Example**

- Hosted Approach
- Microsoft Virtual PC

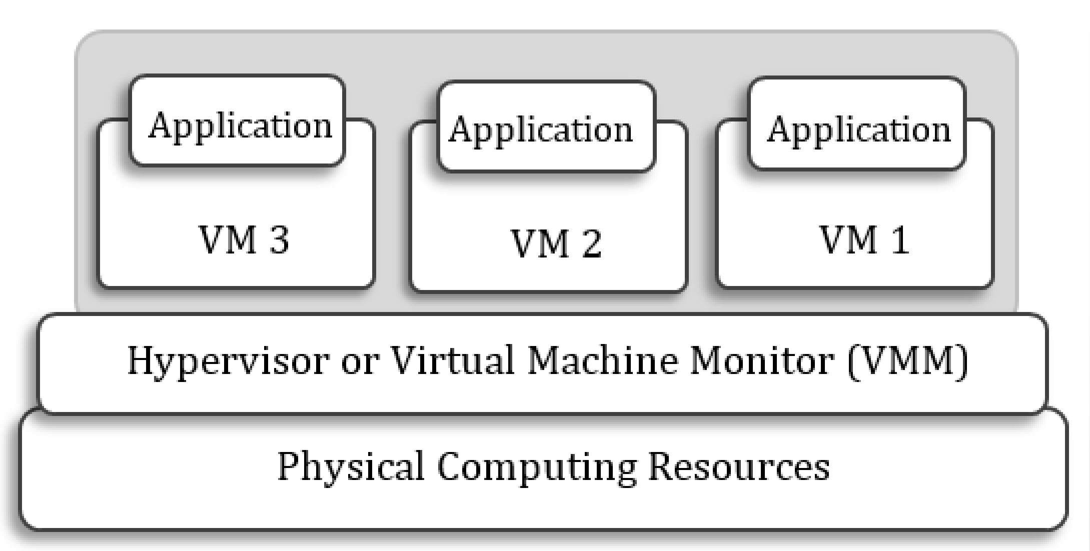


Bare Metal Approach: Removal of the host OS

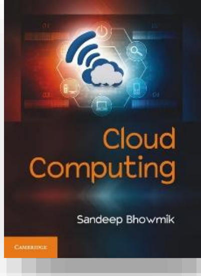
- In this approach of machine virtualization, the hypervisor is directly installed over the physical machine.
- Since, the hypervisor is the first layer over hardware resources hence, the technique is referred as bare metal approach.
- Here the VMM or the hypervisor communicates directly with system hardware.
- The hypervisor acts as low-level virtual machine monitor and also called *Type 1 Hypervisor* or *Native Hypervisor*.



Bare Metal Approach: Removal of the host OS


Application
VM 3
Application
VM 2
Application
VM 1
Hypervisor or Virtual Machine Monitor (VMM)
Physical Computing Resources

A model for the bare metal approach of machine virtualization.

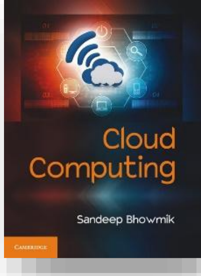


Bare Metal Approach: Removal of the host OS

- **Benefits**

- Since the bare metal hypervisor can directly access the hardware resources, in most of the cases it provides better performance.

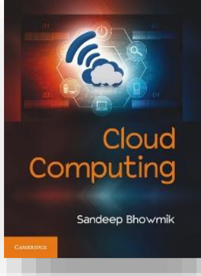
- Administrators get more control over the host environment.



Bare Metal Approach: Removal of the host OS

- **Drawbacks**

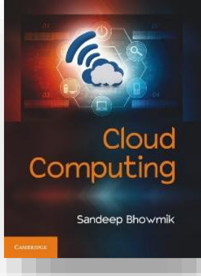
- As any hypervisor usually have limited set of device drivers built into it, so, bare metal hypervisors have limited hardware support and can't run on a wide variety of hardware platform.



Bare Metal Approach: Removal of the host OS

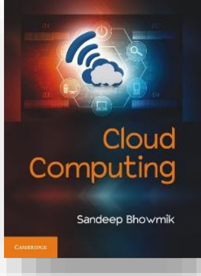
- **Example**

- VMware’s ESX
- VMware’s ESXi Servers
- Microsoft Hyper-V
- Open source solution Xen



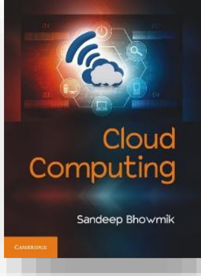
Hypervisor Based Virtualization Approaches

- Hypervisor based virtualization techniques can be divided into three categories –
    - Full virtualization,
    - Paravirtualization,
    - Hardware assisted virtualization

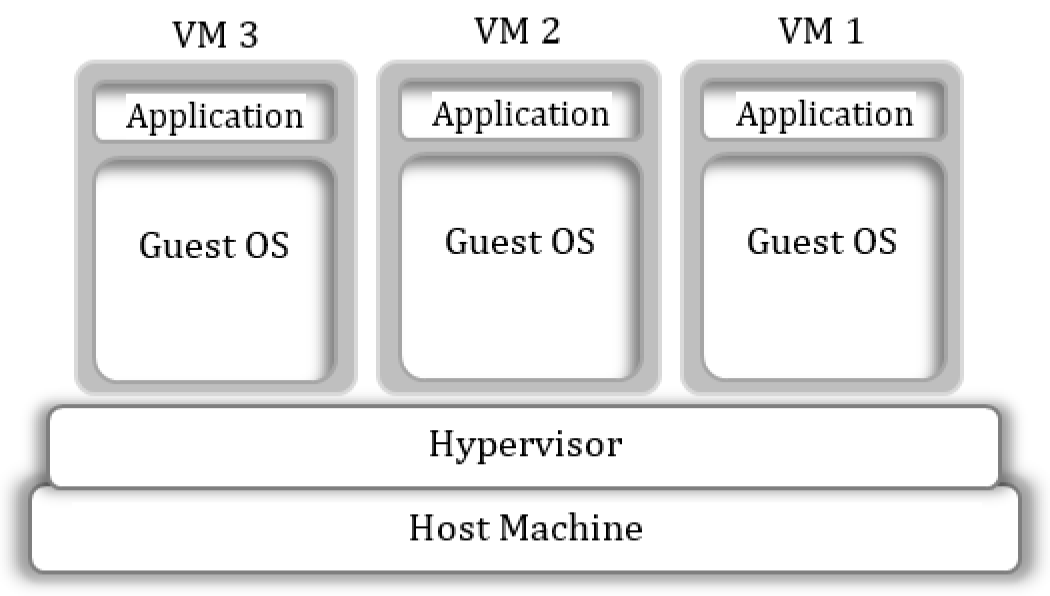


Full Virtualization

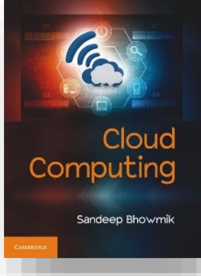
- In full virtualization, the hypervisor fully simulates or emulates the underlying hardware.
- The guest operating systems assume that they are running on actual physical resources.
- This enables the unmodified versions of available operating systems (like Windows, Linux) to run as guest OS over hypervisor.



Full Virtualization

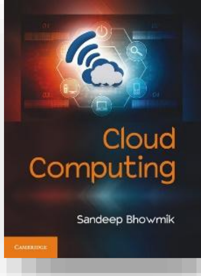


A model of full virtualization



Full Virtualization

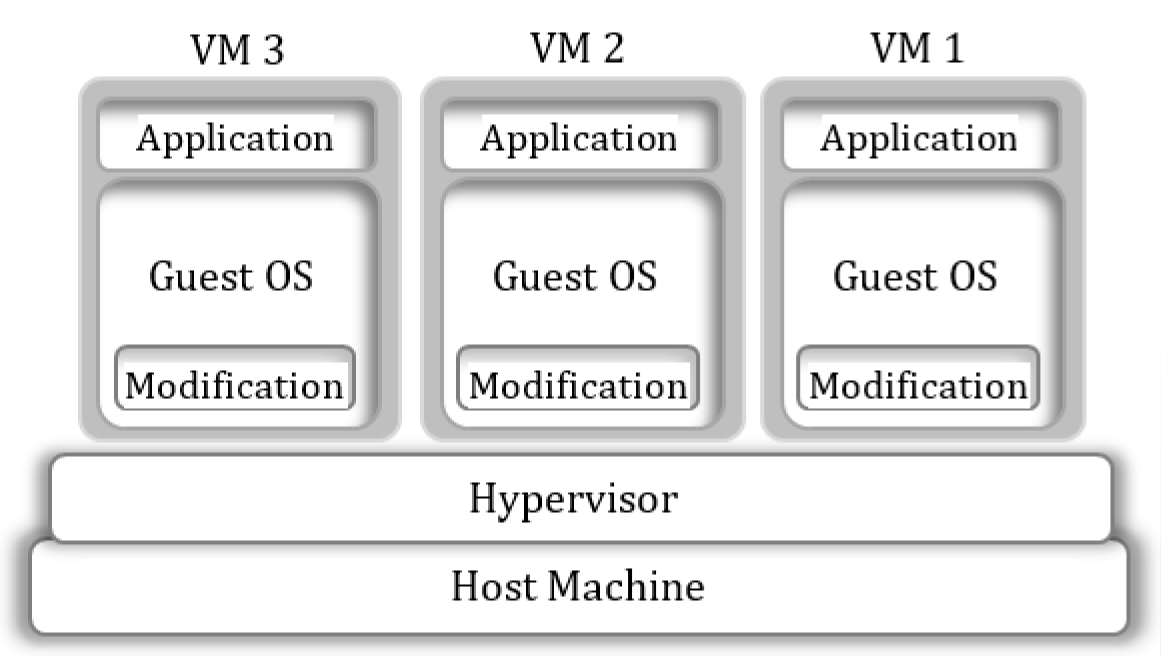
- The guest OS remains completely isolated from physical resource layer by the hypervisor.
- This provides flexibility, as almost all the available operating systems can work as guest OS.
- Full virtualization solution –
  - VMWare ESXi Server
  - Microsoft Virtual Server



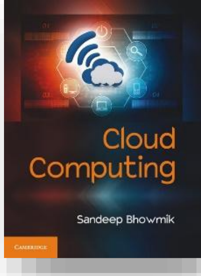
Paravirtualization or OS-assisted Virtualization

- “Para” is an English affix of Greek origin that means "beside" or "alongside.”
- A portion of the virtualization management task is transferred (from the hypervisor) towards the guest operating systems.
- Guest operating systems need special modification for this capability inclusion.
- This modification is called *porting*.

Paravirtualization or OS-assisted Virtualization

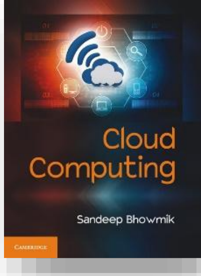


A model of paravirtualization



Paravirtualization or OS-assisted Virtualization

- Paravirtualization requires hypervisor specific modifications of guest operating systems.
- The unmodified versions of available operating systems (like Windows, Linux) can’t be used in paravirtualization.
- Since it involves modifications of the OS, paravirtualization is referred to as *OS-assisted Virtualization* also.
- Example of paravirtualization hypervisor is the open source Xen project.



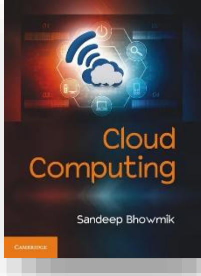
Paravirtualization or OS-assisted Virtualization

- **Advantages**

- Paravirtualization allows calls from guest OS to directly communicate with hypervisor.

- In paravirtualization the system is not restricted by the device drivers provided by the virtualization software layer.

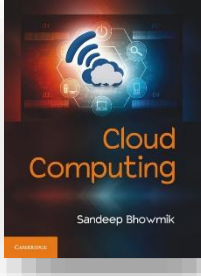
- Paravirtualization reduces the load of host machine and can run more number of VMs over a host machine in comparison to full virtualization.



Paravirtualization or OS-assisted Virtualization

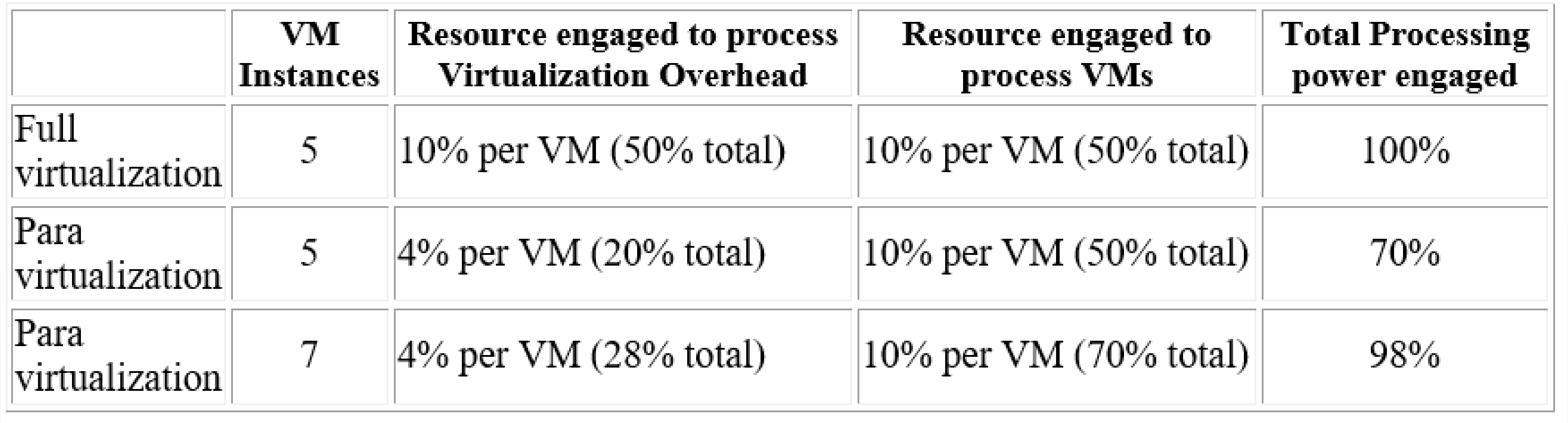
- **Limitations**
- Unmodified versions of available operating systems (like Windows, Linux) are not compatible with paravirtualization hypervisors.
- Security is compromised in this approach, as the guest OS has a comparatively more control of the underlying hardware.

Paravirtualization can provide enhanced virtualization performance at the cost of security.



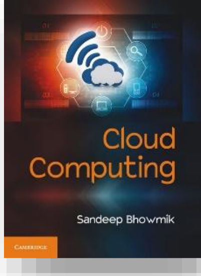
Full Virtualization vs. Paravirtualization

- A comparison between processing power utilization



	VM Instances	Resource engaged to process Virtualization Overhead	Resource engaged to process VMs	Total Processing power engaged
Full virtualization	5	10% per VM (50% total)	10% per VM (50% total)	100%
Para virtualization	5	4% per VM (20% total)	10% per VM (50% total)	70%
Para virtualization	7	4% per VM (28% total)	10% per VM (70% total)	98%

- Here it is assumed that, in a fully virtualized environment each guest machine consumes 10% of host machine’s processor power, whereas in paravirtualization they consume 4% of host machine’s processor power



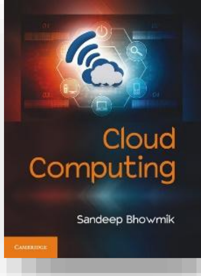
Hardware Assisted Virtualization

- Inspired by software enabled virtualization, hardware vendors later started manufacturing devices tailored to support virtualization.

- Intel and AMD started this by including new virtualization features in their processors.

- They allows some privileged CPU calls from the guest OS to be directly handled by the CPU.

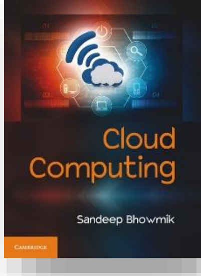
- Hypervisors like Xen, Microsoft’s Hyper-V or VMWare ESXi Server can take advantage of the hardware assisted virtualization.



A side-by-side Comparison

- Comparison between non-virtualized and virtualized machine environment.

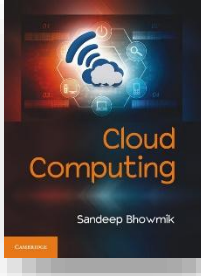
Full Virtualization	Paravirtualization or OS Assisted Virtualization	Hardware Assisted Virtualization
Guest OS has no role in virtualization.	Guest OS plays role in virtualization.	Guest OS has no role in virtualization.
Guest OS remains unaware about the virtualization.	Guest OS has to be aware about the virtualization.	Guest OS remains unaware about the virtualization.
Normal version of available OS can be used as guest OS.	Modified version of available OS is required.	Normal version of available OS can be used as guest OS.



A side-by-side Comparison

- Comparison between non-virtualized and virtualized machine environment.

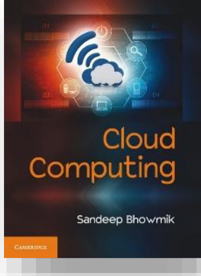
Full Virtualization	Paravirtualization or OS Assisted Virtualization	Hardware Assisted Virtualization
Provides good options for guest OS.	Provides lesser options for guest OS.	Provides good options for guest OS.
Guest OS is not hypervisor specific.	Guest OS is tailored to be hypervisor specific.	Guest OS is not hypervisor specific.
No special feature is required in the host CPU.	No special feature is required in the host CPU.	Requires explicit features in the host CPU.



A side-by-side Comparison

- Comparison between non-virtualized and virtualized machine environment.

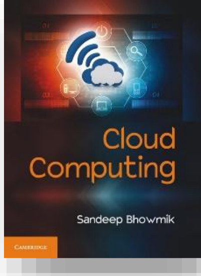
Full Virtualization	Paravirtualization or OS Assisted Virtualization	Hardware Assisted Virtualization
Hardware does not play role in virtualization.	Hardware does not play role in virtualization.	Hardware plays role in virtualization.
Hypervisor takes care of all the virtualization tasks.	Guest OS, along with hypervisor takes care of the virtualization tasks.	Specialized hardware device along with hypervisor takes care of virtualization tasks.
Virtualization overhead of hypervisor is more.	Virtualization overhead of hypervisor is less.	Virtualization overhead of hypervisor is less.



A side-by-side Comparison

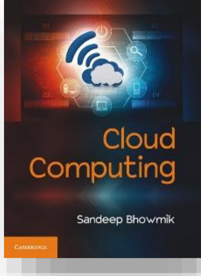
- Comparison between non-virtualized and virtualized machine environment.

Full Virtualization	Paravirtualization or OS Assisted Virtualization	Hardware Assisted Virtualization
Virtualization performance is little slow.	Virtualization performance is better.	Virtualization performance is better.
Provide high level of security as all virtualization controls remain with the hypervisor.	Security is compromised as guest OS has some control in virtualization.	Security is compromised as calls from guest OS can directly access the hardware.



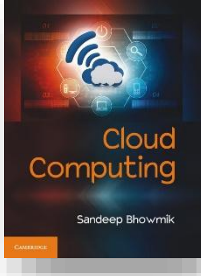
Threats to Hypervisor

- **Rogue Hypervisor**
- Hackers may create rogue hypervisor (hypervisor made with wrong intention) and can replace an original hypervisor with that one to attack a system.
- Rogue hypervisor may create cover channel for malware to attack the system.



Threats to Hypervisor

- **VM Escape**
- One advantage of running applications in virtual machine is that the applications as well as the users can't get direct access to the hypervisor or the host operating of the system.
- But, an improperly configured or manipulated virtual machine may allow codes to completely bypass this security.
- Such bypass is known as virtual machine escape, where the exploiter can directly access the hypervisor or host OS.

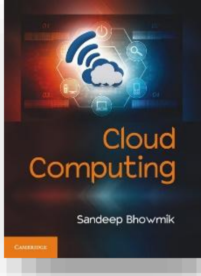


OS Level Virtualization: Removal of the hypervisor

- Here, no hypervisor is used, and the virtual servers are enabled by the operating system kernel of the physical machine.

- The kernel of the OS installed over physical system is shared among all the virtual servers those run over it.

- Since all virtual servers share a single kernel, it is evident that all of them will have same OS as the parent system.



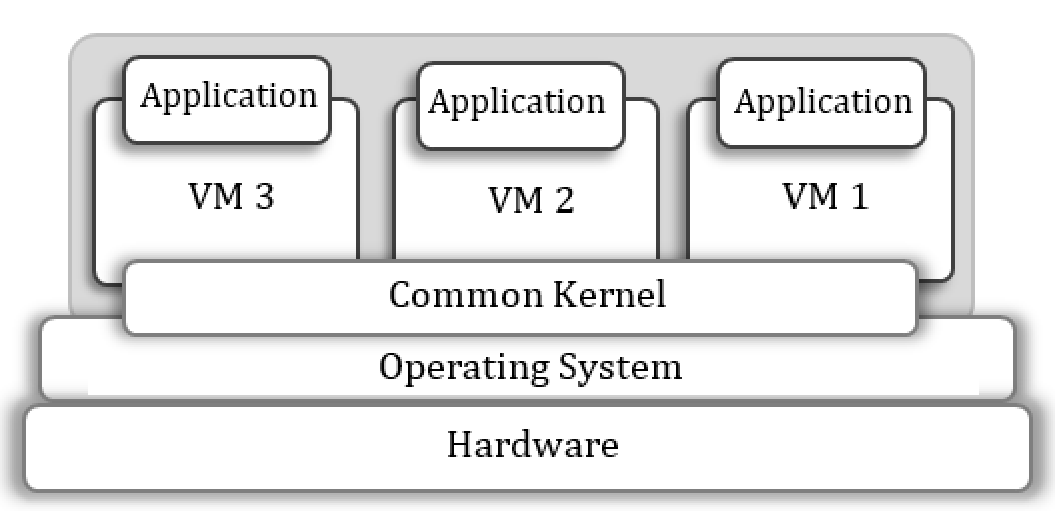
OS Level Virtualization: Removal of the hypervisor

- The goal of this approach is to create multiple logically distinct user space instances (virtual servers) over a single instance of an OS kernel.

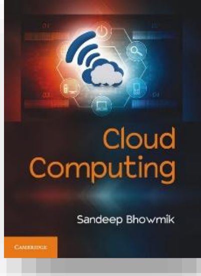
- This approach is also known as *Operating System Virtualization* or *Shared Kernel Approach*.

- Virtualization solutions such as FreeBSD’s jail, Linux VServer, OpenVZ are few examples of OS-level virtualization.

OS Level Virtualization: Removal of the hypervisor



A model of operating system level virtualization approach

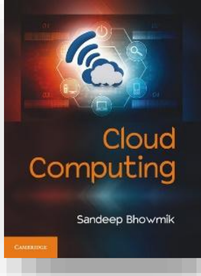


OS Level Virtualization: Removal of the hypervisor

- **Advantage**
- The advantage of OS level virtualization is that it is lighter in weight, since all the virtual servers share a single instance of an OS kernel.

- **Disadvantage**
- The advantage of OS level virtualization is that it is lighter in weight, since all the virtual servers share a single instance of an OS kernel.

OS level virtualization facilitates the creation of multiple logically distinct user space instances rather than complete VMs.

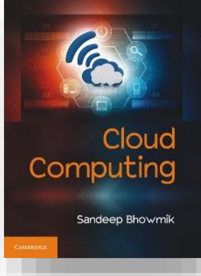


Major Server Virtualization Products & Vendors

- There are many enterprise level server virtualization products available in the market.

- A number of VMMs exist which are the basis of many cloud computing environments.

- Companies like VMware, Citrix and Microsoft are among the leading vendors of server virtualization products.



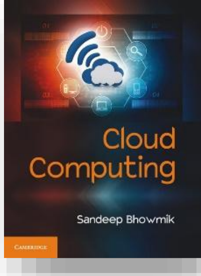
Major Server Virtualization Products & Vendors

- **VMware vSphere**

- VMware is a pioneer in the virtualization market, especially in server and desktop virtualization.

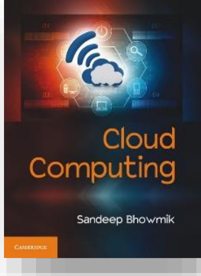
- This hypervisor is Type 1 or bare-metal hypervisor.

- vSphere uses ESXi hypervisor, which is also a product of VMware.



Major Server Virtualization Products & Vendors

- **Citrix XenServer**
- It is one among the leading open source server virtualization solution.
- Xen originated as an open source research project at the University of Cambridge, and first release was made in 2003.
- Xen hypervisor, which has pioneered the paravirtualization concept, is the basis of XenServer.



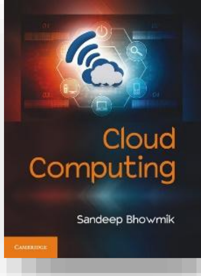
Major Server Virtualization Products & Vendors

- **Microsoft Hyper-V**

- It is a server virtualization solution from Microsoft.
- It was First launched in 2008.

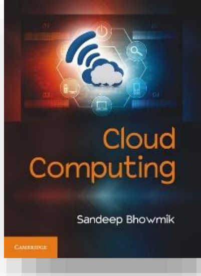
- **Oracle VM VirtualBox**

- The virtualization software package from Oracle Corporation.
- It is a Xen hypervisor based open source product.



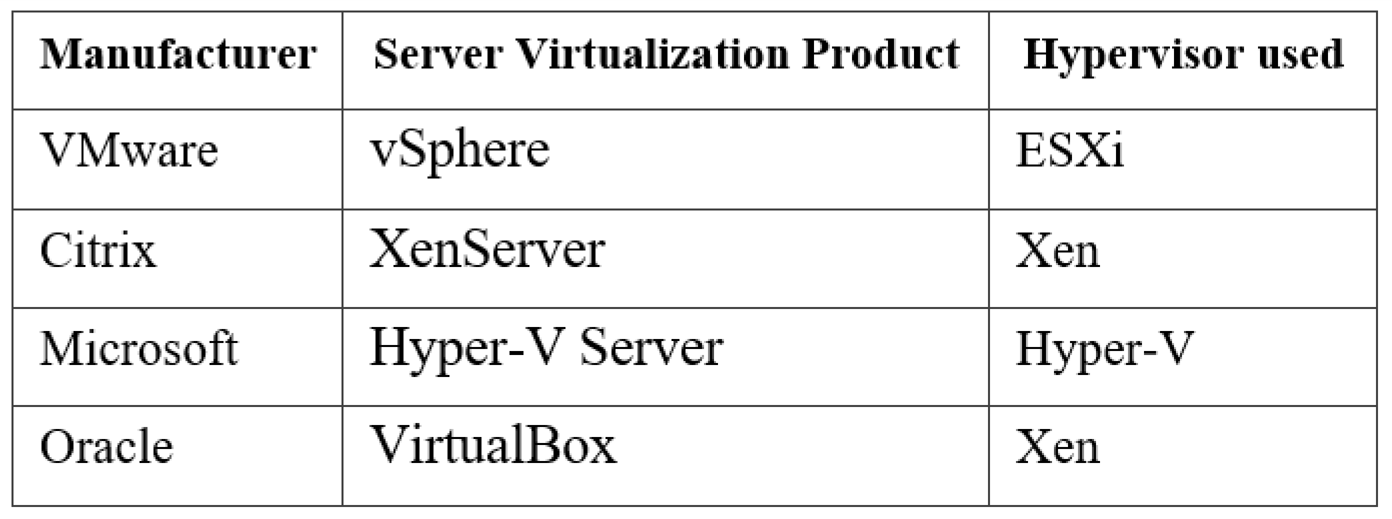
Major Server Virtualization Products & Vendors

- **Kernel-based virtual machine (KVM)**
- KVM is a hypervisor built into the Linux kernel.
- This open source solution was developed by Red Hat Corporation.
- A wide variety of guest operating systems work with KVM including several versions of Windows, Linux, and UNIX.

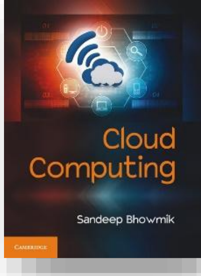


Major Server Virtualization Products & Vendors

- Server virtualization products and corresponding hypervisors .

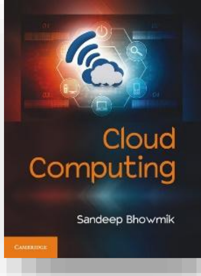


Manufacturer	Server Virtualization Product	Hypervisor used
VMware	vSphere	ESXi
Citrix	XenServer	Xen
Microsoft	Hyper-V Server	Hyper-V
Oracle	VirtualBox	Xen



High-Level Language Virtual Machine

- This concept goes against the idea of conventional computing environment, where a compiled application is firmly tied to a particular OS and architecture.
- It eases the porting of compiler by rendering HLLs to intermediate representation targeted towards abstract machines.
- The abstract machine then translates the intermediate code to physical machine’s instruction set.
- Such abstract machine is referred as high-level language VM or *HLL VM*.



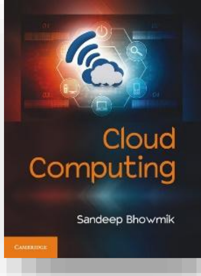
High-Level Language Virtual Machine

- Java Virtual Machine (JVM) or Microsoft's Common Language Run-time (CLR) are examples of high-level language VMs.

- High-level language VM is also known as *application VM* or *process VM*.

- Application or process virtualization can be considered as the smaller version of machine virtualization.

- Virtual machines designed to run only a single application or process written in high level language are referred to as HLL VM.

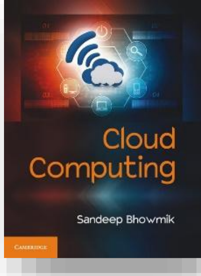


Emulation

- Emulation in computing is done by making one system imitate another.

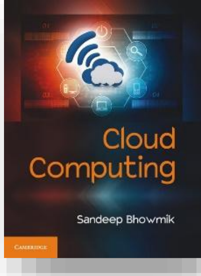
- Emulation software converts binary data written for execution on one machine to an equivalent binary form suitable for execution on another machine.

- There are two ways for implementation of emulations –
  - Interpretation
  - binary translation



Emulation

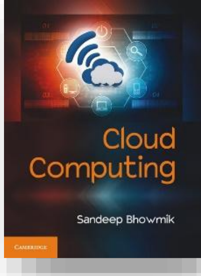
- In binary translation, it recompiles the whole instruction into another binary form.
- In interpretation, each instruction is interpreted by the emulator every time it is encountered.
- Interpretation is easier to implement, but slower than binary translation process.



Simple Virtualization vs. Emulation based Virtualization

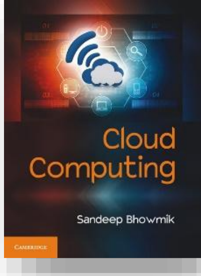
- Both can enable multiple virtual machines with different guest operating systems to run on single physical (or host) system.

- The key difference between the two is -
- whether applications running on the virtual machines are compiled for the native instruction set of the host machine
- or,
- they have been compiled for some other architecture and instruction set



Simple Virtualization vs. Emulation based Virtualization

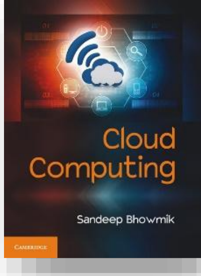
- In emulation, the main focus of a system is to pretend to be another system.
- In simple virtualization the focus is to simulate the environment of native system into two or more duplicate systems.
- Microsoft’s VirtualPC is example of an emulation based virtual machine.



Some Other Type of Virtualizations

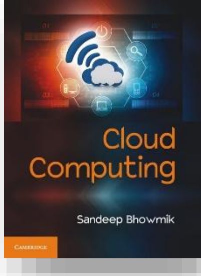
- Virtualization of computing infrastructure is not only about machine or server virtualization. There are many other types also.

- Network Virtualization
    - Virtual device based virtual network
    - Protocol based virtual network
- Storage Virtualization
    - Google Cloud Storage, Microsoft Azure Storage, Amazon Simple Storage System (S3), Amazon Elastic Block Store (EBS).
- Desktop Virtualization
    - It does not fall under the core category of computing infrastructure virtualization concept. But it is key to business.



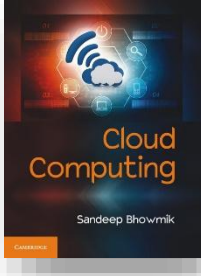
Advantages of Virtualization

- Better utilization of existing resources
- Reduction in hardware cost
- Reduction in computing infrastructure costs
- Improved fault tolerance or Zero downtime maintenance
- Simplified system administration
- Simplified capacity expansion
- Simplified system installation
- Support for legacy systems and applications
- Simplified system-level development
- Simplified system and application testing
- Security



Advantages of Virtualization

- The benefits of virtualization directly propagates into cloud computing and have empowered it.

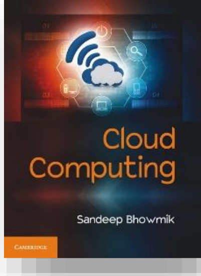


Downsides of Virtualization

- Every technology has its own shortcomings and virtualization is no exception.

- The area of concerns are -
  - Single point of failure problem
  - Lower performance issue
  - Difficulty in root cause analysis

- However, the positive effects of virtualization outweigh the negatives by far.

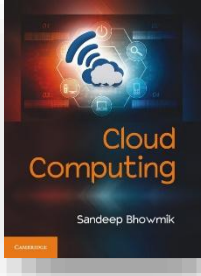


Virtualization Security Threats

- The traditional threats of any computing system are all applicable to virtual computing system also.

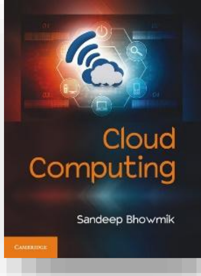
- Additional security threats to virtualized system include -
  - The single point host
  - Threats to hypervisor
  - Complex configuration
  - Privilege escalation
  - Inactive virtual machines
  - Consolidation of different trust zones

- However, Any virtualization threats can be mitigated by maintaining security recommendations while designing a computing system.



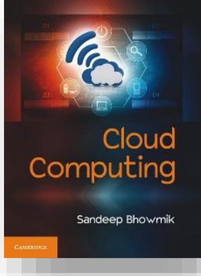
Virtualization Security Recommendations

- Hardening virtual machines
- Hardening the hypervisor
- Hardening the host operating system
- Restrictive physical access to the host
- Implementation of single primary function per VM
- Use of secured communications
- Use of separate NIC for sensitive VM



Virtualization and Cloud Computing

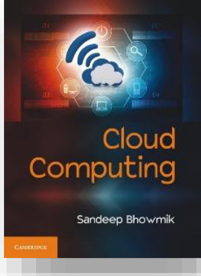
- Resource pooling is one important feature of cloud computing.
- But consumers of cloud services are given access to virtualized pool of resources.
- This way all resources at cloud data center are virtualized and it is referred as data center virtualization.
- Data center virtualization is one foundation of cloud computing.



Virtualization and Cloud Computing

- Virtualization is considered as a major step in the direction of cloud computing.

- Virtualization is the key enabler of most of the fundamental attributes of cloud computing, like
  - Shared service
  - Elasticity
  - Service orientation
  - Metered usage



Thank You