Virtualization Issues in Cloud Computing Service

1st Rakesh Pv
PG Scholar , Department of Computer Science
Christ Deemed To Be University
Bangalore, India
rakesh.pv@mca.christuniversity.in

***Abstract*—The ability of cloud computing to lower costs while enhancing scalability, performance, and flexibility for numerous activities has made it a well-known buzzword in today's society. In cloud computing environments, virtualization has grown in popularity and appeal. Sharing a single physical machine among numerous separate virtual machines results in more efficient use of the hardware and improves the migration of a virtual system relative to its physical counterpart. A key technology in a cloud environment is virtualization. However, including a second abstraction layer between software and hardware creates fresh security concerns. Due to several new security challenges, security concerns around virtualization technologies have become a significant worry for enterprises. The primary difficulties and dangers associated with virtualization in cloud computing systems will be discussed in this presentation. Additionally, it focuses on a few prevalent virtual-related threats and assaults that have an impact on cloud computing security.**

I. Introduction

The development of a cloud computing environment relies heavily on virtualization technology. It enables multiple operating systems to co-exist on the same physical server as virtual machines (VMs), using the dynamic resource allocation on the same machine without interfering with one another. The use of several instances of the same application on a single or several cloud resources is made possible by virtualization technology [1]. Multiple users being able to run their applications simultaneously is scaleability that the virtualization layer naturally enables. The user can execute their programs on a single virtual machine without having access to the data of other users

The rapid advancement of cloud computing has resulted in a several non-traditional security threats, and proposed a new and increased demand for information security. Even though the world's IT (Information Technique) companies have launched many of their cloud-computing products, the security problem has not been resolved due to a spate of security incidents; combined with the popularity of the concept of cloud computing, people to deepen their understanding of cloud computing, security has become the most significant concern.

Virtualization has resurfaced as a means of improving system security and delivering on the value of cloud computing. It allows businesses to cut IT costs while improving their existing computer hardware's efficiency, utilization, and flexibility. It gives organizations and people an opportunity to utilize and improve the use of their hardware by increasing the number and types of tasks that a single machine can handle . Resource sharing and isolation are two significant advantages in a virtualization environment. One of the essential advantages of virtualization is the ability to allocate physical resources to VMs based on their needs. More than one VM can run on the same host, and each VM can share the host's resources. Virtual machines share access to central processing units, disc controllers, physical network cards, etc.

Another advantage the virtual environment can provide is isolation; the VM isolates its data from other VMs. The failure of one VM has no bearing on the performance or execution of other VMs running on the same host. When a VM fails, it does not affect users' ability to access other VMs or other VMs on the same host's ability to access resources. Furthermore, isolation implies that programs running on one VM cannot see those running on another. This study aims to identify and understand the main challenges and security issues of virtualization in cloud computing environments. Furthermore, it presents baseline recommendations for improving security and mitigating risks encountered virtualization to adopt secure cloud computing

II. SECURITY CHALLENGES AND RISKS

A. User awareness

Because cloud service providers do not monitor their customers' surroundings, cloud service users are the weakest link in any information security system. Suspicious user accounts can enable attackers to conduct malicious activities undetected. Additionally, an attacker could use attack vectors for various social engineering techniques to visit malicious websites and gain access to the user's computer. It can then observe user actions, see the same data as the user, and steal user credentials to authenticate the cloud service. A frequently overlooked security concern is security awareness.

B. Insecure APIs

A cloud computing provider provides users with infrastructure, software, and platform services, which they can access via interfaces. They created their interfaces using publicly available application programming interfaces. APIs pose several security issues, including improper authorizations, weak credentials, and clear-text transmission, which can impact the availability and security of cloud services

C. Inadequate security policies

The organization defines security policies to determine how to protect its assets from potential threats and deal with such situations when they arise. The cloud service provider's security policies may be insufficient or incompatible with an organization's security requirements. Inadequate security policies may expose some vulnerabilities, creating an insecure VM environment.On another side, VMs can be moved between physical environments as required. When a VM is migrated or moved from the source host to another, the destination host might not have enough security to protect the VM. Mobile VMs need baseline histories and security policies to move with them.

D. .Inadequate authentication and session management

Authentication techniques protect the system from bad actors who pose as legitimate users, developers, or operators to read, delete, or modify data. A virtual environment's authentication mechanism applies to end users and system components. Improperly designed or implemented authentication and session management application functions may impact access and control policy [6]. Furthermore, it allows attackers to compromise keys, session tokens, or passwords and exploit

E. Incorrect VM isolation

The hypervisor ensures VM isolation. The isolation between VMs prevents one VM from accessing another VM's virtual discs, applications, or memory on the same host. Furthermore, VM isolation limits the attack's scope. It complicates access to resources and sensitive data on the physical machine. An isolation violation occurs when an attacker communicates with other VMs on the same host using a compromised VM. As a result, a shared environment necessitates precise configuration to maintain strong isolation.

F. Insecure VM migration/mobility

The benefit of virtualization is the ability to transfer applications transparently from one host machine to another without stopping the VM. After migration, the application continues to run without interruption. The user is unaware that his VM has been migrated. The VM is migrated by copying the VM's application and the entire system state, including memory, CPU state, and sometimes disc, to the destination host. During migration, however, the attacker may steal and snoop or actively modify confidential information. As a result, the transmission channel must be protected and secured from various passive and active attacks.

III. PROBLEM DEFINITION

One of the most severe threats to virtualization and cloud computing is malicious software that allows computer viruses or other malware that have infiltrated one computer's system to spread to the underlying hypervisor and, eventually, to the design of another customer. In a nutshell, one cloud computing customer could download a virus, such as one that steals user data, and then spread that virus to all other customers' systems.

A. Solution of the above problem

To prevent this, Hyper safe employs two components. The hyper-safe program uses a technique known as non-passable memory lockdown, which explicitly and reliably prevents anyone other than the hypervisor administrator from introducing new code. This also prevents external users from modifying existing hypervisor code. The technique used by Hyper-safe is known as restricted pointer indexing. This technique is known for first characterizing a hypervisor's normal behavior and then preventing any deviation from that profile. Only the hypervisor administrator can modify the male hypervisor code.

IV. VIRTUALIZATION THREATS AND ATTACKS

A. Cross-VM Attack:

When a malicious virtual machine bypasses hypervisor-level isolation to attack co-located VMs, this is referred to as a cross-VM attack. Cross-VM attacks range from controlling other VMs by exploiting guest or hypervisor vulnerabilities to gaining personal data via side-channel attacks. Several VMs are co-residents on a single server to maximize resource usage; this co-resident placement may result in a cross-VM side-channel attack. A cross-VM side-channel episode begins with a co-location attack and poor isolation method implementation; a malicious VM conducts side-channel raids. As a result, sensitive information can be extracted to continue the attack using a different method to gain control of the entire system.

B. VM Rollback

Without VM awareness, the hypervisor can pause a running VM, capture a snapshot of the current disc, memory, and CPU states, and resume the image in the future. This feature is used for VM maintenance and fault tolerance, but it also allows the attacker to launch a VM rollback attack. The attacker can use old VM snapshots to run them without the user's knowledge, then delete the history of the VM execution and execute a different or identical shot again. Because the VM execution history is lost, the attacker can avoid or undo updates to some security mechanisms.

C. VM Sprawl

It occurs when the number of VMs on the same host continues to grow without control, and some are idle. Because VMs retain system resources such as network channels and memory, these system resources are effectively missing and cannot be allocated to other VMs. VM sprawl is a problem for cloud providers because many VMs necessitate a large amount of memory

D. VM Escape

A VM avoids a threat designed to exploit a hypervisor. It is a situation in which a malicious VM or user escapes the hypervisor's control. Malware software running in a VM can bypass the isolation between the VMs and the host in VM escape. As a result, the attacker gains access to the hypervisor, causing the entire system to fail. When the attack is successful, the attacker gains access to the storage hardware, computing power, shared resources, and other virtual machines.

E. VM Hopping

The process of jumping from one VM to another by exploiting vulnerabilities in the hypervisor or virtual infrastructure is known as VM hopping. Because the hypervisor has high privileges, using it would have serious consequences. When attackers gain malicious access to other users' VMs, they can monitor the target VM's resources, changing its configurations, removing stored data, and affecting the VM's integrity, availability, and confidentiality.

F. Hyperjacking

The hyperjacking attack inserts VM-based rootkits into the virtualized environment to control the entire virtualized environment. It injects and modifies a fake hypervisor beneath the original one. A VM-based rootkit established a covert channel to the hypervisor for malicious injection code, hiding it from the security mechanism. Because the hypervisor operates at a system's highest level of privilege, it would be challenging, if not impossible, for any operating system (OS) running on the hypervisor to detect it.

V. RECOMMENDATION

A. User Awareness

To counter any attempt to tamper with the system, user awareness is essential to any plan. All parties involved, including service providers and organizations, must focus on staff education and training and use assurance processes to evaluate human resources. Small and medium-sized businesses, corporations, and government agencies can help raise user awareness by encouraging their professional staff to attend skill-building training courses at relevant institutes. End users should be aware of their rights and the threats to their privacy in virtual environments by participating in relevant courses and instructional activities.

B. Secure Host OS

Because the virtualization layer exists above the operating system (OS), protecting the OS on the host machine is critical. A compromised operating system provides an ideal environment for attacking the virtualization layer. Service providers must update the operating system version, remove or disable unnecessary software and services, and install a host intrusion detection system and anti-virus.

C. Secure the Hypervisor

The hypervisor is an additional software layer that sits between virtual machines and the underlying hardware, with or without a host operating system. Some hypervisors check for and install updates automatically. Updates can be administered using centralized patch management solutions. Disconnecting unused devices from the host can aid in hypervisor security. It is preferable to harden the hypervisor configuration to reduce areas of vulnerability.

D. Protect the VM

A virtual firewall is required to prevent VM-to-VM attacks, and a robust authentication mechanism is needed to avoid unauthorized access to VM. If a virtual machine is compromised, we must assume that all VMs on the same server is compromised. In this case, restore each guest OS to a previous good image or snapshot before the compromise. As a result, making a backup of the virtual drive used by the guest OS is a good idea. We must isolate and protect the memory of guest VMs from other VMs sharing the same physical system and from an untrustworthy hypervisor.

VI. CONCLUSION

Virtualization is a widely used technique for extending the capabilities of physical computers by dividing resources among operating systems. Virtualization enablesmany instances of the same application on one or more cloud resources. In this study, we investigated the common challenges and risks of virtualization technology, as well as the main threats and attacks that may compromise virtualized systems in cloud computing environments.

REFERENCES

[1] . Geelan (2008),"Twenty one experts define cloud computing,"Virtualization, Electronic Mag., article available at http://virtualization.sys-con.com/node/612375.

[2] B. Loganayagi and S. Sujatha, "Creating virtual platform for cloud computing," in Proc. 2010 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1

[3] L. Garber, "The Challenges of Securing the Virtualized Environment," Computer, vol. 45, no. 1, pp. 17-20, 2012

[4] Cloud Security Alliance,"The Notorious Nine. Cloud Computing Top Threats in 2013," CSA, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.cloudsecurityalliance.org. [Accessed: Oct.-2017].

[5] Cloud Security Alliance,"The Notorious Nine. Cloud Computing Top Threats in 2013," CSA, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.cloudsecurityalliance.org. [Accessed: Oct.-2017].

[6]] A. Parashar and A. Borde, "Cloud Computing: Security Issues and its Detection Methods," Int. J. of Engg. Sci. Mgmt., vol. 5, no. 2, 2015, pp. 136–140

[7] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning,"Managing security of virtual machine images in a cloud environment," in Proc. ACM workshop on Cloud computing security - CCSW '09, 2009, p. 91.