CE644 Cloud Computing and Applications

- Virtualization is an enabling technology for the different cloud computing services.
- It helps to improve scalability and resource utilization of the underlying infrastructure.
- It also enables the IT personnel to perform the administration task easier.
- With the help of resource sharing, the hypervisor supports the green IT services. The virtualization reduces the huge amount invested in buying additional resources
- To increase the resource utilization and ROI, the companies started using the technology called *virtualization* where a single physical infrastructure can be used to run multiple operating systems (OSs) and applications
- It enables the single physical infrastructure to function as a multiple logical infrastructure or resources.
- It is not only limited to the hardware, it can take many forms such as memory, processor, I/O, network, OS, data, and application.

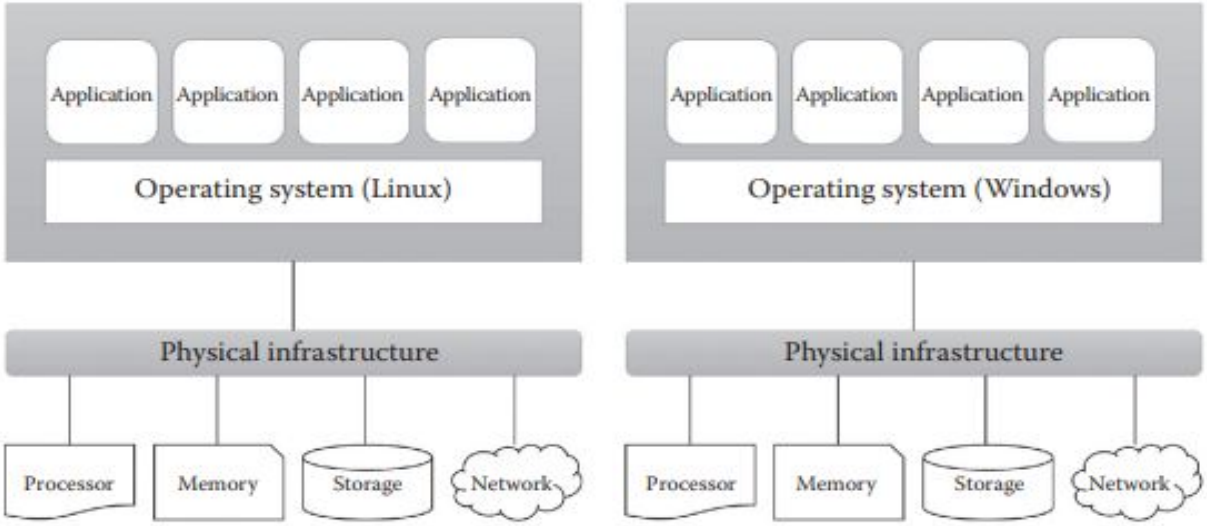

FIGURE 7.1
Before virtualization.

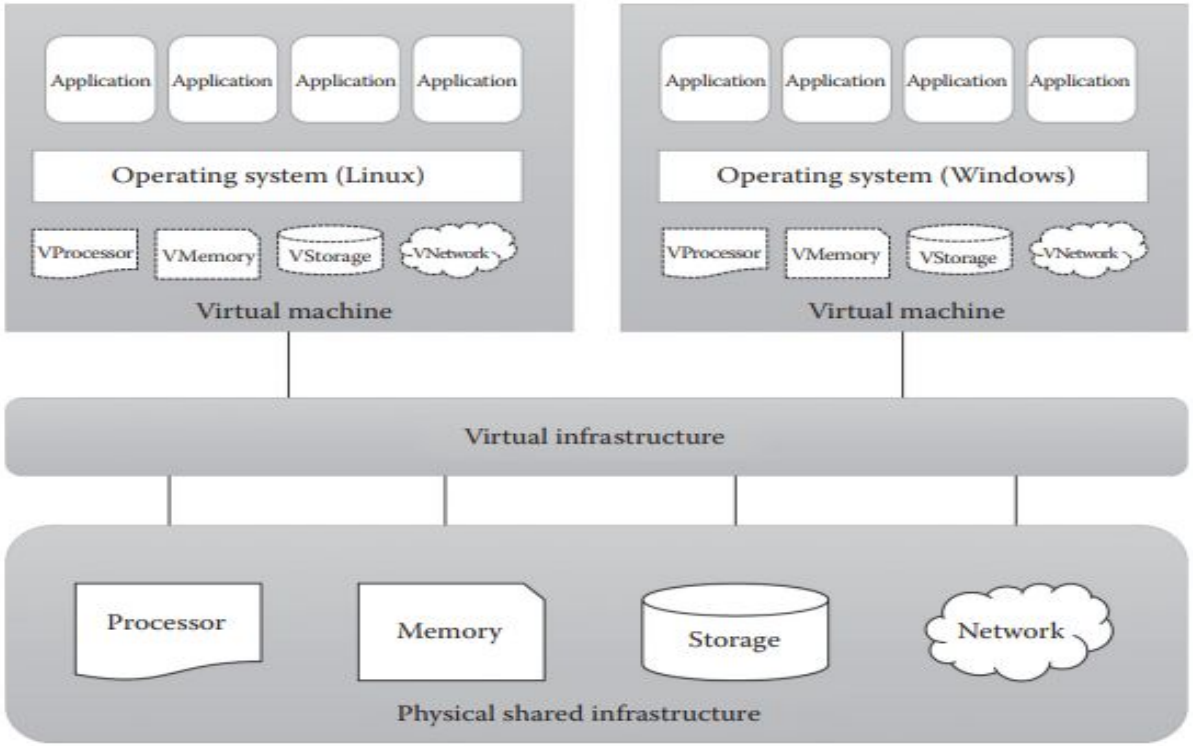

FIGURE 7.2
After virtualization.

Role of virtualization in enabling cloud

- Virtualization is the underlying core technology of cloud computing
- Advantages
- Using virtualization, the physical infrastructure owned by the service provider is shared among many users, **increasing the resource utilization**.
- Virtualization provides **efficient resource utilization** and **increased return on investment** (ROI).
- Ultimately, it results in **low capital expenditures** (CapEx) and **operational expenditures** (OpEx).
- Promotes the green IT by reducing energy wastage.
- Dynamic data center
- Improves disaster recovery

- Disadvantages
- Single point of failure
- Demands high-end and powerful infrastructure
- May lead to lower performance
- Requires specialized skill set

Virtualization Opportunities

- Virtualization is the process of abstracting the physical resources to the pool of virtual resources that can be given to any virtual machines (VMs).
- The different resources like memory, processors, storage, and network can be virtualized using proper virtualization technologies.

Processor Virtualization

- allows the VMs to share the virtual processors that are abstracted from the physical processors available at the underlying infrastructure.
- The virtualization layer abstracts the physical processor to the pool of virtual processors that is shared by the VMs.
- The virtualization layer will be normally any hypervisors.
- But processor virtualization can also be achieved from distributed servers

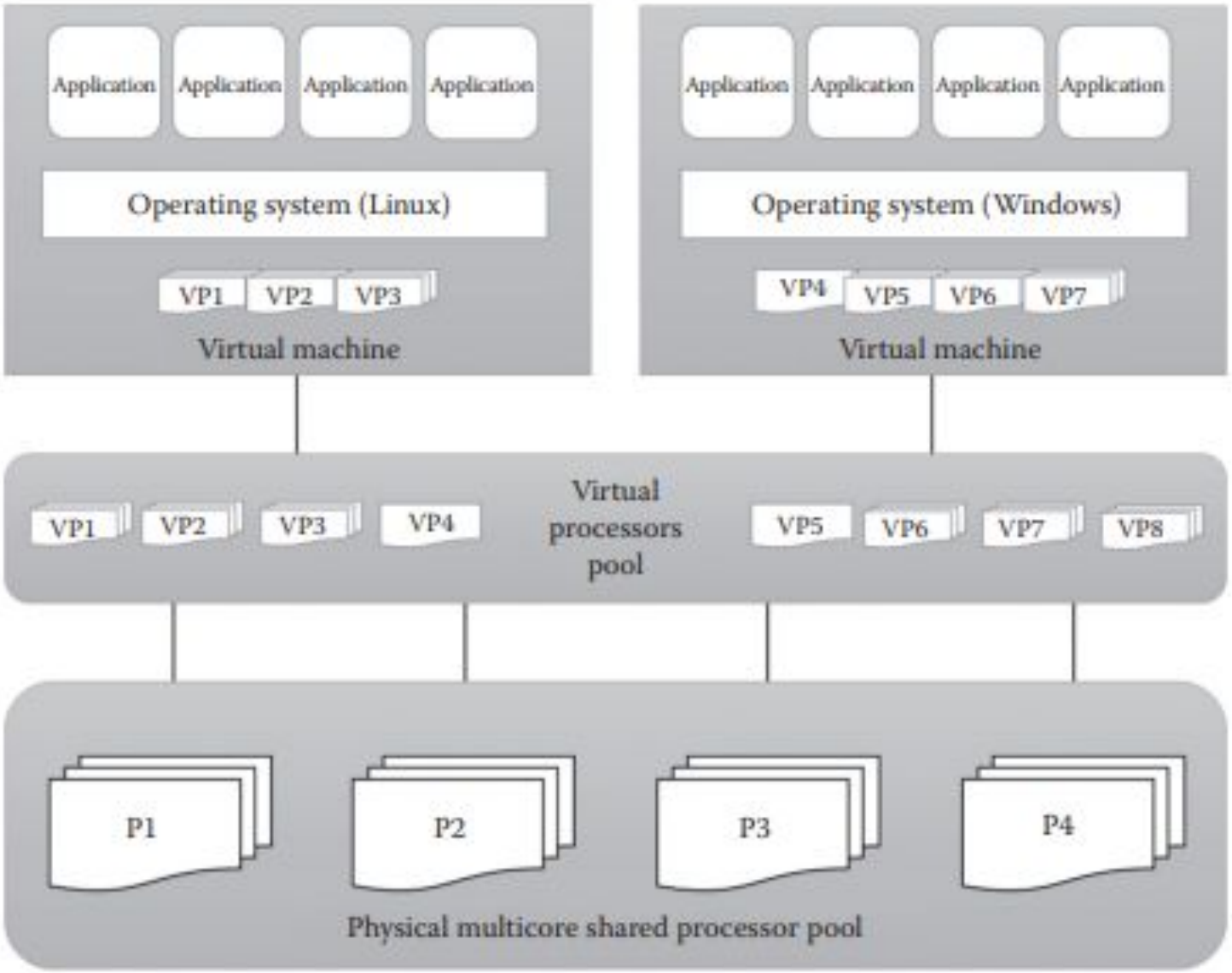

FIGURE 7.3
Processor virtualization.

Memory Virtualization

- The process of providing a virtual main memory to the VMs is known as memory virtualization or main memory virtualization.
- In main memory virtualization, the physical main memory is mapped to the virtual main memory as in the virtual memory concepts in most of the OSs.
- The main idea of main memory virtualization is to map the virtual page numbers to the physical page numbers.
- Main memory virtualization can also be achieved by using the hypervisor software. Normally, in the virtualized data centers, the unused main memory of the different servers will consolidate as a virtual main memory pool and can be given to the VMs.

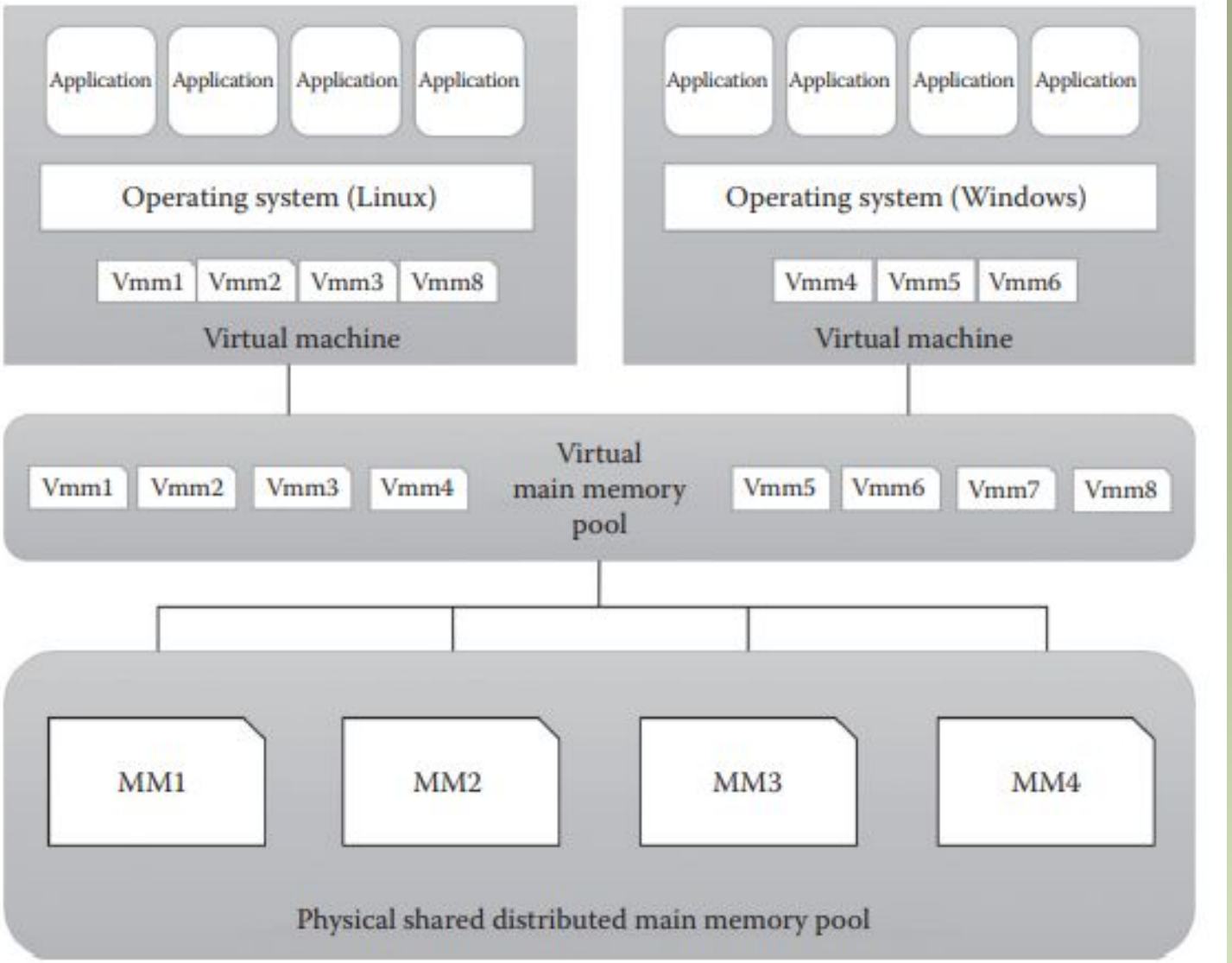

FIGURE 7.4
Main memory virtualization.

Storage Virtualization

- Storage virtualization is a form of resource virtualization where multiple physical storage disks are abstracted as a pool of virtual storage disks to the VMs. Normally, the virtualized storage will be called a logical storage.
- Storage virtualization is mainly used for maintaining a backup or replica of the data that are stored on the VMs.
- It can be further extended to support the high availability of the data.
- It can also be achieved through the hypervisors. It efficiently utilizes the underlying physical storage.
- The other advanced storage virtualization techniques are storage area networks (SAN) and network-attached storage (NAS).

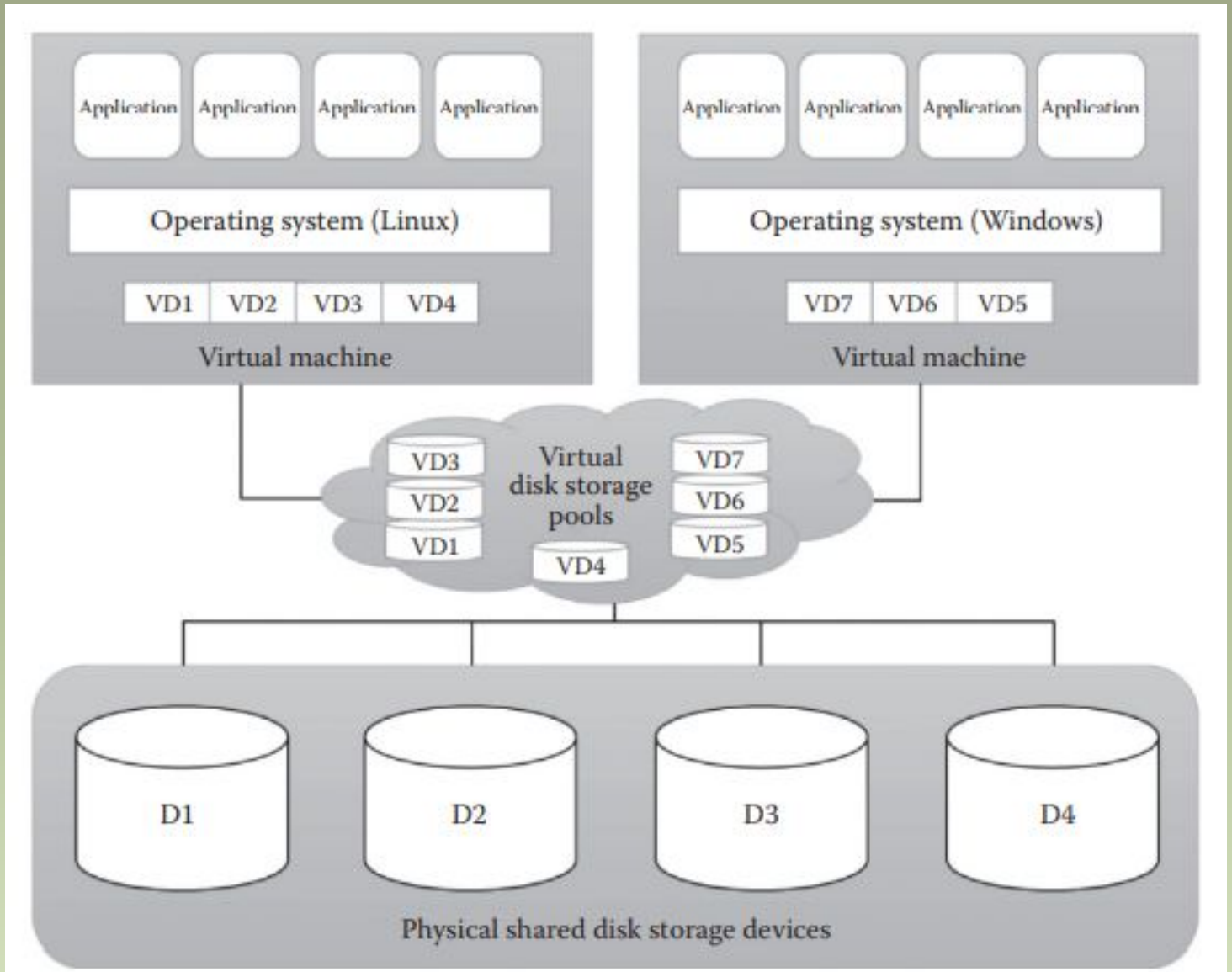

FIGURE 7.5
Storage virtualization.

Network Virtualization

- Network virtualization is a type of resource virtualization in which the physical network can be abstracted to create a virtual network.
- The physical network components like router, switch, and Network Interface Card (NIC) will be controlled by the virtualization software to provide virtual network components.
- The virtual network is a single software-based entity that contains the network hardware and software resources.
- Network virtualization can be achieved from internal network or by combining many external networks.
- it enables the communication between the VMs that share the physical network. There are different types of network access given to the VMs such as bridged network, network address translation (NAT), and host only.

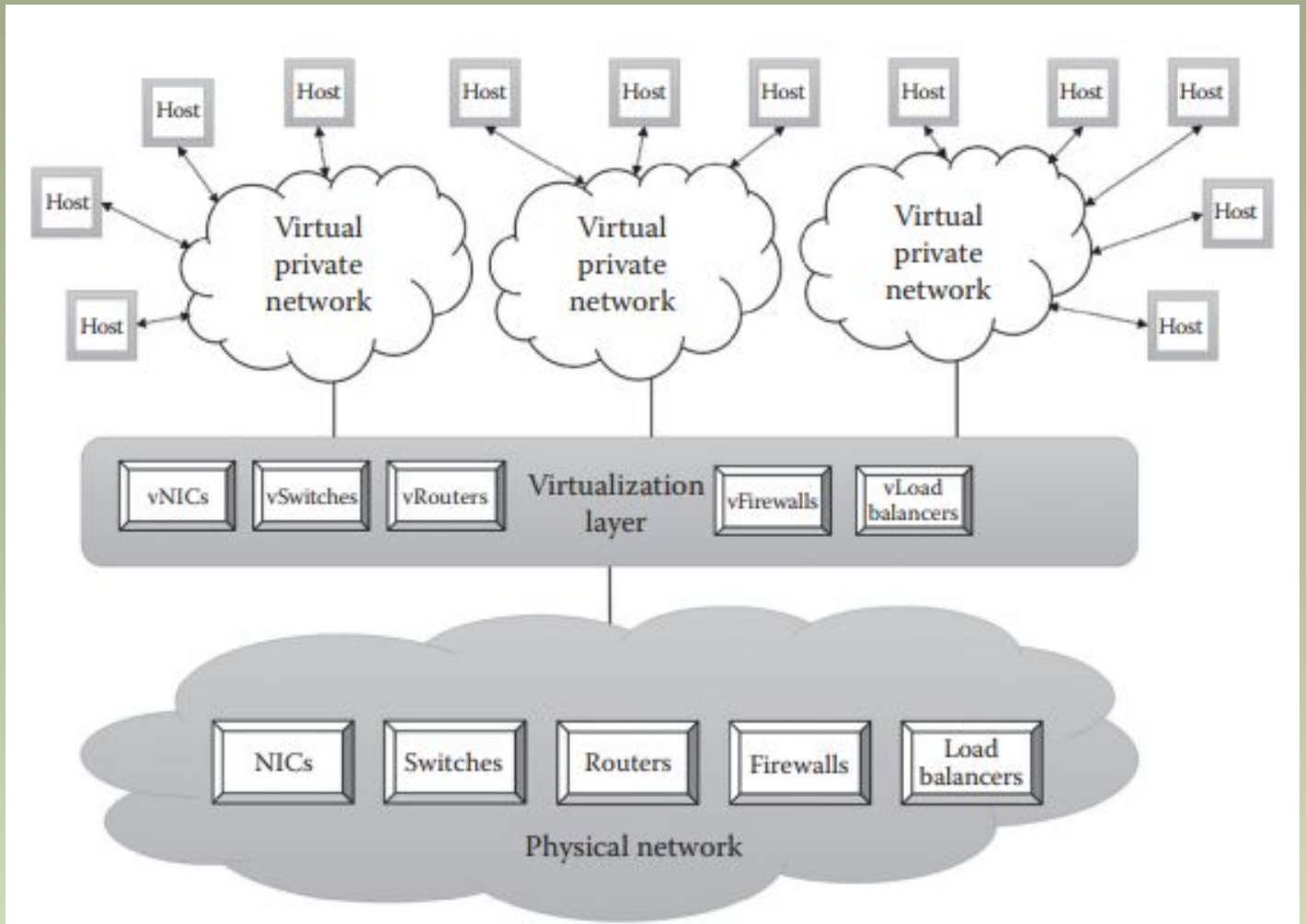

FIGURE 7.6
Network virtualization.

Data Virtualization

- Data virtualization is the ability to retrieve the data without knowing its type and the physical location where it is stored.
- It aggregates the heterogeneous data from the different sources to a single logical/virtual volume of data.
- This logical data can be accessed from any applications such as web services, E-commerce applications, web portals, Software as a Service (SaaS) applications, and mobile application.
- Data virtualization hides the type of the data and the location of the data for the application that access it.
- It also ensures the single point access to data by aggregating data from different sources. It is mainly used in data integration, business intelligence, and cloud computing

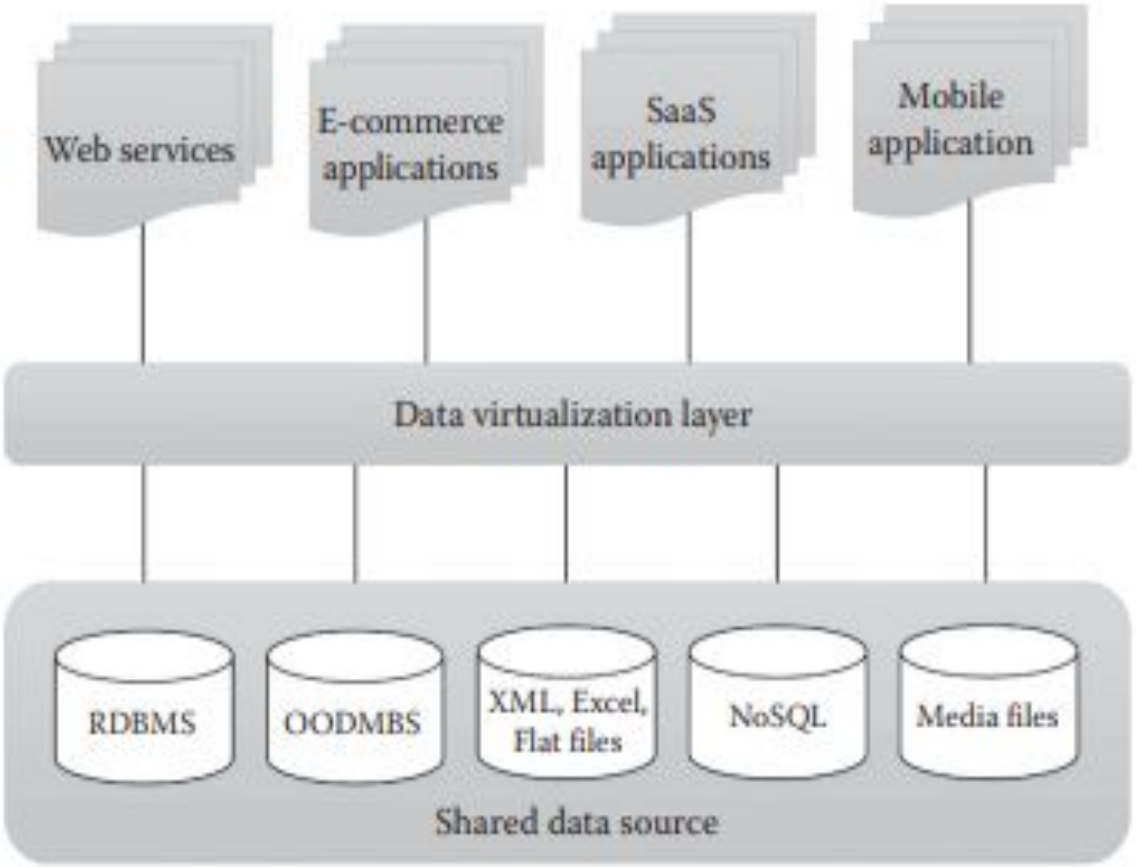

FIGURE 7.7
Data virtualization.

Application Virtualization

- Application virtualization is the enabling technology for SaaS of cloud computing.
- The application virtualization offers the ability to the user to use the application without the need to install any software or tools in the machine.
- Here, the complexity of installing the client tools or other supported software is reduced.
- Normally, the applications will be developed and hosted in the central server.
- The hosted application will be again virtualized, and the users will be given the separated/isolated virtual copy to access.

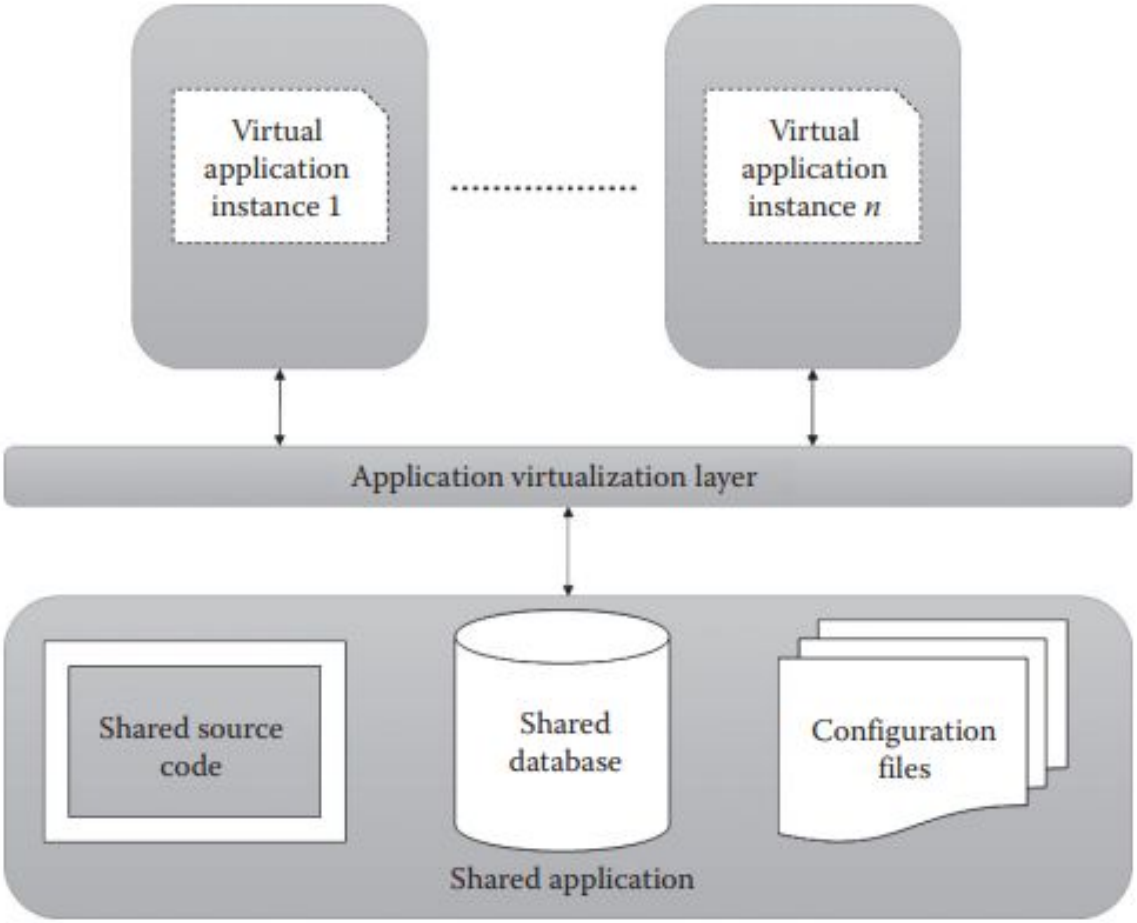

FIGURE 7.8
Application virtualization.

Protection rings

- Protection rings are used to isolate the OS from untrusted user applications. The OS can be protected with different privilege levels.
- In protection ring architecture, the rings are arranged in hierarchical order from ring 0 to ring 3 as shown in Figure 7.9.
- Ring 0 contains the programs that are most privileged, and ring 3 contains the programs that are least privileged. Normally, the highly trusted OS instructions will run in ring 0, and it has unrestricted access to physical resources.
- Ring 3 contains the untrusted user applications, and it has restricted access to physical resources. The other two rings (ring 1 and ring 2) are allotted for device drivers. This protection ring architecture restricts the misuse of resources and malicious behavior of untrusted user-level programs.
- Depending on the type of virtualization, the hypervisor and guest OS will run in different privilege levels. Normally, the hypervisor will run with the most privileged level at ring 0, and the guest OS will run at the least privileged level than the hypervisor.

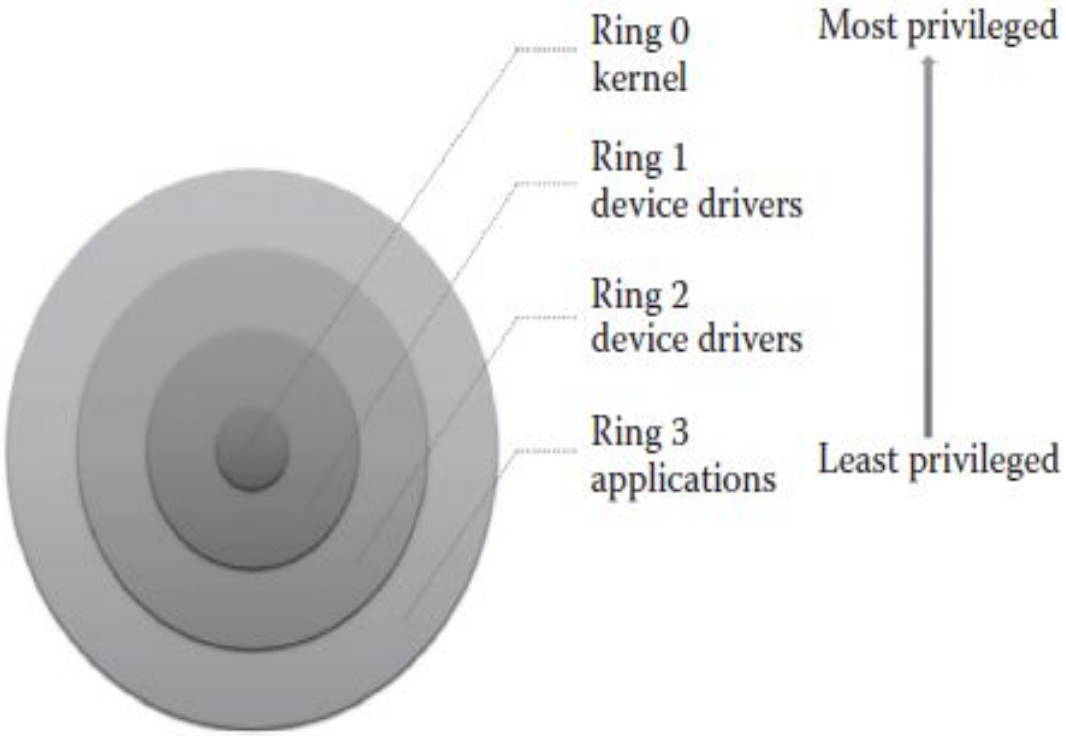

FIGURE 7.9
Protection rings in OSs.

Approaches in Virtualization

- **Full Virtualization**

- Full virtualization uses a special kind of software called a **hypervisor.**
- The hypervisor interacts directly with the physical server's hardware resources, such as the CPU and storage space, and acts as a platform for the virtual server's OSs.
- It helps to keep each virtual server completely independent and unaware of the other virtual servers running on the physical machine.
- Each guest server or the virtual machine (VM) is able to run its own OS. That means one virtual server could be running on Linux and the other one could be running on Windows.
- Examples include VMWare ESX and VirtualBox.
- In the full virtualization, the guest OS is unaware of the underlying hardware infrastructure. That means the guest OS is not aware of the fact that it is running on a virtualized platform and of the feeling that it is running on the real hardware.

Pros

- This approach provides the best isolation and security for the VMs.
- Different OSs can run simultaneously.
- The virtual guest OS can be easily migrated to work in native hardware.
- It is easy to install and use and does not require any change in the guest OS.

Cons

- Binary translation is an additional, overhead, and it reduces the overall system performance.
- There is a need for correct combination of hardware and software

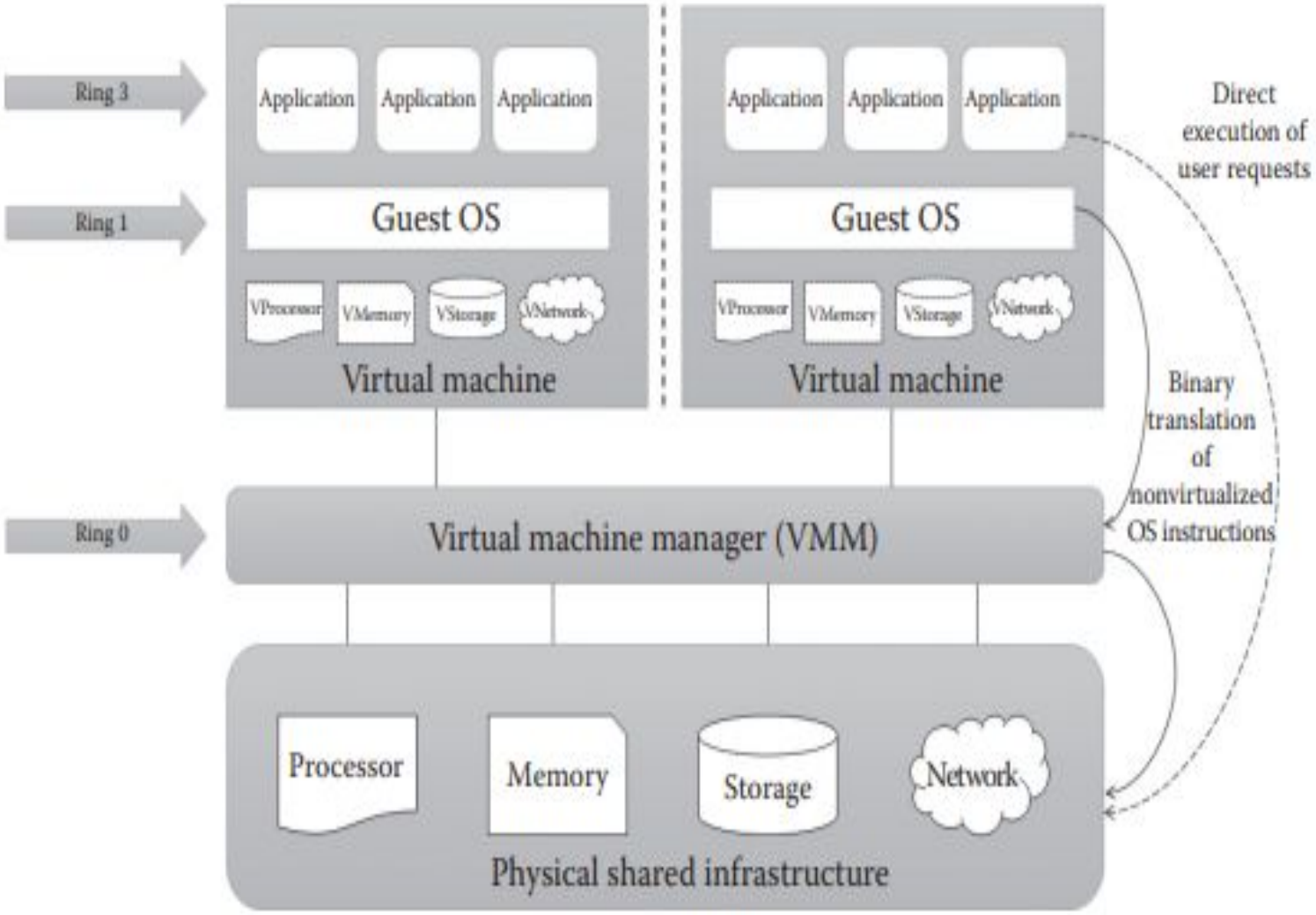

FIGURE 7.10
Full virtualization.

- **Paravirtualization**

- In this case, VMs do not simulate the underlying hardware, and this uses a special API that a modified guest OS must use.
- Examples include Xen and VMWare ESX server.
- In this type of virtualization, partial simulation of the underlying hardware infrastructure is achieved. This is also known as **partial virtualization or OS-assisted virtualization**.
- This virtualization is different from the full virtualization in that, here, the guest OS is aware of the fact that it is running in a virtualized environment.
- In this case, **hypercalls** are used for the direct communication between the guest OS and the hypervisor.

Pros

- It eliminates the additional overhead of binary translation and hence improves the overall system efficiency and performance.
- It is easier to implement than full virtualization as there is no need for special hardware.

Cons

- There is an overhead of guest OS kernel modification.
- The modified guest OS cannot be migrated to run on physical hardware.
- VMs suffer from lack of backward compatibility and are difficult to migrate to other hosts.

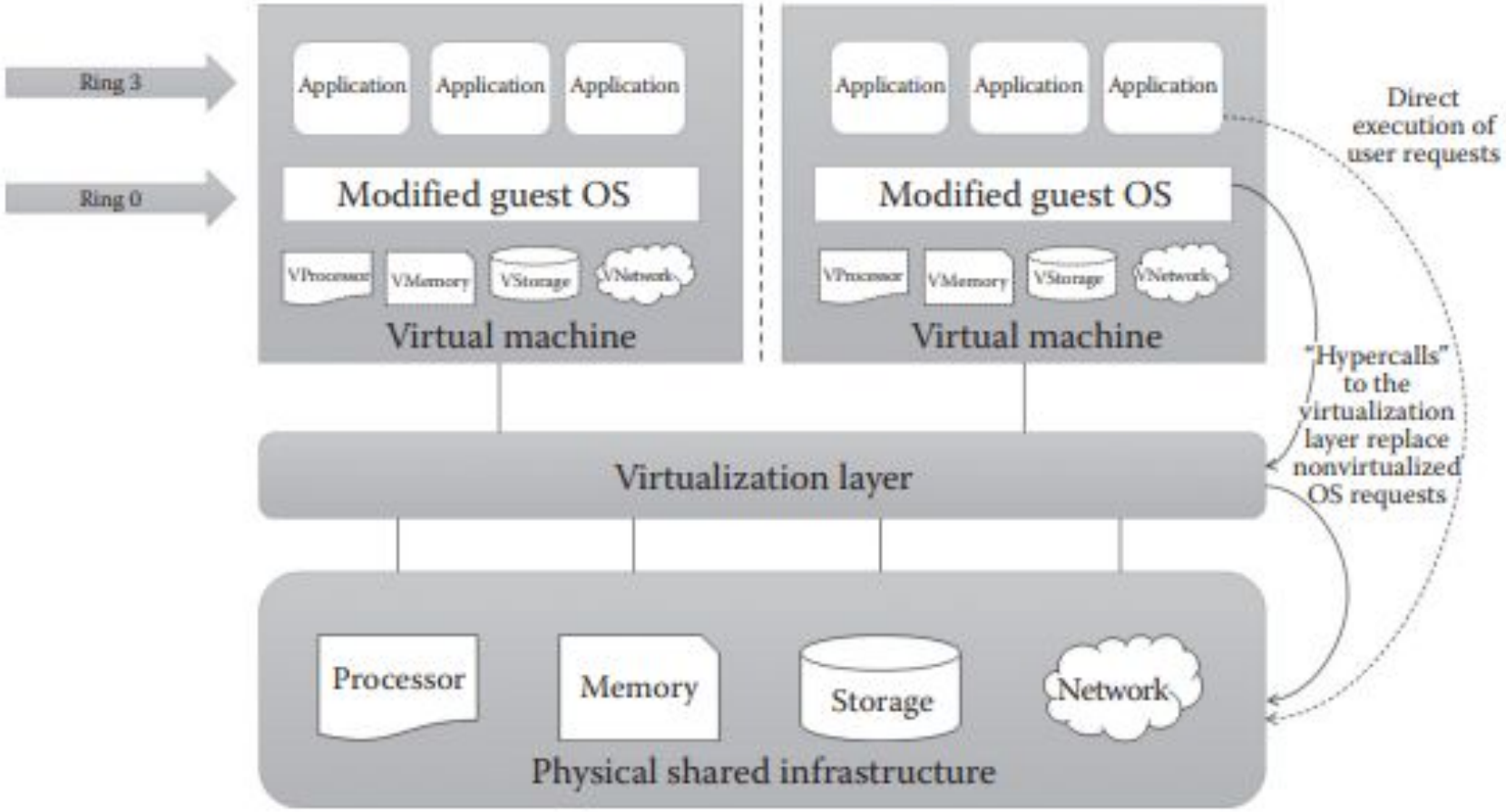

FIGURE 7.11
Paravirtualization.

- **Hardware-Assisted Virtualization**

- In this type of virtualization, hardware products supporting the virtualization are used.
- Hardware vendors like Intel and AMD have developed processors supporting the virtualization through the hardware extension.
- Intel has released its processor with its virtualization technology VT-x, and AMD have released its processor with its virtualization technology AMD-v to support the virtualization.
- An advantage of this approach could be that it **eliminates the overhead of binary translation and paravirtualization.**
- A disadvantage includes the lack of support from all vendors.

Pros

- It reduces the additional overhead of binary translation in full virtualization.
- It eliminates the guest OS modification in paravirtualization.

Cons

- Only new-generation processors have these capabilities. All x86/x86_64 processors do not support hardware-assisted virtualization features.
- More number of VM traps result in high CPU overhead, limited scalability, and less efficiency in server consolidation.

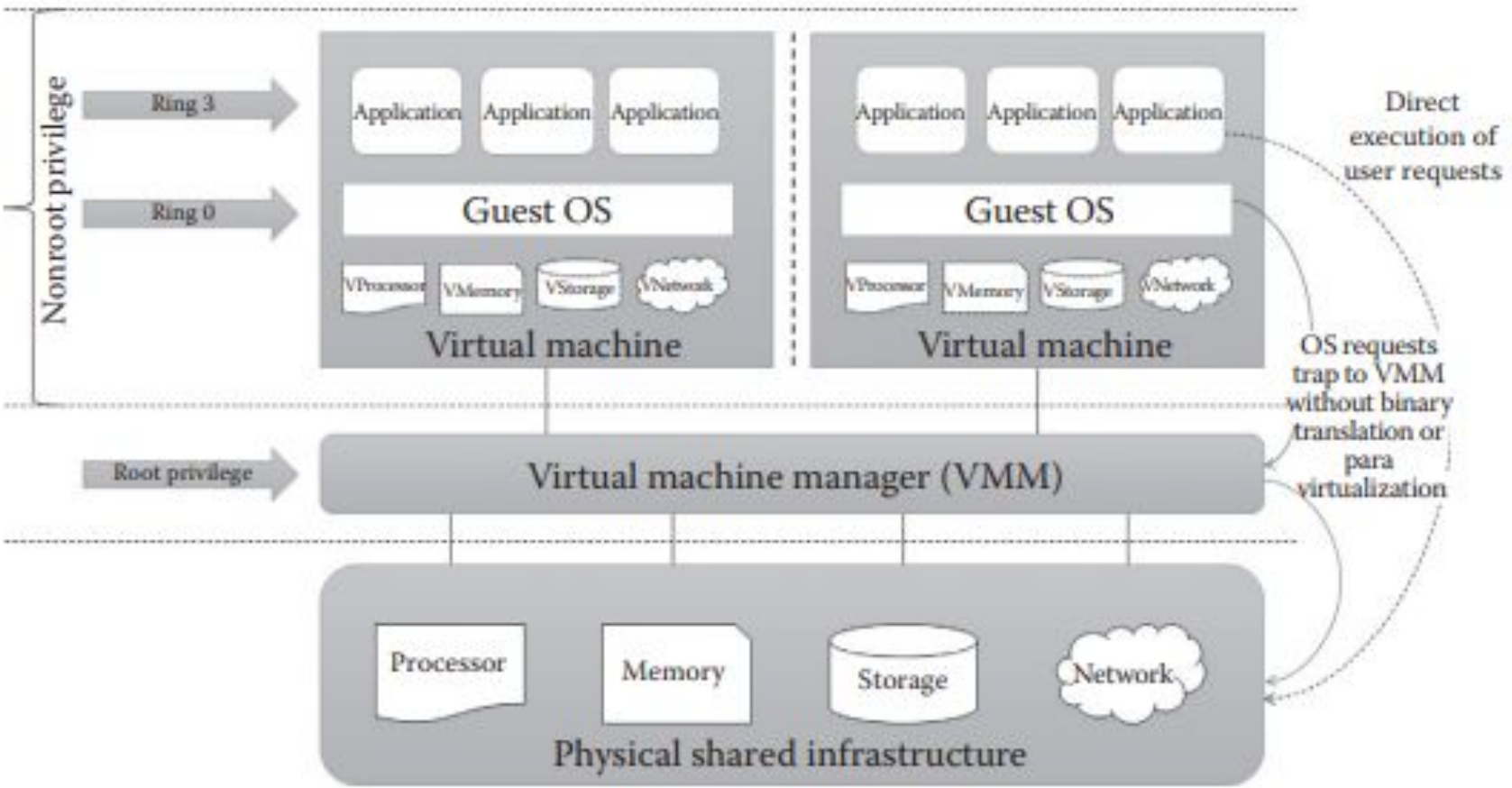

FIGURE 7.12
Hardware-assisted virtualization.

Hypervisor and Its Role

- Definition: Hypervisors are software tools used to create the VMs, and they produce the virtualization of various hardware resources such as CPU, storage, and networking devices. They are also called **virtual machine monitor (VMM)** or **virtualization managers**. They help in the virtualization of cloud data centers (DCs).
- The various hypervisors used are **VMware, Xen, Hyper-V, KVM**, etc.
- Hypervisors help to run multiple OSs concurrently on a physical system sharing its hardware. Thus, a hypervisor allows multiple OSs to share a single hardware host. In this case, every OS appears to have the host's processor, memory, and other resources allocated solely to it. However, the hypervisor is actually controlling the host processor and resources and in turn allocates what is needed to each OS. The hypervisor also makes sure that the guest OSs (called VMs) do not interrupt each other.
- hypervisor manages multiple OSs or multiple instances of the same OS on a single physical computer system.
- Hypervisors are designed to suit a specific processor, and they are also called **virtualization managers.**

- Types of Hypervisor:
- Type 1 hypervisor:
- This type of hypervisor runs directly on the **host computer's hardware** in order to control the hardware resources and also to manage the guest OSs.
- This is also known as **native or bare-metal hypervisors**.
- The additional overhead of communicating with the host OS is reduced and offers better efficiency when compared to type 2 hypervisors.
- This type of hypervisors is used for servers that handle heavy load and require more security.
- Examples include VMware ESXi, Citrix XenServer, and Microsoft Hyper-V hypervisor.

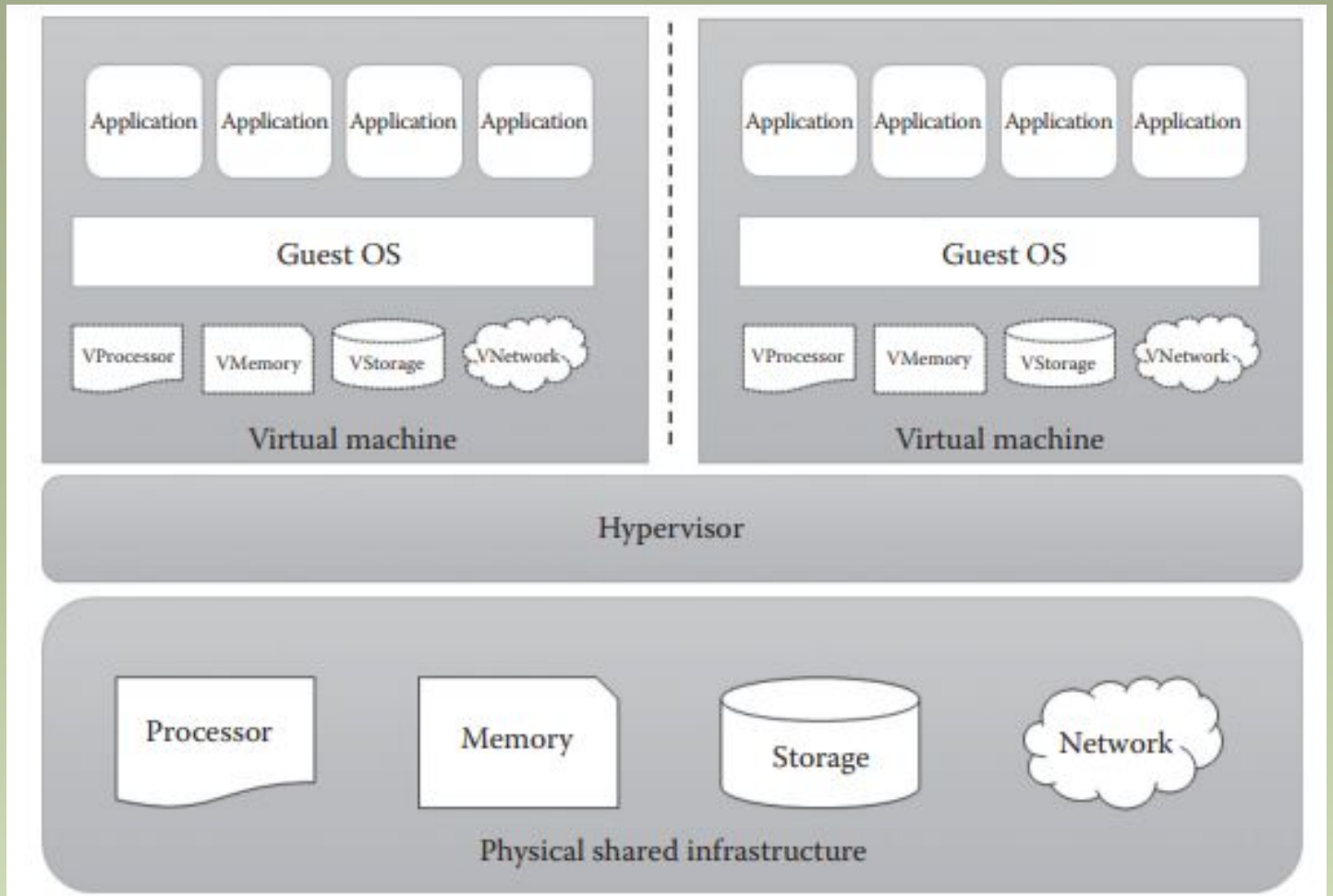

FIGURE 7.13
Type 1 or bare metal hypervisor.

- Type 2 hypervisor:
- This type of hypervisor runs **within a formal OS environment**.
- In this type, the hypervisor runs as a distinct second layer while the guest OS runs as a third layer above the hardware.
- This is also known as the **hosted hypervisors**.
- The host OS is also known as physical host, which has the direct access to the underlying hardware.
- The major disadvantage of this approach is if the host OS fails or crashes, it also results in crashing of VMs.
- So, it is recommended to use type 2 hypervisors only on client systems where efficiency is less critical
- Examples include VMware Workstation and VirtualBox.

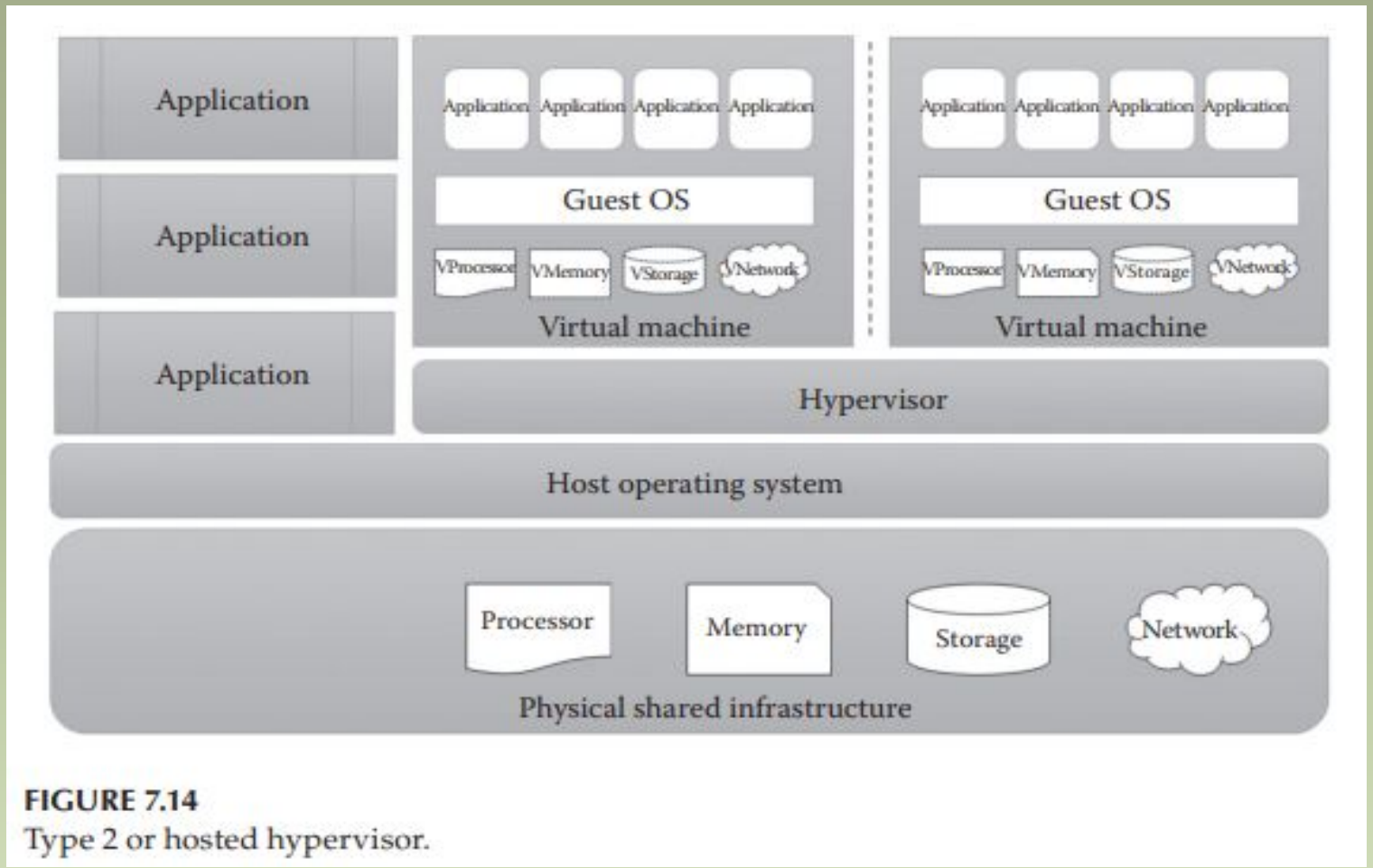

FIGURE 7.14
Type 2 or hosted hypervisor.

Security Issues

- The hypervisor creates a virtual environment in the data centers. So, the better way to attack the resources is attacking the hypervisor.
- The hypervisor attack generally compromises the hypervisor through malicious code written by any attacker to disrupt or corrupt the whole server.
- In a virtualized environment, hypervisor is the higher authority entity that has the direct access to the hardware.
- So, most of the attackers will target the hypervisor as an entry point to attack the system. In bare metal hypervisor (type 1), it is very difficult to perform the attack as it is deployed directly on the hardware. But the hosted hypervisors (type 2) are more vulnerable to the attacks as hypervisors are running on top of the host OSs.
- There are two possibilities of attacking the hypervisor:
  - Through the host OS
  - Through the guest OS

Attack through the host OS

- Attacks from the host OS can be performed by exploiting the vulnerabilities of the host OS.
- It is known that even the modern OSs are also vulnerable to the attacks. Once the OS gets compromised, the attackers have full control over the applications running on top of the OS.
- As hypervisors (type 2) are also an application that is running on top of the OS, there is a possibility of attacking the hypervisor through the compromised host OS.
- Once the attacker gets full control over the hypervisor through the compromised OS, the attacker will be able to run all the privileged instructions that can control the actual hardware. The attacker can do the following malicious activities:
  - Denial of service attack, where the attacker can deny the virtual resources when there is a request from the new VM
  - Stealing the confidential information that is stored in the VMs

Attack through the guest OS

- The hypervisor can also be compromised or attacked from the malicious script from the compromised guest OS.
- Since the guest OS is communicating with the hypervisor to get virtual resources, any malicious code from the guest OS or VMs can compromise the hypervisor.
- The attacks from the guest OS will try to abuse the underlying resources attack or compromise the hypervisor from the malicious VMs. Once the hypervisor gets compromised from the guest OS or malicious VMs, it can misuse the hypervisors' high privilege on the hardware.
- This type of attack is possible in both type 1 and type 2 hypervisors.
- After the hypervisor gets compromised, the attacker can do the following malicious activities:
  - Get the unauthorized access to the other VMs that share the physical hardware.
  - Attacker can utilize the hardware resources fully to launch resource exhaustion attacks, etc.

Recommendations to avoid hypervisor attacks

- Most of the attacks on the hypervisor are through the host OS or the guest OS. So, the OS should be protected from the malicious attacker or the hypervisors should be protected from the compromised OSs.

There are several best practices to keep the hypervisor secured:

- Update the hypervisor software and the host OS regularly.
- Disconnect the unused physical resources from the host system or hypervisor.
- Enable least privilege to the hypervisor and guest OS to avoid the attacks through unauthorized access.
- Deploy the monitoring tools in the hypervisor to detect/prevent malicious activities.
- Strong guest isolation.
- Employ mandatory access control policies.

From Virtualization to Cloud Computing

- Virtualization is not cloud computing:-

1. ***Type of service:*** Generally, virtualization offers more infrastructure services rather than platform and application services. But cloud computing offers all infrastructure (IaaS), platform (PaaS), and software (SaaS) services.

2. ***Service delivery:*** The service delivery in cloud computing is on-demand and allows the end users to use the cloud services as per the need. But virtualization is not made for on-demand services.

3. *Service provisioning*: In cloud computing, automated and self-service provisioning is possible for the end users, whereas in virtualization, it is not possible and a lot of manual work is required from the providers or system administrator to provide services to the end users.

4. *Service orchestration*: Cloud computing allows the service orchestration and service composition to meet end user requirements. Some providers are also providing automated service orchestration to the end users. But in virtualization, orchestrating different service to get composite services is not possible.

5. *Elasticity*: In cloud computing, we can add or remove the infrastructure dynamically according to the need, and adding or removing the infrastructure is automatic. But virtualization fails to provide elasticity as stopping and starting a VM is manual and is also difficult.

6. *Targeted audience*: Cloud computing targets the service providers for high resource utilization and improved ROI. At the same time, it also facilitates the end users to save money by using on-demand services. In the case of virtualization, the targeted audience is only the service providers or IT owners, not the end users.

IAAS

- The virtualization concept is fully utilized in the infrastructure layer of the cloud computing.
- The IaaS service offers virtual memory, virtual processors, virtual storage, and virtual networks to run the VMs.
- The IaaS service utilizes the memory, processor, storage, and network virtualization of the underlying infrastructure.
- The IaaS layer uses the hypervisors to abstract the underlying resources for the VMs.
- The virtual data center will not be simply referred to as a cloud data center. The virtualized data center will be called as cloud data center if it delivers the service on a pay-per-use basis.
- type 1 hypervisors will be selected rather than type 2 hypervisors as the type 1 hypervisors are directly accessing the underlying hardware.

PAAS

- the service provider will provide all the development tools as a service to the end users through the Internet.
- The end users need not install any integrated development environments (IDEs), programming languages, and component libraries in their machine to access the services. The programming languages, databases, language runtimes, middleware, and component libraries will be provided to the customers by abstracting the actual platform that runs in the provider data center.
- the PaaS services utilize the OS-level, database-level, programming language–level virtualization to provide the virtual development platform to the end users.
- Generally, the PaaS providers will provide a variety of client tools such as WebCLI, REST APIs, and Web UI to the developers for accessing the virtual platform.
- Some PaaS providers allow the offline development by integrating with the IDEs like eclipse to make the development environment availability. The developers need not be online to use their services. They can work offline and push the application online whenever it is ready for the deployment.

SaaS

- Like infrastructure and platform, software applications can also be virtualized. The software delivery model that allows the customers to access the software that is hosted in the service provider data center through the Internet is known as Software as a Service (SaaS).
- SaaS is a subscription-based application rather than a licensed application.
- To access the SaaS application, customers need not install it on their machine. With the simple web browser, they can access the application from the service provider data center through the Internet.
- utilizes application-level virtualization to deploy the application.
- allows multiple customers to share the same instance of an application. This technology is popularly known as multitenancy
- Virtualization is used as an enabling technology to provide multitenant infrastructure, development platform, and SaaS.
- Additionally, there are other cloud services that use virtualization such as Network as a Service using network virtualization, Storage as a Service using storage virtualization, and Database as a Service using database virtualization.