Security of Cloud Computing with Infrastructure of Virtualized Network

Dr. Neelam Dahiya
Associate Professor
Government P.G. College
Sector 9, Gurugram.
Gurugram University
Email: dahiyaneedahiya@gmail.com

Abstract

Despite the rapid development in the field of cloud computing, Security is still one of the major hurdles to cloud computing adoption. Most cloud services such as Amazon EC2 are offered at low cost without much protection to users. At the other end of the spectrum, highly secured cloud services (e.g. Google "Government cloud") are offered at much higher cost by using isolated hardware, facilities, and administrators with security clearance. In the Paper, we explore the "middle ground" where users can still share physical hardware resources, but user networks are isolated and accesses are controlled in the way. Similar to that in enterprise networks, we believe this covers the need of most enterprise and individual users.

Keywords

Cloud, Networks, Security, Isolated.

Reference to this paper should be made as follows:

Received: 06.02.2023
Approved: 15.03.2023

Dr. Neelam Dahiya

Security of Cloud Computing with Infrastructure of Virtualized Network

Article No.03
RJPSS Oct.-Mar. 2023,
Vol. XLVIII No. 1,
pp. 018-025

Online available at:
https://anubooks.com/rjpss-2023-vol-xlviii-no-1/

https://doi.org/10.31995/rjpss.2023.v48i01.003

https://doi.org/10.31995/rjpss.2023.v48i01.003

Introduction

Cloud computing is an efficient way to increase the capacity dynamic scalability or add capabilities using virtualization resources, platforms, infrastructure and software as a service that can be accessed over the internet. To improve the utilization of cloud resources we use Virtual Machines (VMs). A virtual machine is a virtual computer similar to a physical computer in which an application or operating system can be installed and run.

Despite the rapid development in the field of cloud computing, security is still one of the major obstacles to cloud computing adoption . To ease the concerns of IT managers, it is critical to ensure data privacy and integrity in the cloud at a level that is at least comparable to that in current enterprise networks. However, the current cloud computing services fall in short of isolating computing resources and networks between customers. This is not surprising because the success of cloud computing depends on the economy on large scale. It is essential for cloud service providers to take advantage of resource sharing and multiplexing among customers. Virtual machines of different customers may reside on the same physical machine, and their data packets may share the same LAN. Virtualization is an innovative technology , which is significantly expanding in the Information Technology industry. It provides multiple logical resources on a single server. Various benefits that can be provided by virtualization are hardware utilization, resource protection, remote access, and other resources. This technique gives organizations and people an opportunity to improve the use of hardware by increasing the number of tasks that one machine can handle.

Virtualization is used to match the customers' requirements for security, control, economy, scaling, speed, and so forth. It may affect the choice of cloud service provider. Furthermore, it empowers the cloud users to start up and shut down their resources rapidly, which can be in some applications has its advantage.

In this paper, we explore the "middle ground", where users can still share physical hardware resources, but user networks are isolated and accesses are controlled in a way similar to that in enterprise networks. We believe this covers the need of most enterprise and individual users.

Virtualization Network

Virtualization architecture is a model, which determines the interrelationships among particular virtual components, such as an operating system, network resources, servers, and storage spaces. In general, the virtualization is based on a hypervisor. The hypervisor isolates operating systems and applications from system hardware, whereas the host can run multiple Virtual Machines (VM) as

guests that share the physical resources of the system, such as processors, memory, network bandwidth, and so forth. Virtualization architecture might be divided into two types, hosted and bare-metal architectures .

In hosted architecture, first, an essential Operating System (OS) is installed on the host system, and then a hypervisor or VM monitor software is installed on the top of the OS. This OS-based architecture entirely enables the user to control multiple guest OSs, or VMs installed on the hardware. Hosted virtualization architecture is substantially less complex to implement, and it is more useful for software development, running legacy applications, and supporting different operating systems. However, it has some severe disadvantages due to controlling the virtual machines by operating system directly. Therefore, it turns out to be more straightforward for an attacker to inject malicious attacks or DOS attacks into the kernel of the operating system. The entire virtualization infrastructure can be influenced, and the attacker can have control over all virtual machines and might be able to damage the virtual machines later. In the second architecture, the hypervisor runs directly on the host hardware. Like hosted architecture, VMs and higher-layer applications are installed above the hypervisor.

The cloud-computing environment can be virtualized on every layer of cloud computing services, such as IaaS resources including virtualized storage, networking, and servers, or virtualized datasets, and development environments in PaaS, and any software application instances. The rapid expansion of cloud computing and virtualization technology makes cloud infrastructure more complicated and has brought a series of security threats. This study aims to identify the main challenges and security issues of virtualization in cloud computing environments.

Virtualization Challenges

Many vulnerabilities and risks are existing in current virtualization technologies that an attacker can exploit to penetrate the security and privacy systems in cloud computing environments. In this study, we have classified vulnerabilities into several categories regarding their characteristics and relevance to virtualization technology.

Virtualization Characteristic-Related Issues

The essential characteristics that make virtualization technology suitable for cloud computing are mobility, transience, state recording, isolation, and scalability. Although all these characteristics constitute a successful virtualization environment, the characteristic of virtualization technology causes some risks to cloud systems. This section demonstrates common vulnerabilities and risks that may arise due to a characteristic of virtualization technology.

https://doi.org/10.31995/rjpss.2023.v48i01.003

Incorrect VM Isolation (VC1)

The hypervisor is responsible for ensuring isolation between the different VMs9. The isolation between virtual machines prevents the VM from direct access to others' virtual disks, applications, or memory on the same host10. Isolation of virtual machines limits the scope of the attack. Furthermore, the isolation of virtual machines makes it more difficult for the attacker to access resources and access unauthorized data on the physical machine. Each VM is isolated from the other virtualized machines and its host physical system, so if one VM is broken-down, it does not affect any of the other VMs on the same host. A violation of the isolation principle happens when the attacker uses a compromised VM for communicating with other VMs on the same host.

Unsecured VM Migration/Mobility (VC2)

The migration technique is one of many advantages of Virtualization. It enables the application to transparently transmit from one host machine to another without halting the virtual machine. After migration, the application continues in execution without any loss of progress. VM migration is done by transmitting the application along with its VM's entire system state, including memory, the state of CPU, and sometimes disk too, to the destination host. VM migration offers many valuable advantages such as load balancing, and conserving energy.

VM Diversity (VC3)

Many IT enterprises overcome the problem of security by enforcing homogeneity, as all devices must have the latest patching software. Virtualization can facilitate more efficient usage models that get the benefit of implementing older or unpatched versions of the software.

Uncontrolled Scaling (VC4)

Virtualization technology allows the creation of new virtual machines easily and quickly on demand. Scalability provides a very cost-effective way to handle business expansion and any additional resources of the server requirements. Users can have several particular purposes for virtual machines, for example, for testing or viewing purposes.

VM Transience (VC5)

In the physical computing environment, users have one or more devices that run online most of the time and are in a stable state. In contrast, VMs in a virtualized environment can come and go from the network intermittently.

Access and Communication Security Issues

The user's interaction with the cloud begins when he attempts to access

cloud services. The user must first authenticate his identity before accessing cloud services. The communication process arises when the user and the cloud exchange data or services. Furthermore, there are communications between VMs within the cloud that introduce vulnerabilities that may affect the host machine and all VMs running on it. An illegal user can exploit access and communication vulnerabilities related to access and communication security.

Hidden Identity (AC1)

In physical computing environments, there is usually a custom identity correlated to a physical device such as MAC addresses, or device IDs. It is used to differentiate between devices and determine who the owner of a machine is. This static method is not effective in virtual environments due to creating VMs dynamically or mobility of VMs that make it very difficult to identify or track the owner of a VM running on a particular physical host.

Insecure Channel (AC2)

The cloud service providers use the Internet as a communication infrastructure to provide services to customers or transfer their data. An efficient and secure transmission channel is a critical component in a cloud environment and forms the basis for managing information and any related processes. When transmitting the data from users to the cloud environment, the data must be sent using an encrypted secure transmission channel such as SSL/TLS. It protects network traffic against a potential interception attack.

VMs-VMs or VMs-Host Communications (AC3)

In a cloud-computing environment, communication mechanisms in virtual networks are similar to those used in real networks. In the same way that physical devices are connected, virtual machines are connected and built on a network infrastructure of the host to connect to the public network. VMs need to communicate and share data. If the connection does not meet critical security standards, they become a target for attacks.

Weak Authentication and Session Management (AC4)

Authentication is a mechanism used to determine whether something or someone is what or who it is declared to be. Authentication techniques protect the system against bad actors that masquerade as legitimate users, developers, or operators to read, delete, and modify data. In a virtual environment, the authentication mechanism applies to end users and to components of the system. Most of the widely utilized authentication methods are poor and may affect access and control policy. Sometimes, it is easy to break some authentication mechanisms

that have weaknesses in their design, such as one-factor authentication mechanisms, to get access to the system.

Virtualization Security Solutions

Many types of research offer solutions for virtualization security. These solutions may be useful for centers and organizations interested in developing cloud security solutions and standards. In this section, we focus on some solutions covered in the literature survey. HyperSafe is an approach proposed to provide control-flow integrity for the Type-I bare-metal hypervisors. This approach relies on two techniques. The first one protects the code integrity of the hypervisor by preventing memory pages from being manipulated at execution time. Authors have used the Write Protect bit (WP bit) to check how the supervisor code acts with write-protection bits in page tables. The write-protection is skipped if the WP is off, otherwise, it is decided if the supervisor can write or not to the memory page. In order to allow the good updates to proceed, the WP bit is temporarily cleared right before each update and then re-enabled immediately after the update. The other techniques protect control data by converting them into restricted pointer indexes. It extends the protection provided by the first technique from code integrity to control-flow integrity to prevent attackers from controlling the flow of the system. HyperSafe aggregates control data into target tables and then replaces them with a restricted pointer index. A VM security monitoring model based on memory introspection has been proposed. The security of the host or VM can be recognized by using a hardware-based approach to obtain the real-time physical memory of the host. Moreover, a VM Control Structure (VMCS) based approach is proposed for VM memory forensics. Based on the results of memory forensics of the host/VM malicious behavior can be detected. These techniques were used to develop a prototype of a VM defense system that is called VEDefe VEDefender, which incorporates a PCI device and a terminal program.

The VEDefender prototype was implemented on top of a kernel-based VM (KVM). VEDefender is transparent to the guest machines, and it is hard to be accessed even from a compromised VM. It can gather and analyze data for discovering any malicious activity whether being on the host or guest machine. Experiments results show that the proposed system can deal with virtual machines from different OS versions and have an acceptable execution time.

Conclusion

The rapid expansion of cloud computing and virtualization technology makes cloud infrastructure more complicated and has brought a series of security challenges. This research has identified critical security issues of virtualization technology in

cloud computing environments. The collective security vulnerabilities and risks have been classified into several categories according to their effect on virtual environments. Furthermore, security threats and virtual-based attacks have been presented according to virtualization uses of the vulnerabilities and security risks. In this study, we have reviewed some solutions and alleviation techniques suggested in the literature review for improving the security of cloud virtualization systems. Finally, these reviewed mitigation techniques are compared according to five specified security criteria; data confidentiality, data integrity, securing the hypervisor, securing the VM, and access control.

References

1. A taxonomy and survey of cloud computing systems. Available from: https://ieeexplore.ieee.org/document/5331755.
2. Chatzikyriakidis, I. (2011). Trends and risks in Virtualization. Kingston University: London. Pg. **1–97.**
3. Virtual machine security guidelines; 2017. Available from: https://www.cisecurity.org/wpcontent/uploads/2017/04/CIS_VM_Benchmark_v1.0.pdf.
4. (2009). Demystifying the cloud: Important opportunities, crucial choices. Global Netoptex Incorporated. Pg. **4–14.**
5. Haeberlen, T., Dupre, L. (2016). Cloud computing: benefits, risks, and recommendations for information security. European Network and Information Security Agency. Pg. **1–50.**
6. Bulusu, S., Sudia, K. (2012). A study on cloud computing security challenges. Blekinge Institute of Technology. Pg. **1–137.**
7. Infrastructure as a Service Security: Challenges and Solutions. Available from: 11. A survey on the security of virtual machines. Available from: http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec/.
8. Birje, M. (2015). Security issues and countermeasures in cloud computing. *International Journal of Applied Engineering Research*. 10(86). Pg. **71–5.**
9. Wu, H., Ding, Y., Winer, C., Yao, L. (2010). Network security for virtual machine in cloud computing. 5th International Conference on Computer Sciences and Convergence Information Technology. Pg. **1–4.**
10. Anala, M., Shetty, J., Shobha, G. (2013). A framework for secure live migration of virtual machines. *International Conference on Advances in Computing, Communications, and Informatics*. Pg. **243–8.** https://doi.org/10.1109/ ICACCI.2013.6637178.

11. (2015). Cloud security alliance. Best Practices for Mitigating Risks in Virtualized Environments. Pg. **1–35.**
12. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P. (2009). Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACM workshop on Cloud Computing Security. Pg. **91–6.** https://doi. org/10.1145/1655008.1655021.
13. Modi, C.N., Acha, K. (2017). Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. *The Journal of Supercomputing*. 73(3). Pg. **1192–234.** https://doi. org/10.1007/s11227-016-1805-9.
14. Reuben, J.S. (2007). A survey on virtual machine security. Seminar on Network Security. Pg. **1–5.** 28. Ranjith, P., Priya, C., Shalini, K. (2012). On covert channels between virtual machines. Journal in Computer Virology. 8(3). Pg. **85–97.** https://doi.org/10.1007/s11416-012-0168-x.
15. Cloud Computing: Security Risk, SLA, and Trust. Jönköping University. Available from: http://hj.diva-portal.org/smash/record.jsf?pid=diva 2%3A323596&dswid=-3340.
16. Batra, S., Applications, C., Group, C. (2013). Preliminary analysis of cloud computing vulnerabilities. *International Journal of Innovation Science and Research*. 2(5). Pg. **49–51.**
17. Khorshed, T., Ali, A., Wasimi, S. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems. 28(6). Pg. **833–51.** https:/ /doi. org/10.1016/j.future.2012.01.006.
18. Security issues in cloud computing. Available from: https://ieeexplore. ieee.org/document/6513028.
19. Threats to virtual environments. Security Response. Available from: https:/ /www.symantec.com/content/dam/symantec/docs/security-center/white-papers/threats-tovirtual-environments-14-en.pdf.
20. Xianqin, C., Han, W., Sumei, W., Xiang, L. (2009). Seamless virtual machine live migration on network security enhanced hypervisor. IEEE International Conference on Broadband Network and Multimedia Technology. Pg. **847–53.** https://doi.org/10.1109/ICBNMT.2009.5347800.