7

Virtualization

Learning Objectives

The main objective of this chapter is to introduce the concept of virtualization and how it is used as enabling technology for cloud computing. After reading this chapter, you will

- Understand the basics of virtualization
- Understand how the different resources such as processors, memory, storage, and network can be virtualized
- Understand the pros and cons of different approaches to virtualization
- Understand the basics of hypervisor and its security issues
- Understand how cloud computing is different from virtualization
- Understand how cloud computing leverages the virtualization for its different service models

Preamble

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. This chapter describes virtualization and discusses the benefits of virtualization and, different resources that can be virtualized. This chapter also explains the different approach for virtualization such as full virtualization, hardware-assisted virtualization, and paravirtualization. The different types of hypervisors and its security issues are also discussed. At the end of the chapter, the difference between cloud computing and virtualization and how virtualization is used by cloud computing to provide services are discussed.

7.1 Introduction

In recent years, computing becomes more complex and requires large infrastructure. The organizations invest huge amount on buying additional physical infrastructure as and when there is a need for more computing resources. If you look at the capital expenditure (CapEx) and operational expenditure (OpEx) of buying and maintaining large infrastructure, it is really high. At the same time, the resource utilization and return on investment (ROI) on buying the additional infrastructure are very low. 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. The virtualization is not a new word to the computing world; it is being used for at least past four decades. The term *virtualization* becomes a buzzword in recent years and most organizations started to adopt it rapidly because of its benefits like efficient resource utilization and increased ROI, ease of administration, and green IT support.

Virtualization is a technology that enables the single physical infrastructure to function as a multiple logical infrastructure or resources. Virtualization is not only limited to the hardware, it can take many forms such as memory, processor, I/O, network, OS, data, and application. The different forms of virtualization will be discussed in the next section.

Before virtualization, the single physical infrastructure was used to run a single OS and its applications, which results in underutilization of resources. The nonshared nature of the hardware forces the organizations to buy a new hardware to meet their additional computing needs. For example, if any organization wants to experiment or simulate their new idea, they have to use separate dedicated systems for different experiments. So to complete their research work successfully, they tend to buy a new hardware that will increase the CapEx and OpEx. Sometimes, if the organization does not have money to invest more on the additional resources, they may not be able to carry out some valuable experiments because of lack of resources. So, people started thinking about sharing a single infrastructure for multiple purposes in the form of virtualization. The computing scenarios before and after virtualization are shown in Figures 7.1 and 7.2, respectively.

After virtualization was introduced, different OSs and applications were able to share a single physical infrastructure. The virtualization reduces the huge amount invested in buying additional resources. The virtualization becomes a key driver in the IT industry, especially in cloud computing. Generally, the terms *cloud computing* and *virtualization* are not same. There are significant differences between these two technologies, which will be

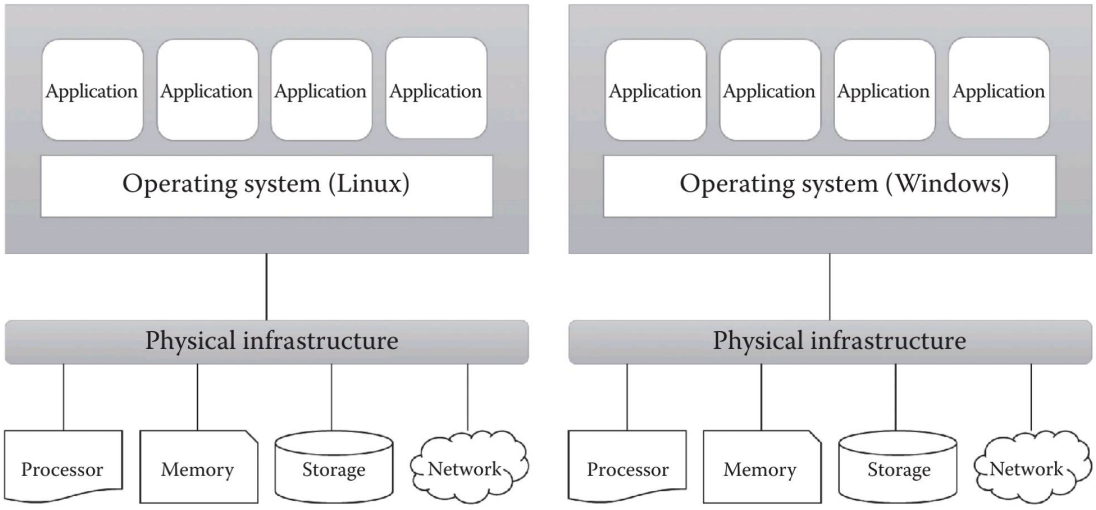

FIGURE 7.1
Before virtualization.

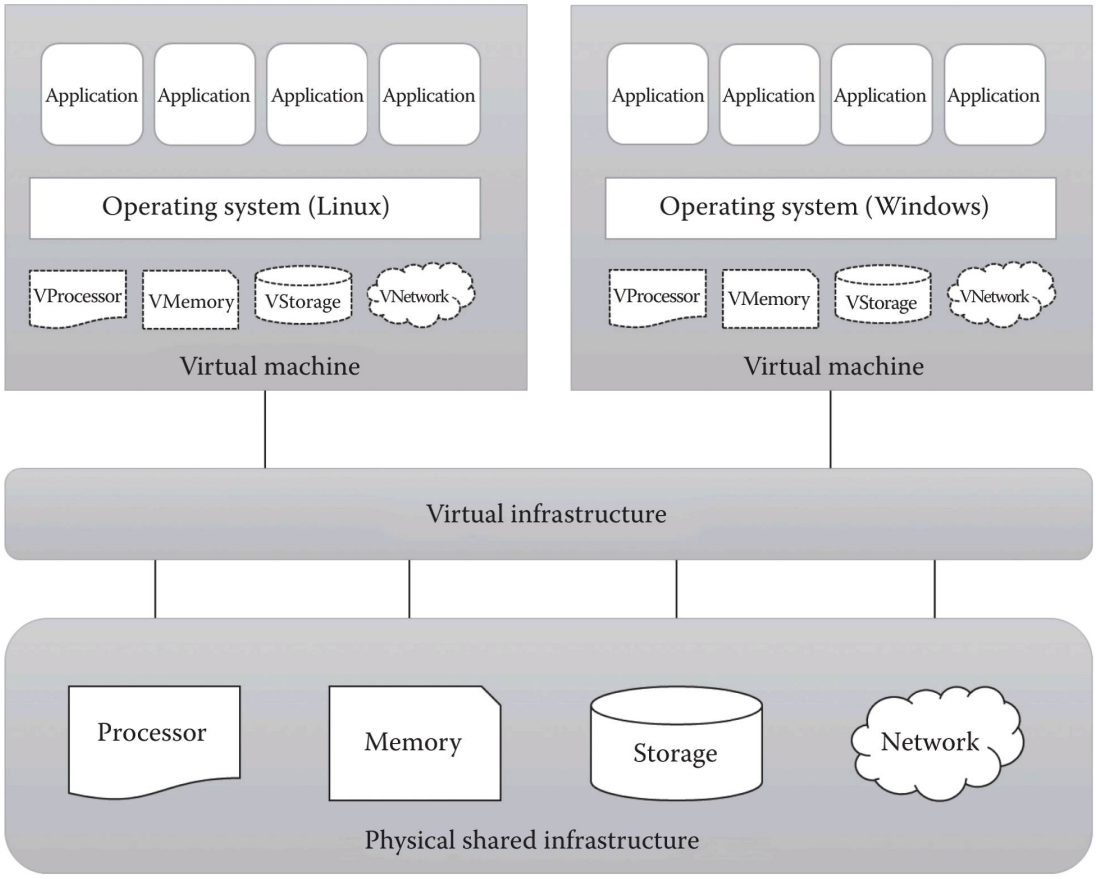

FIGURE 7.2
After virtualization.

discussed in the later part of this chapter. Industries adopt virtualization in their organization because of the following benefits:

- Better resource utilization
- Increases ROI
- Dynamic data center
- Supports green IT
- Eases administration
- Improves disaster recovery

While virtualization offers many benefits, it also has some drawbacks:

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

This chapter focuses on the different virtualization opportunities, different approaches to virtualization, role of the hypervisors in virtualization, attacks that target the hypervisors, and virtualization for cloud computing.

7.2 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. In this section, we shall discuss some of the resources that can be virtualized.

7.2.1 Processor Virtualization

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. Processor virtualization from a single hardware is illustrated in Figure 7.3. But processor virtualization can also be achieved from distributed servers.

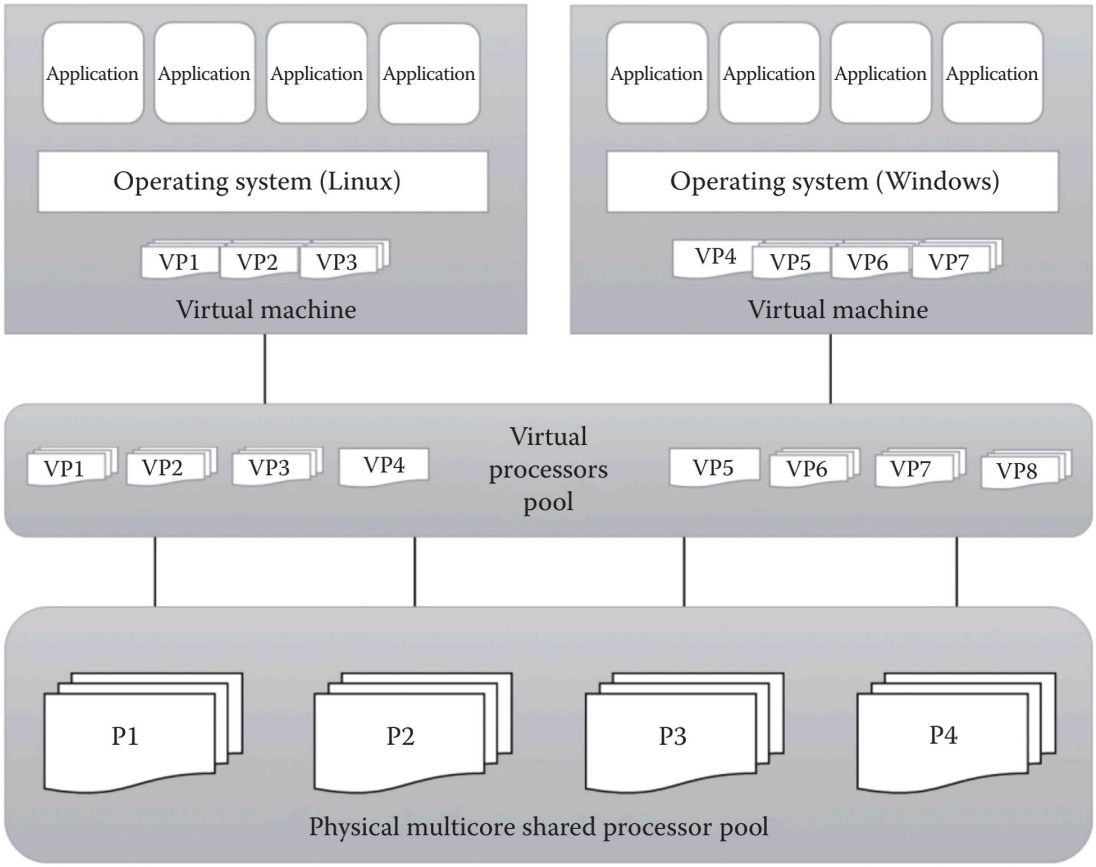

FIGURE 7.3
Processor virtualization.

7.2.2 Memory Virtualization

Another important resource virtualization technique is 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. All the modern x86 processors are supporting main memory virtualization.

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. The concept of main memory virtualization is illustrated in Figure 7.4.

7.2.3 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

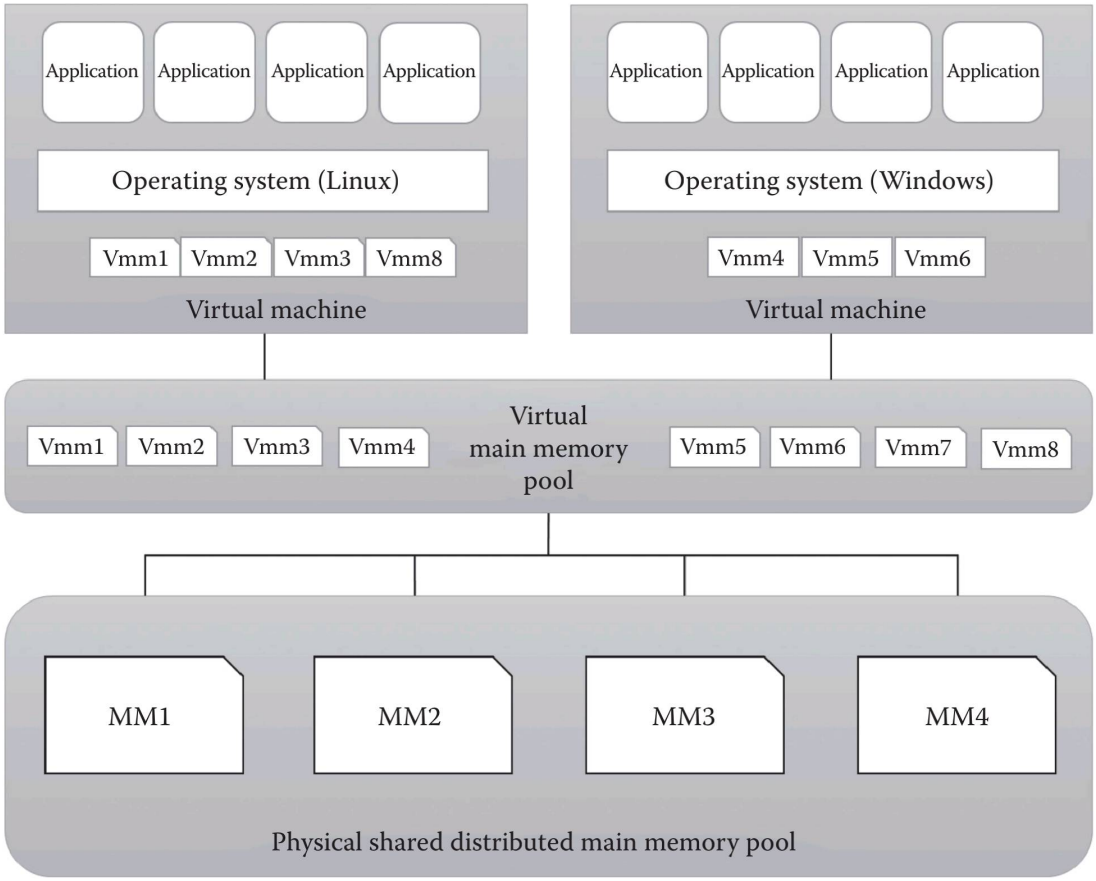

FIGURE 7.4
Main memory virtualization.

the VMs. Normally, the virtualized storage will be called a logical storage. Figure 7.5 illustrates the process of storage virtualization.

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).

7.2.4 Network Virtualization

Network virtualization is a type of resource virtualization in which the physical network can be abstracted to create a virtual network. Normally, 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. The other advantage

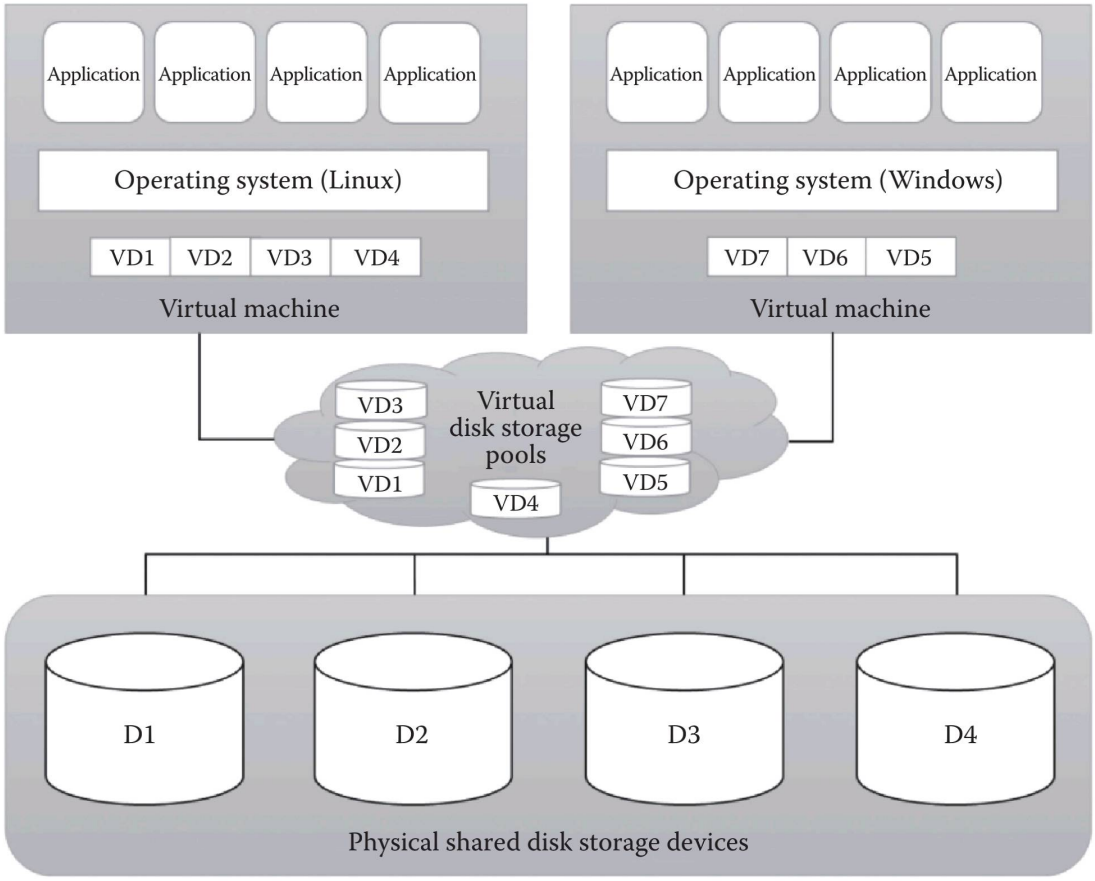

FIGURE 7.5
Storage virtualization.

of network virtualization is 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. The concept of network virtualization is illustrated in Figure 7.6.

7.2.5 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 represents data virtualization technology.

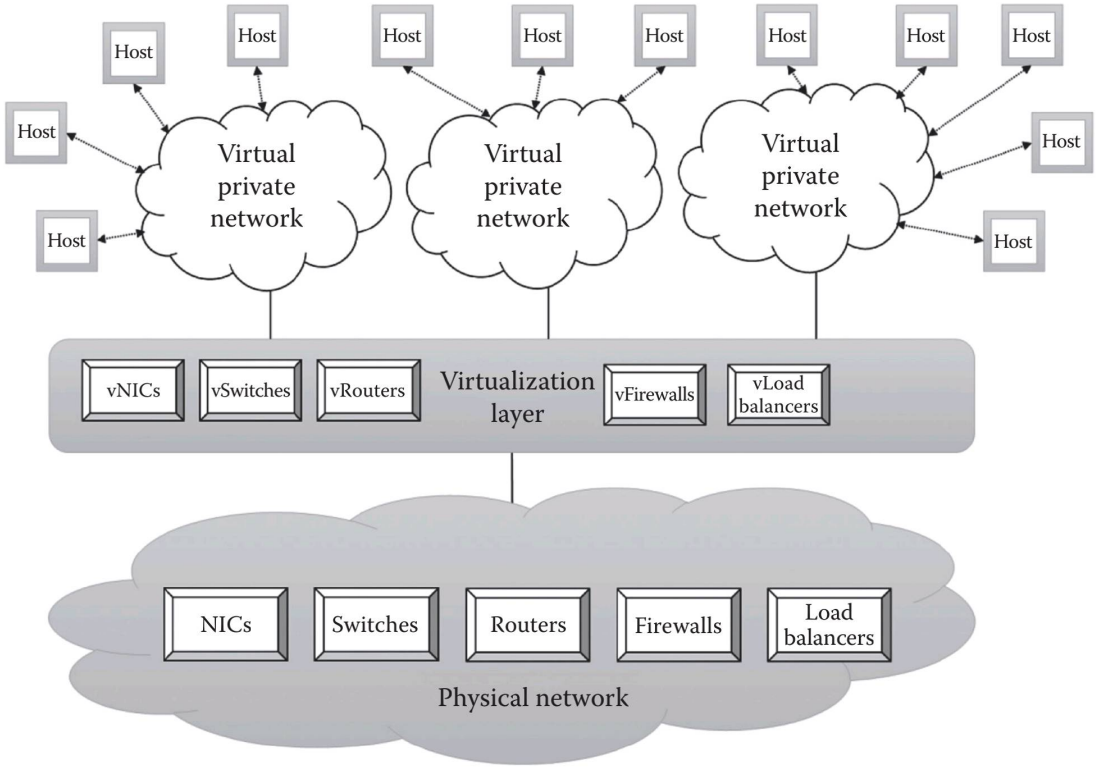

FIGURE 7.6
Network virtualization.

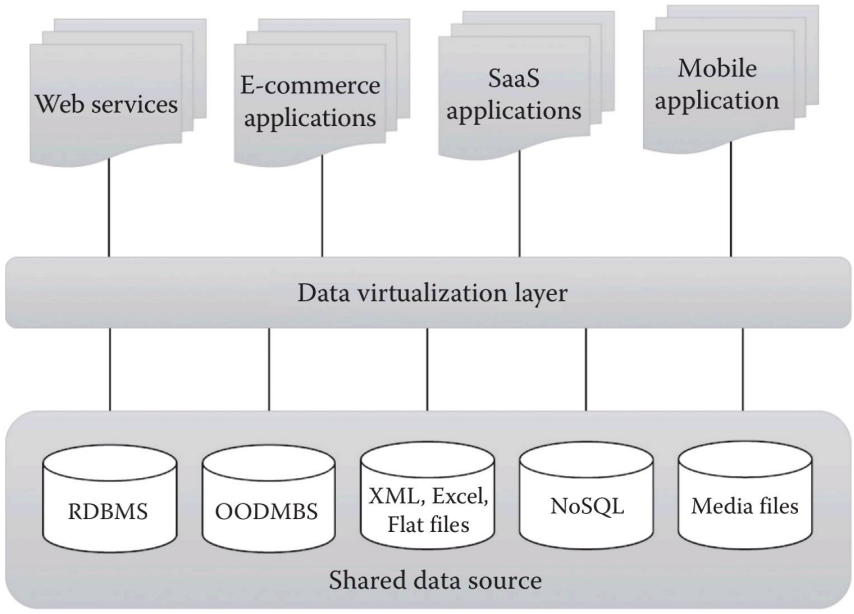

FIGURE 7.7
Data virtualization.

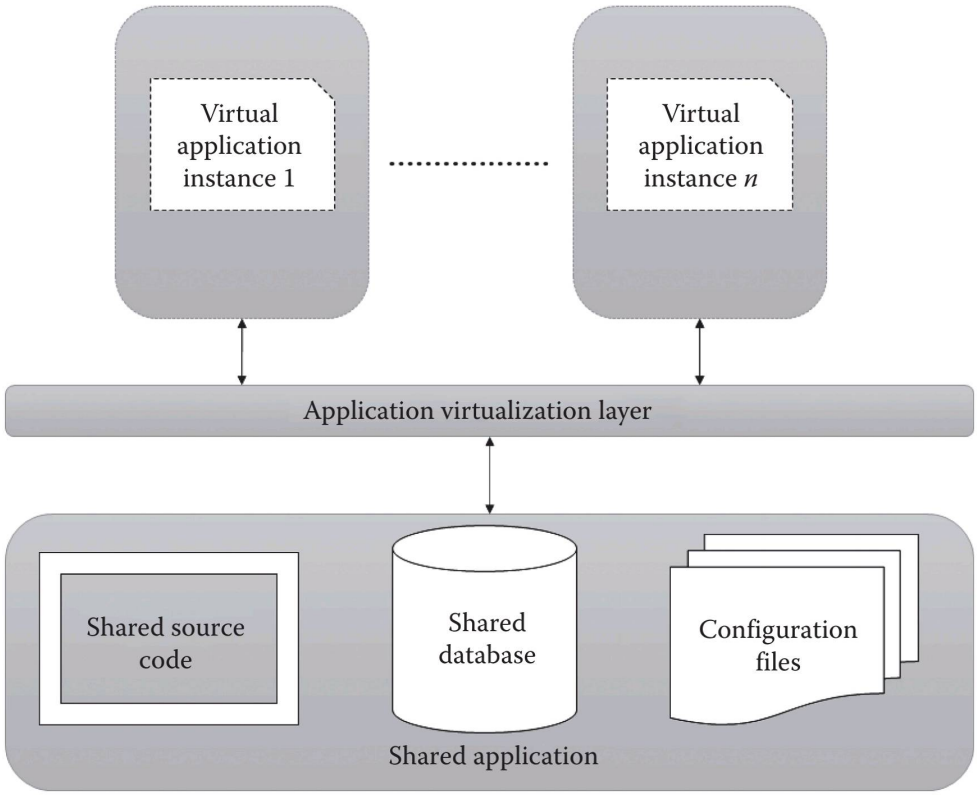

FIGURE 7.8
Application virtualization.

7.2.6 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. The concept of application virtualization is illustrated in Figure 7.8.

7.3 Approaches to Virtualization

There are three different approaches to virtualization. Before discussing them, it is important to know about *protection rings* in OSs. 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

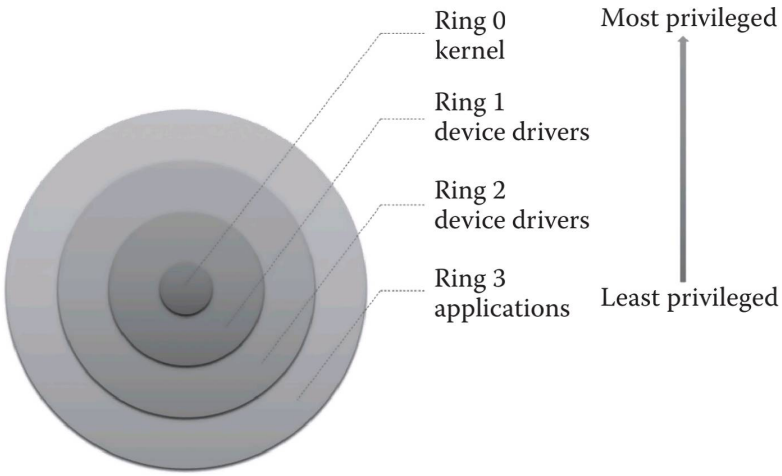

FIGURE 7.9
Protection rings in OSs.

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. For example, any user application from ring 3 cannot directly access any physical resources as it is the least privileged level. But the kernel of the OS at ring 0 can directly access the physical resources as it is the most privileged level.

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. There are three types of approaches followed for virtualization:

1. Full virtualization
2. Paravirtualization
3. Hardware-assisted virtualization

Each of the virtualization approaches is discussed in detail in this section.

7.3.1 Full Virtualization

In full virtualization, the guest OS is completely abstracted from the underlying infrastructure. The virtualization layer or virtual machine manager (VMM) fully decouples the guest OS from the underlying infrastructure. The guest OS is not aware that it is virtualized and thinks it is running on the real hardware. In this approach, the hypervisor or VMM resides at ring 0 and provides all the virtual infrastructures needed for VMs.

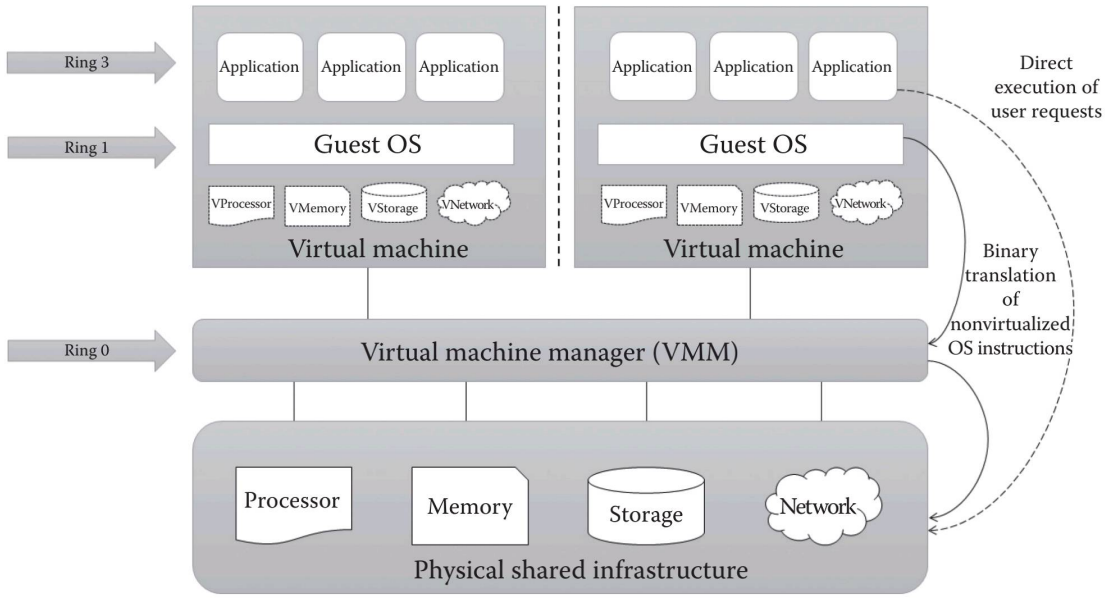

FIGURE 7.10
Full virtualization.

The guest OS resides at ring 1 and has the least privilege than the hypervisor. Hence, the OS cannot communicate to the physical infrastructure directly. It requires the help of hypervisors to communicate with the underlying infrastructure. The user applications reside at ring 3, as shown in Figure 7.10. This approach uses binary translation and direct execution techniques. Binary translation is used to translate nonvirtualized guest OS instructions with new sequences of instructions that have the same intended effect on the virtual infrastructure. On the other hand, direct execution is used for user application requests where the applications can directly access the physical resources without modifying the instructions.

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.

7.3.2 Paravirtualization

This approach is also known as *partial virtualization* or *OS-assisted virtualization* and provides partial simulation of the underlying infrastructure. The main difference between the full virtualization and paravirtualization is the guest OS knows that it is running in virtualized environment in paravirtualization. But in full virtualization, this information is not known to the guest OS. Another difference is that the paravirtualization replaces the translation of nonvirtualized OS requests with *hypercalls*. Hypercalls are similar to system calls and used for the direct communication between OS and hypervisor. This direct communication between the guest OS and hypervisor improves performance and efficiency. In full virtualization, the guest OS will be used without any modification. But in paravirtualization, the guest OS needs to be modified to replace nonvirtualizable instructions with the hypercalls.

As shown in Figure 7.11, the modified guest OS resides at ring 0 and the user applications at ring 3. As the guest OS is at privileged position, it can communicate directly to the virtualization layer without any translation by means of hypercalls. Like in full virtualization, the user applications are allowed to access the underlying infrastructure directly.

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.

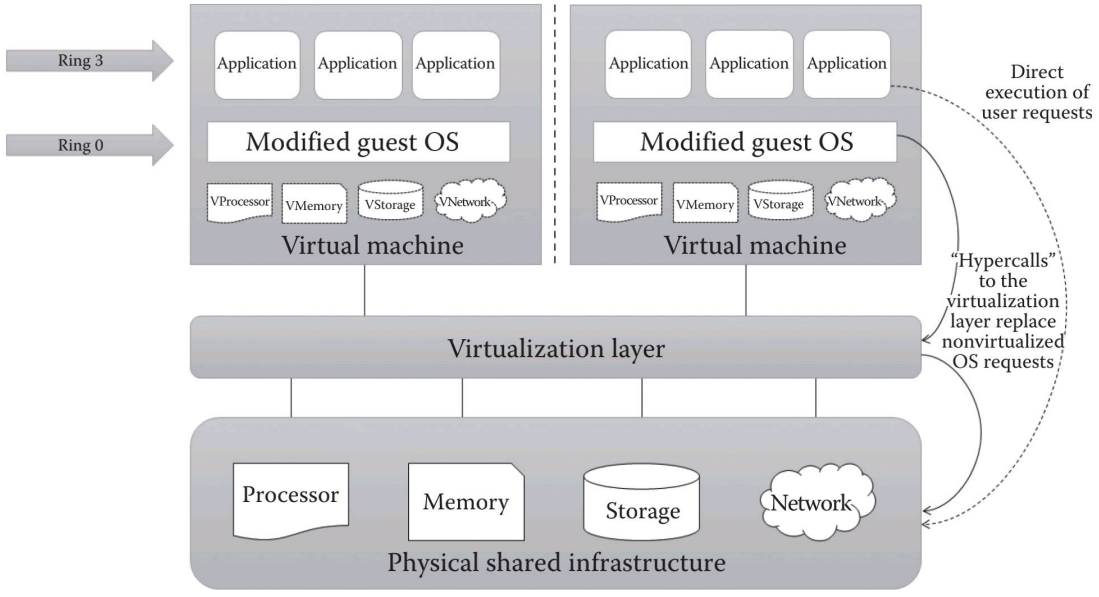

FIGURE 7.11
Paravirtualization.

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.

7.3.3 Hardware-Assisted Virtualization

In the two previous approaches, there is an additional overhead of binary translation or modification of guest OS to achieve virtualization. But in this approach, hardware vendors itself, like Intel and AMD, offer the support for virtualization, which eliminates much overhead involved in the binary translation and guest OS modification. Popular hardware vendors like Intel and AMD has given the hardware extension to their x86-based processor to support virtualization.

For example, the Intel releases its Intel Virtualization Technology (VT-x) and AMD releases its AMD-v to simplify the virtualization techniques. In VT-x, the guest state is stored in *virtual machine control structures* and in AMD-v in *virtual machine control blocks*. In hardware-assisted virtualization, the VMM has the highest privilege (root privilege) level even though it is working below ring 0. The OS resides at ring 0 and the user application at ring 3, as shown in Figure 7.12. Unlike the other virtualization approaches, the guest OS and the user applications are having the same privilege level (nonroot privilege level). As discussed earlier, the hardware-assisted virtualization technique removes binary translation and paravirtualization. Here, the OS requests directly trap the hypervisor without any translation. As in other virtualization approaches, the user requests are directly executed without any translation.

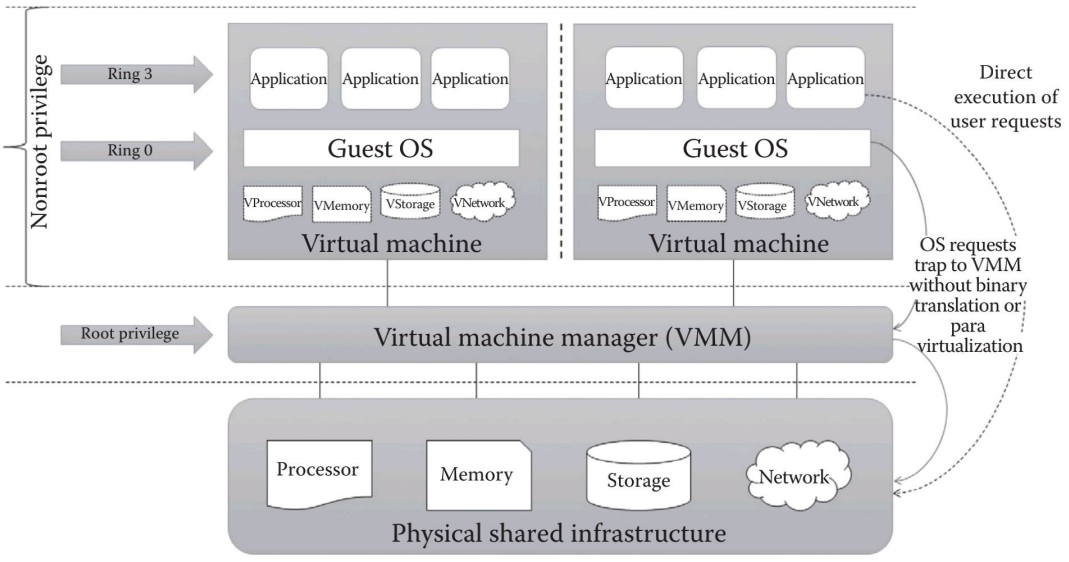

FIGURE 7.12
Hardware-assisted virtualization.

TABLE 7.1

Summary of the Different Approaches to Virtualization

	Full Virtualization	Paravirtualization	Hardware-Assisted Virtualization
Technique	Binary translation and direct execution	Hypercalls	OS requests trap to VMM without binary translation or paravirtualization
Guest OS modification	No	Yes	No
Compatibility	Excellent compatibility	Poor compatibility	Excellent compatibility
Is guest OS hypervisor independent?	Yes	No	Yes
Performance	Good	Better in certain cases	Fair
Position of VMM and privilege level	Ring 0 Root privilege	Below ring 0	Below ring 0 Root privilege
Position of guest OS and privilege level	Ring 1 Nonroot privilege	Ring 0 Root privilege	Ring 0 Nonroot privilege
Popular vendor(s)	VMware ESX	Xen	Microsoft, Virtual Iron, and XenSorce

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.

A summary of the different approaches to virtualization is given in Table 7.1.

7.4 Hypervisors

VMs are widely used instead of physical machines in the IT industry today. VMs support green IT solutions, and its usage increases resource utilization, making the management tasks easier. Since the VMs are mostly used,

the technology that enables the virtual environment also gets attention in industries and academia. The virtual environment can be created with the help of a software tool called *hypervisors*. Hypervisors are the software tool that sits in between VMs and physical infrastructure and provides the required virtual infrastructure for VMs. Generally, the virtual infrastructure means virtual CPUs (vCPUs), virtual memory, virtual NICs (vNICs), virtual storage, and virtual I/O devices. The hypervisors are also called VMM. They are the key drivers in enabling virtualization in cloud data centers. There are different hypervisors that are being used in the IT industry. Some of the examples are VMware, Xen, Hyper-V, KVM, and OpenVZ. The different types of hypervisors, some popular hypervisors in the market, and security issues with recommendations are discussed in this section.

7.4.1 Types of Hypervisors

Before hypervisors are introduced, there was a one-to-one relationship between hardware and OSs. This type of computing results in underutilized resources. After the hypervisors are introduced, it became a one-to-many relationship. With the help of hypervisors, many OSs can run and share a single hardware. Hypervisors are generally classified into two categories:

1. Type 1 or bare metal hypervisors
2. Type 2 or hosted hypervisors

The major difference between these two types of hypervisors is that type 1 runs directly on the hardware and type 2 on host OS. Figures 7.13 and 7.14 illustrate the working of type 1 and type 2 hypervisors, respectively.

Type 1 hypervisor is also known as bare metal or native hypervisor. It can run and access physical resources directly without the help of any host OS. Here, 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. Some examples of type 1 hypervisors include Microsoft Hyper-V, Citrix XenServer, VMWare ESXi, and Oracle VM Server for SPARC.

Type 2 hypervisors are also known as embedded or hosted hypervisors. This type of hypervisors requires the host OS and does not have direct access to the physical hardware. These types of hypervisors are installed on the host OS as a software program. 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 of type 2 hypervisors include VMWare Workstation and Oracle Virtualbox.

A summary of some of the popular hypervisors that are in the market is given in Table 7.2.

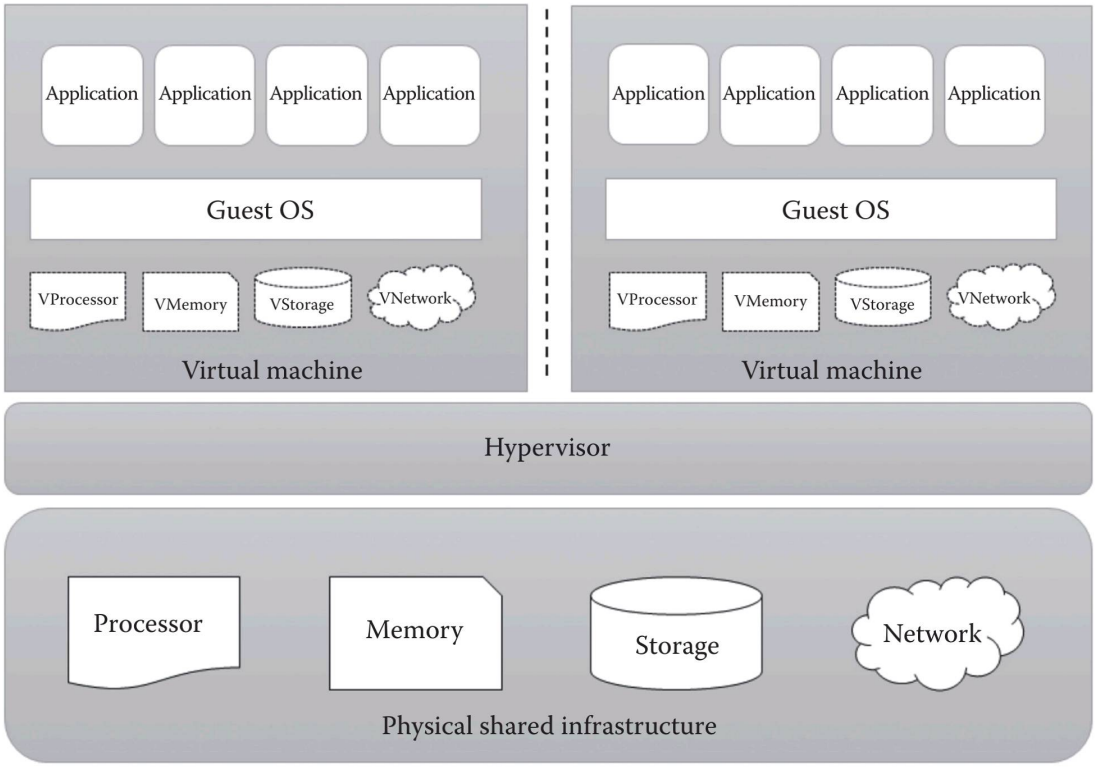

FIGURE 7.13
Type 1 or bare metal hypervisor.

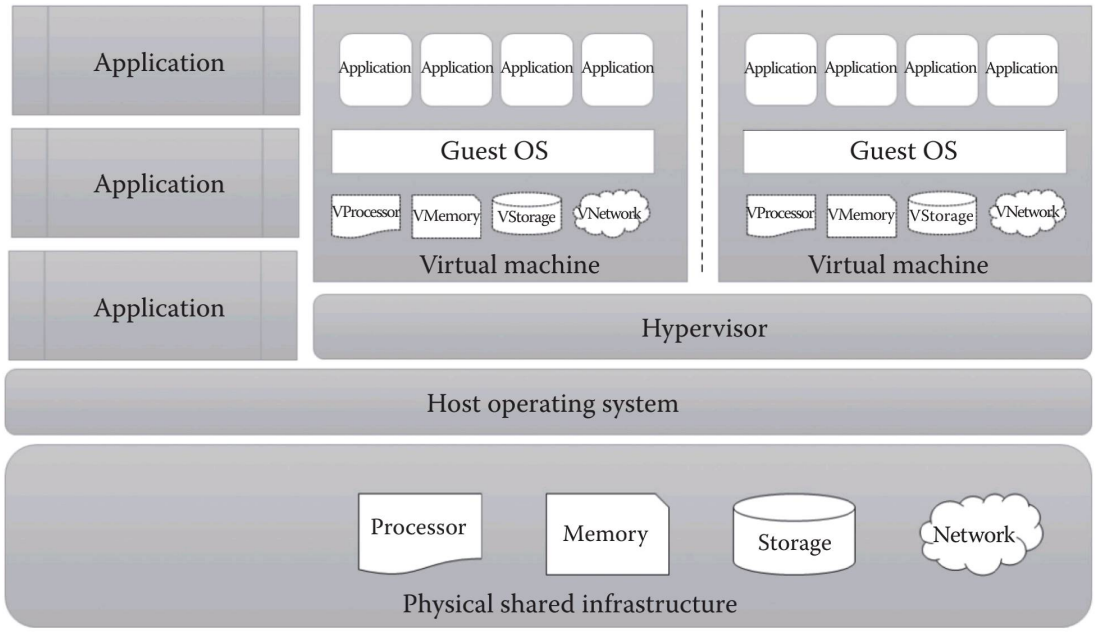

FIGURE 7.14
Type 2 or hosted hypervisor.

TABLE 7.2

Summary of Hypervisors

Hypervisor	Vendor	Type	License
Xen	University of Cambridge Computer Laboratory	Type 1	GNU GPL v2
VMWare ESXi	VMware, Inc.	Type 1	Proprietary
Hyper-V	Microsoft	Type 1	Proprietary
KVM	Open virtualization alliance	Type 2	GNU general public license
VMWare workstation	VMware, Inc.	Type 2	Shareware
Oracle Virtualbox	Oracle Corporation	Type 2	GNU general public license version 2

7.4.2 Security Issues and Recommendations

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:

1. Through the host OS
2. 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. The idea behind attacking the hypervisor through the host OS is illustrated in Figure 7.15. 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.

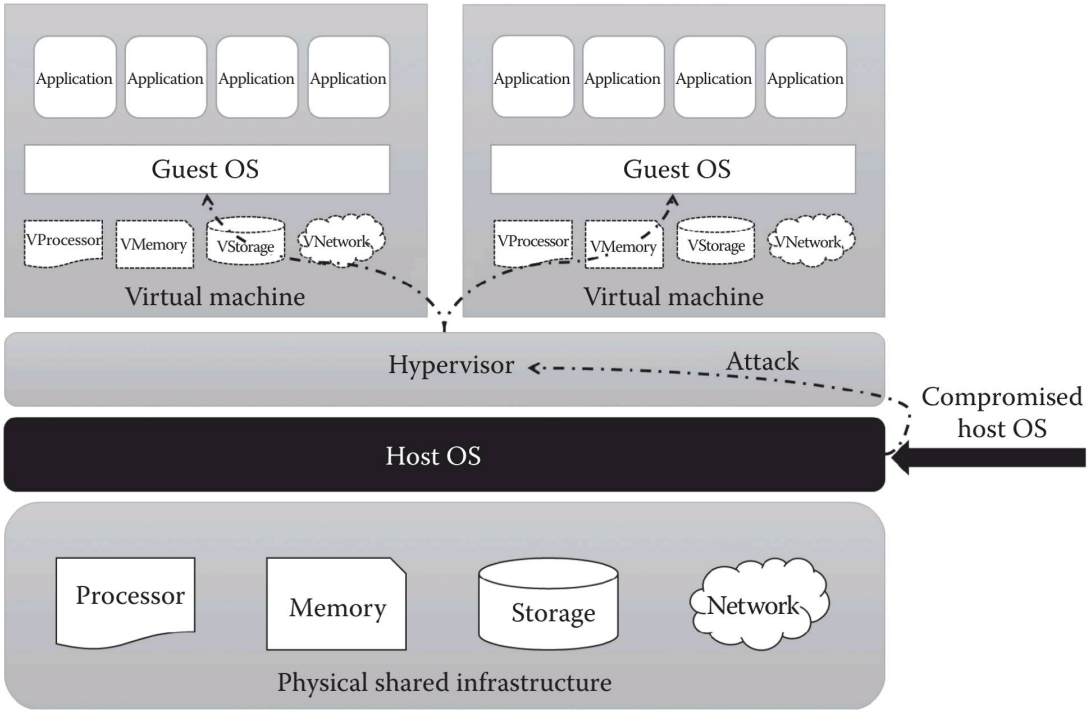

FIGURE 7.15
Attack through the host OS.

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. Normally, the attacks from the guest OS will try to abuse the underlying resources. The idea behind the attack through the guest OS is illustrated in Figure 7.16. As shown in the figure, the attacker will try to

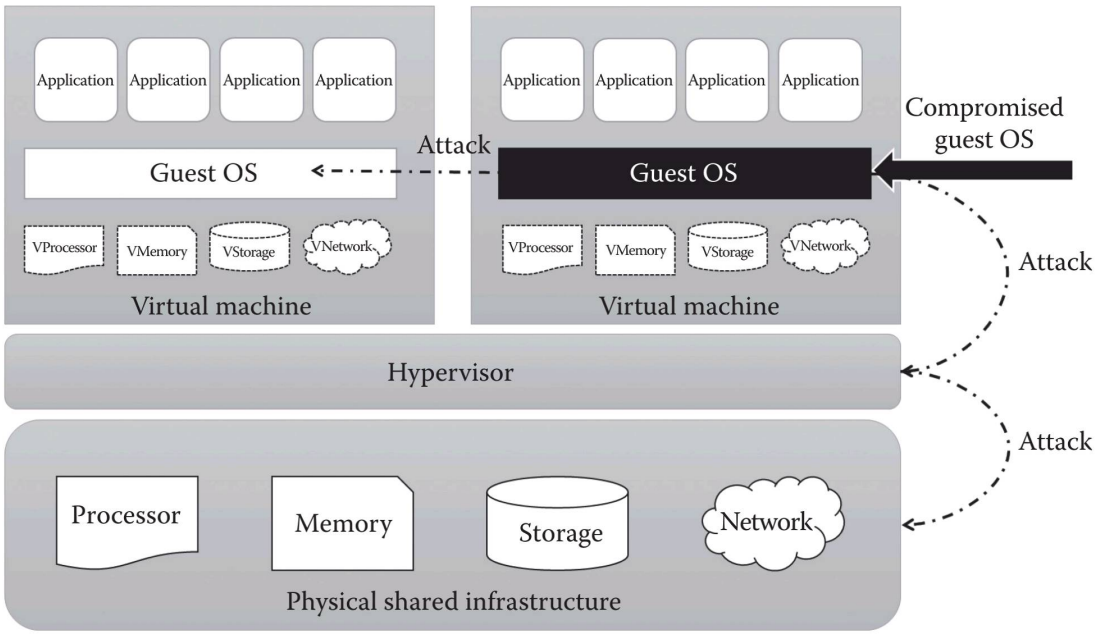

FIGURE 7.16
Attack through the guest OS.

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.

7.5 From Virtualization to Cloud Computing

Many users of current IT solutions consider the technologies *virtualization* and *cloud computing* as the same. But both technologies are actually different, or in other words, we can say virtualization is not cloud computing. We can prove this claim with the following parameters:

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*: One of the important characteristics that differentiate cloud computing from virtualization is 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*: The targeted audience of these two technologies is also different. 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.

With this short discussion, we can conclude that *cloud computing and virtualization are different*. But there might be some question that will arise from the IT owners: "I already invested more in virtualization technology, do I need to change everything to get the benefits of cloud computing?" The answer to this question is *no* as cloud computing uses virtualization for its service delivery. Cloud computing can run on any virtualized environment as virtualization is one of the enabling technologies for cloud computing. Of course, without virtualization, cloud computing might not exist. Cloud computing uses virtualization for better resource utilization and is coupled with utility computing to benefit service providers, developers, and end users. In other words, we can say that cloud computing takes virtualization to the next step. Cloud computing and virtualization converge in better resource utilization, and virtualization stops there whereas cloud computing moves one step ahead and joins utility computing to provide IT as a service. There are different cloud service models available, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS. In this section, we shall discuss how cloud computing uses the virtualization technology to provide different cloud services.

7.5.1 IaaS

The cloud computing service delivery model that allows the customers to access the resources as a service from the service provider data center

is known as the Infrastructure as a Service (IaaS) model. 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. Normally, for achieving IaaS services, type 1 hypervisors will be selected rather than type 2 hypervisors as the type 1 hypervisors are directly accessing the underlying hardware. IaaS is generally provided in the form of VMs that uses the virtual resources abstracted from the physical resources.

Normally, the real cloud data centers will contain the networked server machines for providing massive infrastructure services. So, whenever one server is overloaded with many VMs, the additional request will be migrated to the other free physical server by using the load balancer. There are many IaaS providers that are available in the market, which include Amazon, Microsoft, OpenStack, Eucalyptus, and CloudStack. The general service provisioning mechanism of IaaS services is illustrated in Figure 7.17.

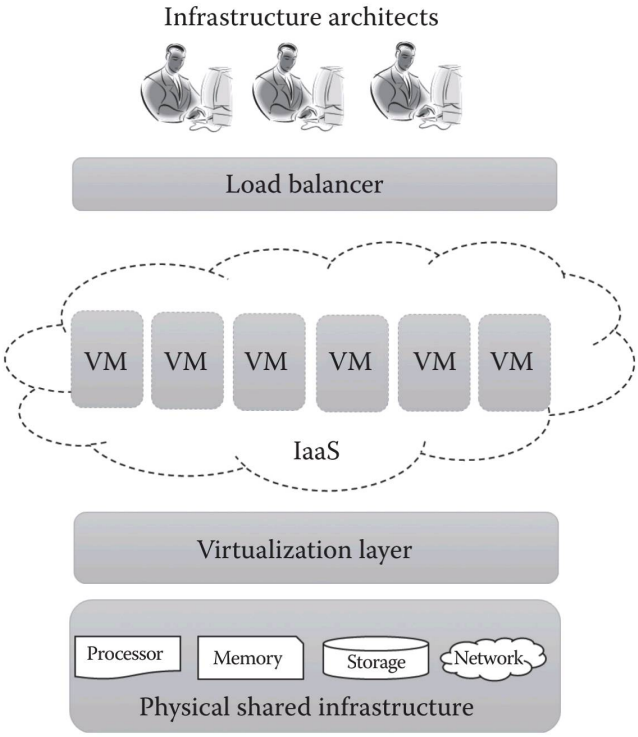

FIGURE 7.17
IaaS.

7.5.2 PaaS

The Platform as a Service (PaaS) allows the end user to develop and deploy the application online by using the virtual development platform provided by the service provider. Generally, 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. Generally, the deployment of application developed using the PaaS service depends on the type of cloud deployment model. If the end users select any public cloud deployment model, the application will be hosted as an off-premise application. If the users select the private deployment model, the application will be accessed as an on-premise application. Generally, 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. Here, application scalability is a very important factor. The scalability of the application can be achieved by the proper load balancer that transfers the extra load to the new server. Examples of PaaS service providers include Google App Engine, Microsoft Windows Azure, Redhat OpenShift, and force.com. A general overview of the PaaS service is illustrated in Figure 7.18.

7.5.3 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).

Generally, 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. SaaS utilizes application-level virtualization to deploy the application. The SaaS application allows multiple customers to share the same instance of an application. This technology is popularly known as multitenancy. Since many users are sharing the application, the load on the application will

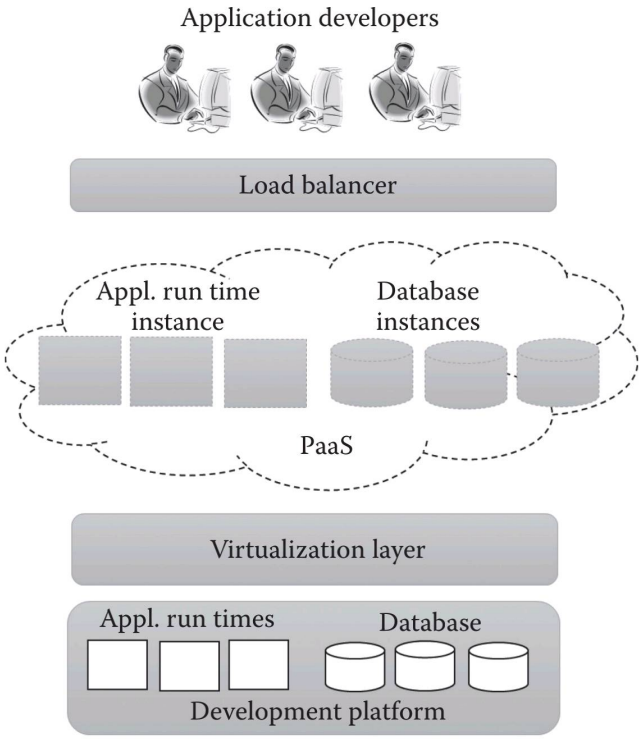

FIGURE 7.18
PaaS.

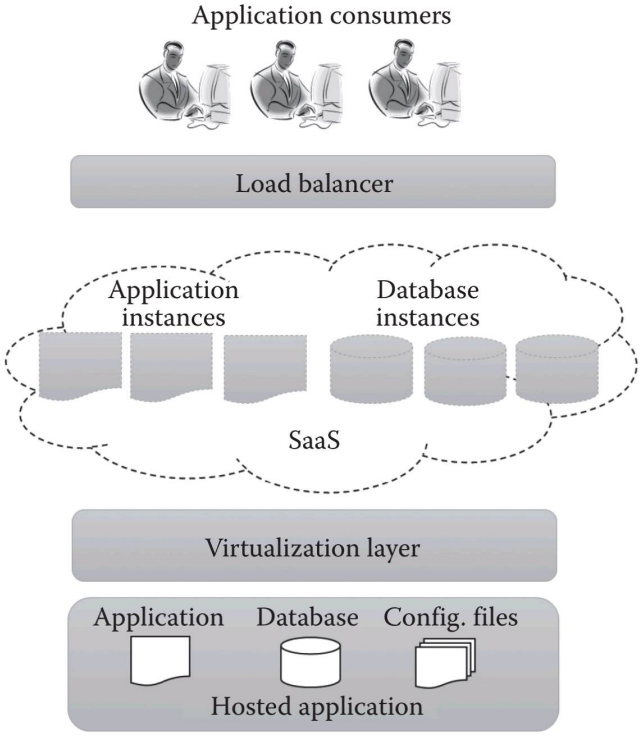

FIGURE 7.19
SaaS.

be more and unpredictable. The ability of handling the extra load decides the scalability of the application. The scalability of the application will be increased by the software load balancer, which will transfer the additional load to the new application/database server. Here, multiple application instances and database instances will be created to ensure high scalability. Some of the popular SaaS applications are Google Docs, Google Drive, and Microsoft Office 360. An overview of a SaaS application is illustrated in Figure 7.19.

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.

7.6 Summary

Virtualization is a widely used technology in the IT industry to increase resource utilization and ROI. It allows the same physical infrastructure to be shared between multiple OSs and applications. The other benefits of virtualization include dynamic data center, green IT support, ease of administration, and improved disaster recovery. There are three types of approaches used to achieve virtualization, namely full virtualization, paravirtualization, and hardware-assisted virtualization. Full virtualization completely abstracts the guest OS from the underlying infrastructure. Paravirtualization provides partial abstraction of the guest OS from the underlying infrastructure with slight modification of the guest OS. In hardware-assisted virtualization, the hardware vendor itself offers the support for virtualization. Hypervisors are the key drivers in enabling virtualization in large-scale cloud data centers. There are two types of hypervisors available, namely type 1 or bare metal hypervisor and type 2 or hosted hypervisors. Type 1 hypervisors can directly interact with the underlying infrastructure without the help of the host OS. Type 2 hypervisors need the host OS to interact with the underlying infrastructure. Since hypervisors are used as the enabling technology in virtualized data centers, there are different types of attacks targeted on the hypervisors to disrupt the servers. Normally, the attacks are performed by malicious codes to compromise the hypervisors. The attacks may target both the guest OS or host OS. The attacks can be mitigated by strong guest isolation, frequent updates, enabling least privilege policies, monitoring tools, etc. Virtualization helps in creating multitenant cloud environment, where a single instance of the resource can be shared by multiple users. Cloud computing and virtualization are different. Cloud computing uses virtualization with utility computing to provide different services such as IaaS, PaaS, and SaaS.

Review Points

- *Virtualization* is a technology that changes the computing from physical infrastructure to logical infrastructure (see Section 7.1).
- *Processor virtualization* is the process of abstracting physical processor to the pool of virtual processor (see Section 7.2.1).
- *Memory virtualization* is the process of providing virtual main memory to the VMs that are abstracted from the physical main memory (see Section 7.2.2).
- *Storage virtualization* is a form of resource virtualization where a multiple physical storage is abstracted as a multiple logical storage (see Section 7.2.3).
- *Network virtualization* is the process of abstracting physical networking components to form a virtual network (see Section 7.2.4).
- *Data virtualization* aggregates the heterogeneous data from a different source to a single logical or virtual volume of data (see Section 7.2.5).
- *Application virtualization* allows the users to access the virtual instance of the centrally hosted application without installation (see Section 7.2.6).
- *Protection rings* are used to isolate the OS from untrusted user applications (see Section 7.3).
- *Full virtualization* is the process of completely abstracting the underlying physical infrastructure with binary translation and direct execution (see Section 7.3.1).
- *Paravirtualization* or OS-assisted virtualization partially abstracts the underlying infrastructure with hypercalls (see Section 7.3.2).
- *Hardware-assisted virtualization* eliminates the overhead of binary translation and hypercalls, where the hardware vendors itself support virtualization (see Section 7.3.3).
- *Hypervisor* or VMM is a software tool that enables virtualization (see Section 7.4).
- *Bare metal hypervisor* or type 1 hypervisor can run on physical infrastructure without any help from the host OS (see Section 7.4.1).
- *Hosted hypervisor* or type 2 hypervisors require the help of the host OS to communicate with the underlying infrastructure (see Section 7.4.1).
- *Hypervisor attacks* mostly target the VMM by the malicious code either from the guest OS or host OS (see Section 7.4.2).

- *Cloud computing* is different from virtualization by means of type of service, service delivery, elasticity, etc. (see Section 7.5).
- *IaaS* uses the processor, memory, storage, and network virtualization to provide the infrastructure services (see Section 7.5.1).
- *PaaS* virtualizes the development platform and provides it as a service to the developers (see Section 7.5.2).
- *SaaS* allows the multiple end users to share the single instance of centrally hosted software (see Section 7.5.3).

Review Questions

1. What is virtualization? List its benefits and drawbacks.
2. Explain how virtualization changes the computing in the IT industry.
3. Briefly explain how hardware resources such as processor, memory, storage, and networks can be virtualized.
4. Write short notes on data virtualization and application virtualization.
5. What are protection rings? Explain how it is used in virtualization.
6. Explain the different approaches used to achieve virtualization with a neat diagram.
7. Differentiate full virtualization, paravirtualization, and hardware-assisted virtualization techniques.
8. What is the role of hypervisor in virtualization? Briefly explain the different types of hypervisors with a neat diagram.
9. Differentiate type 1 and type 2 hypervisors.
10. Explain the different attacks targeted on hypervisors with a neat diagram.
11. Recommend some of the best practices to avoid/prevent the attacks on hypervisors.
12. Are virtualization and cloud computing the same? Justify your answer.
13. Explain how cloud computing is different from virtualization.
14. Compare and contrast cloud computing and virtualization.
15. Explain how virtualization is used as an enabling technology in delivering cloud services such as IaaS, PaaS and SaaS.

Further Reading

Alam, N. Survey on hypervisors. School of Informatics and Computing, Indiana University, Bloomington, IL.

Business and financial aspects of server virtualization. White Paper, AMD.

Carbone, M., W. Lee, and D. Zamboni. Taming virtualization. *IEEE Security and Privacy* 6(1): 65–67, 2008.

Chen, W. K. *Virtualization for Dummies*. Hoboken, NJ: Wiley Publishing, Inc., 2007.

Goth, G. Virtualization: Old technology offers huge new potential. *IEEE Distributed Systems Online* 8(2): 3, 2007.

Li, Y., W. Li, and C. Jiang. A survey of virtual machine system: Current technology and future trends. *2010 Third International Symposium on Electronic Commerce and Security (ISECS)*, IEEE Computer Society, 2010, pp. 332–336.

Mann, A. Virtualization 101: Technologies, benefits, and, challenges. White Paper, EMA Boulder, CO.

Mosharaf Kabir Chowdhury, N. M. and Boutaba, R. A survey of network virtualization. *Computer Networks* 54(5): 862–876, 2010. ISSN 1389-1286.

Perez-Botero, D., J. Szefer, and R. B. Lee. Characterizing hypervisor vulnerabilities in cloud computing servers. *Proceedings of the 2013 International Workshop on Security in Cloud Computing (Cloud Computing '13)*, ACM, New York, 2013, pp. 3–10.

Reuben, J. S. A survey on virtual machine security. Seminar of Network Security, Helsinki University of Technology, Helsinki, Finland, 2007.

Scarfone, K., M. Souppaya, and P. Hoffman, Guide to security for full virtualization technologies. NIST Special Publication, 800-125, 2011.

The benefits of virtualization for small and medium businesses. White Paper, VMware, Inc., Palo Alto, CA.

Uhlig, R., G. Neiger, D. Rodgers, A. L. Santoni, F. C. M. Martins, A. V. Anderson, S. M. Bennett, A. Kagi, F. H. Leung, and L. Smith. Intel virtualization technology. *Computer* 38(5): 48–56, 2005.

Understanding full virtualization, paravirtualization, and hardware assist. White Paper, VMware, Inc., Palo Alto, CA.

Virtualization in education. White Paper, IBM.

Virtualization is not the cloud. Technical article, Rackspace Support. Available [Online]: http://www.rackspace.com/knowledge_center/sites/default/files/whitepaper_pdf/Rackspace_Virtualization%20Is%20Not%20the%20Cloud_20120503.pdf (Accessed December 30, 2013).

Virtualization overview. White Paper, VMware, Inc., Palo Alto, CA.