Analyzing the Security Risks and their Probable Solutions for Virtualization in Cloud Computing

Santanu Mondal
Michael Madhusudan Memorial College, Durgapur, India

Bubai Das
J. K. College, Purulia, India

Kunal Kumar Mandal
Mankar College, Mankar, India
Corresponding author: Bubai Das, Email: bubai.jkc@gmail.com

Cloud computing has become the platform for different web services. It is because of the technology virtualization, which enables cloud providers to provide service for a large number of customers. It is cost-effective and it also enables an efficient way of data storage and data processing to provide service for a large number of customers. But there is a disadvantage also. There can be a risk of security breach if proper precaution is not taken. The main characteristics of virtualization are resource sharing and isolation. This is the strength of virtualization. But there can be a problem of security if used without taking proper precautions. The environment makes it prone to bugs and the whole system can be damaged by one malicious virtual machine in the cloud. This attacks other virtual machines in the cloud. This paper studies different risks in virtualization and analyses the different methods to overcome them and make the environment less vulnerable to risk.

Keywords: Virtualization, Hypervisor, Virtualization Security.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 383–392. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-40

1 Introduction

Cloud computing is a pool of computing resources that can be shared among users in a network-based environment. Here not only the resources but computation will be shared also. These will be shared by virtualization techniques. Through network infrastructure, cloud providers use this technique with self-service abilities of computing resources via network infrastructures. On the same physical server Internet and multiple virtual machines are hosted. A cloud computing platform has the ability to recover the workload from any software or hardware failure because it supports self-recovering, redundant, highly scalable programming models. Therefore, in clouds, customers have to pay only for what they want to use not for different local resources. In Virtualization a physical computer is divided into several isolated machines. This division can be partial or complete and these division machines are commonly known as virtual machines (VM) or guest machines. In a host computer, multiple virtual machines can run with their operating system and applications. This creates an illusion to the different processes of these virtual machines as if they are running on an individual physical computer, but they are sharing the physical resources of the host machine. There will be isolation between the programs running in different virtual machines. In a virtual environment, there are more numbers of entry points, more interconnection points. So, proper security arrangements are needed. The security expectations are higher here because of more possible points of entry, more holes to patch and there are more interconnection points in the virtualized environment. Deployment of malicious virtual systems, Low-level hypervisor attacks is a few common possible attacks for this virtualization environment. Different new security techniques are also coming into the market from different vendors which are mainly focused on the hypervisor. Between Host OS and the virtual environment, the hypervisor is a new layer. However, virtual machine security not just introducing a new secure hypervisor layer in the environment.

This paper is organized as follows. Section 2 describes briefly the virtualization and its components. Section 3describes the different security issues and Section 4 describes its countermeasures. Section 5 describes the conclusion and future work.

2 Virtualization and its component

Virtualization is a concept of a logical system that has the same functionalities as of physical system. It is a simulation of the software and hardware on which other software runs. The environment is called a virtual machine (VM) [1]. It is part of the physical system. Virtualization framework divides actual the resources of a physical machine like CPU, memory, storage disk, etc. will be divided into different virtual machines in this environment. These virtual machines act as standalone machines with their own OS and applications.

Desktop virtualization, Server Virtualization, Memory, storage, network virtualization are the different categories of virtualization. This paper focuses on Server virtualization where a virtual machine or logical computer with its own OS (guest OS) has been created by sharing the physical resources of the host machine or physical computer.

Three types of Server Virtualization are there:

- **Full Virtualization:** In this mode the virtual machine's OS or guest OS is not aware of the virtualization and requires no modification. Hypervisor handles the privileged instructions by binary translation and communicates to the hardware.

- **Para virtualization**: In this mode, there will be a communication between the hypervisor and guest OS. It improves efficiency and system performance. Instead of privileged instructions here in this mode virtual machine's OS or guest OS hypercalls the hypervisor.
- **Hardware assisted virtualization**: In this mode, modification is done with the processor with an additional privilege level. A new set of instructions was designed which identifies instructions requested by the guest and takes the help of hypervisor to deal with the privileged instructions of guest.

Hypervisor

Hypervisor is a component of computing system which drives virtualization. It is also known as Virtual Machine Monitor (VMM) . Hypervisor or VMM manages operating system or higher-level applications. The hypervisor manages requests by virtual machines to access the hardware by creating isolation paths for virtual machines. On top of the hypervisor different operating systems run in different virtual machines.

Two types of hypervisors are there:

- **Type I or Native hypervisor**: Hypervisor directly runs at the top of the hardware and monitors the operating systems running above it. These are also called bare-metal hypervisors.
- **Type II or Hosted Hypervisor**: Hypervisor runs under the Host OS & then supports other operating systems.

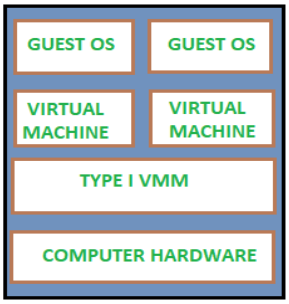

Fig. 1. Type I hypervisor

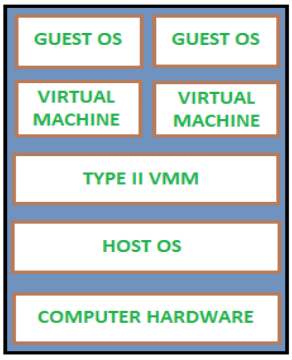

Fig. 2. Type II hypervisor

3 Virtualization Security Issues

In a computing environment virtualization is the concept of logical system which is similar as physical system and provides same functionality. Actually it is a part of physical system. In Virtualization the resources of a physical machine like CPU, memory, storage disk, etc. are becomes divided into different virtual machines and each virtual machine runs as a standalone machine with its own operating system and set of applications. But due to addition of extra layer it attracts the attackers also. Due to numerous numbers of entry points and interconnection complexity in virtualization providing security is a big challenge.

3.1 Virtual Machine Monitor

Virtual Machine Monitor also known as Hypervisor drives the virtualization in computing system. It is a layer between the host system hardware and the virtual machine or guest machine, which imitates the system hardware to guest machines created on the host. To assist guest OS interaction with the host system hardware few mechanisms are implemented in hypervisor but this feature can be a security threat for the system. Interaction between the guest OS with the hypervisor is direct and with the host machine it is indirect through the VM exits [2]. VM Exits are the mechanism used by the Hypervisor uses VM Exit mechanisms to intercept with the guest VMs and carry out operations invoked by guest VMs. A malicious Virtual Machine can inject malicious code in hypervisor or trigger a bug in the hypervisor by using VM Exits. To violate confidentiality or integrity or to slow down the hypervisor or to crash the system injecting code or triggering a bug can be used by malicious VM.

3.2 Shared Resource

Virtual Machines can share CPU, Memory, Input /Output devices etc. if they are located on same server. Due to this sharing each Virtual Machine will be under security threat. a malicious VM can infer some information about other VMs through shared memory or other shared resources a malicious virtual machine can predict some information about other virtual machine. Virtual machines can communicate using some hidden channel bypassing all the security protocols assigned by VMM [3]. This way a malicious Virtual Machine can monitor the system, the shared resources without being noticed by its VMM and predict information about other VMs.

3.3 Public VM Image Repository

VM image is a prepackage template which contains configuration files that are used to create a virtual machine. These VM images are fundamentals for cloud security [13]. Virtual machine can be created using own VM image or public VM image stored in the providers repository. A malicious user can store image with some malicious code into the repository. When any user uses this image his created virtual machine can be infected by hidden malware [11]. There can be chance of data leakage by VM replication. Password, cryptographic keys which are very confidential will be copied.

3.4 VM Escape

If any program can get access to the host machine bypassing virtual layer of virtual machine there can be a security threat. By getting root privileges of host machine a malicious program can manipulate different virtual machines. Since host machine has the control over the entire guest VMs. By exploiting bugs to the VMM along with improper configuration of the host this kind of attacks takes place. Privilege escalation attack from guest to host is one of the ways to VM Escape [4].

3.5 Software lifecycle

VMs are useful for their ability to restore to a previous state. It may raise some security issues. Virtual machine which is returning to an unpatched or compromised state due to some condition may be in a great danger. One scenario is shown in Fig. 3.

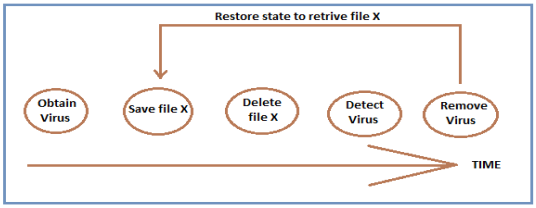

Fig. 3. Possible security concern during software lifecycle

3.6 Data Remanence issue

Data remanence simply indicates to the file system that the file is deleted, but the data in the file remain on the hard drive until the file system eventually overwrites the file. After storage media deletes the file there may be some physical characteristics that allow data to be rebuild [5]. Generally IT organizations have their own servers and they have full control on their servers. To destroy unwanted and important data safety they use different tools. But when they join to the cloud environment they have virtual servers which are controlled by third party there may be a security problem. If any data or properties of any data are not erased securely after the data life cycle, intruder can rebuild the data with the remained data properties and can have access of some sensitive data that is stored in the disk storage.

3.7 Denial of Service

Denial of service attack in virtual machine consumes all the possible resources of the system which are making request for resources [10].

Properly configuring the hypervisor can be the solution for this type of attack[12] .Truly configured hypervisor prevents any VM from gaining 100% access of any resources, including CPU, RAM, graphics memory , Network bandwidth etc.

3.8 Mobility

Hypervisors stores the contents of the virtual disk of as a file. Each VM are stored as a file. This allows VMs to be copied and moved to another disk or another host. Attackers can copy the physical data of any VM and can store it in his own machine. After getting the access of virtual disk the attacker have plenty of time to break all the security measures of the data in the disk [14]. Virtual machine will not show any intrusion report because it is a duplicate copy.

3.9 VM sprawl

In a virtual environment users can create many virtual machines.VM sprawl is the incident when number of virtual machine crosses a threshold value, so the administrator cannot manage them effectively [15]. To prevent VM sprawl, one should carefully analyze the need for all new VMs and enforce a process for the deployment of VMs.

3.10 Transience

In a virtualized environment machines are often appear or disappear from the network. It is known as transience. Network with traditional machines were much more stable than others because it is easy to

analyze the existing network configuration. But in case of transience, where stabilized environment is not there, security is more challenge [16].

Transience complicates security processes though it is not security vulnerability. If a network gets infected by worm, it will be harder to find the infected machines because of transience. A virtual machine which is infected can go offline before detection again can come online at a later time and re-infect all vulnerable machines.

3.11 Scaling

In case of virtualization we can easily create a replicate of VM or can create a copy of the VM. A single effected machine (by worm or malicious code) can be replicated to the others VMs which can destroy the whole virtual environment [17].

3.12 Network Security issue

Virtual machine uses the same physical interface which host machine uses due to resource pooling in multitenant environment [18]. Virtual network increase the VMs interconnectivity which is an important security challenge. This virtual link is exploited by an attacker to sniff traffic directed to one VM from another VM deployed on the same physical host. ARP spoofing is one of such kind of attacks.

4 Countermeasures for the threats

4.1 VM Monitoring

The concept of virtualization has been leveraged to increase the security of host. For that reason the host system has been moved into virtual machine and it will be monitored from outside the system[8]. This way the shortcomings of host security can be overcome.

4.2 Virtual Machine Introspection

Virtual machine introspection techniques are based on the concept of ability hypervisor to introspect the resources from outside the system. This is a way of doing passive monitoring. This approach is used to detect any case of intrusion in virtual machine by following hardware state and events & using this data to figure out the host ‘s software state . A more robust view of the system we can get by observing hardware state directly rather than by an HIDS. Since introspection is done from hypervisor layer, the information obtained here is genuine even in case of compromise of guest OS.

4.3 Mirage

This technique is used to check the validity of the VM images that are used to create the virtual machines. Access control framework, image filters, a provenance tracking and repository maintenance services are the different security features which this feature includes. . However filters in this approach cannot scan all the malware or remove all the sensitive data from the images . This is the limitation of this approach is that filter .

4.4 Hypersafe

It is an approach which provides hypervisor control-flow integrity. Non by passable memory lockdown and restricted index pointing [6] are the two techniques which is used by hypervisors. First one relies

on the features of security built into modern processors to lock down the memory which includes the executable code. This helps to protect the code of hypervisor & all the sensitive data from being compromised even if there is presence of exploitable bugs in the memory. Second technique is to create an initial snapshot of hypervisor's normal behavior & then prevents from any deviation than that.

4.5 Semantic Reconstruction

The system view obtain by the reconstruction method is called trusted view & that system view obtain by calling the system function to query resource information is known as non-trusted view. System resources which are in trusted view and not in the non-trusted view are in hidden view. Cross-View detection methods focus on the content between the trusted and non-trusted view & discover hidden behavior within the system [9].

4.6 Encryption

In this environment user's data is stored in a remote machine rather than a local machine. As data is the most sensitive information, host hypervisor provides different encryption techniques like Digital signature, Homomorphic encryption. Digital signature is a encryption technique which uses RSA algorithm to protect the data. In homomorphic encryption technique, the user's data is computed in memory without being decrypted. Because when the user's data is being computed then the cloud providers have to decrypt their data which is being a privacy concern.

4.7 Protecting the VMM

Hypervisor is also available at the boot time of machine . It controls the resource sharing and monitoring the virtual systems. This approach establishes a more controllable environment. However hypervisor is a single point of failure which makes the system more vulnerable . If any malicious intruder gets control over hypervisor , then all the VMs will be under the control of attacker's . So it is very much crucial to preserve the integrity of VMs. Though it is possible to ensure the integrity of the VMs during boot time , but it is difficult to maintain the runtime integrity. So installing another layer of hypervisor is possible & this can guarantee that hypervisor installed for monitoring it cannot be turned corrupted.

4.8 Protecting the VMs against their VMM

When a data of an organization moved from a single tenant to a multi tenant environment data confidentiality and integrity becomes a security issue. To maintain this CloudVisoris used [7]. The primary idea behind this is to encrypt the data so that data belonging one VM could not decoded by another VM. CloudVisor virtualizes the monitored hypervisor to reach its goal. This removes the second hypervisor which is installed to monitor the other hypervisor from the most privileged zone. Here the monitored hypervisor is running in guest mode while the CloudVisor is running in root mode. CloudVisor traps all the access request generated by VMM. If the request is not valid then the CloudVisor encrypt the content.

4.9 Active Monitoring

Here security tool places a hook inside the system being monitored to do active monitoring[3]. Whenever execution reaches the hook, it will interrupt execution and then control will be passed to the security tool. Active monitoring can be done from outside of the system though these monitors

are restricted to some level. Monitoring is restricted upto the the semantic level provided by the disk and network device abstractions. Security critical code is placed in un trusted domain in case of active monitoring . By write protecting the memory part where the code is kept security of this code can be achieved.

Table 1. Security issues and probable solution

Security Issues	**Definition**	**Probable Solution**
Shared Resources	VMs located on the same environment share the resources so a malicious VM can affect other VMs	Active monitoring can be used by adding hook to the each VM for detecting the malicious VM.
VM Escape	A program bypassing the virtual layer ,getting root privileges of host machine can manipulate other VMs	A tool called hypersafe provides hypervisor control flow integrity. It uses two techniques i.e. non by passable memory lock down and restricted point indexing.
Software Lifecycle	In lifecycle of a virtual machine it can restore to its previous unpatched or compromised state	Semantic reconstruction methods can be used by reconstructing the trusted view and then apply Cross-view detection methods.
Malicious VMM	As the guest VMs interact with the hypervisor through VM exit ,a malicious VM could inject malicious code through VM exit.	Nested Virtualization where a second hypervisor will be installed to monitor the initial hypervisor.
Denial of Service	A guest machine consumes all the possible resources of the system .	Properly configuring the hypervisor such that it prevents any VM from gaining any resource's cent percent usage
Transience	If a network gets infected by a worm, it will be harder to find infected machines because of transience.	Introducing a cloud deployment mechanism that fixes transient errors through re-executing that failed part of deployment.
Public VM image Repository	VM image containing the bogus code stored in the repository affecting the legitimate VM images.	Mirage technique is used to validity of the VM images which includes the security features such as image filters, provenance tracking, and repository maintenance service.
Data remanence	Reconstructing the data from the physical residual of it.	First, to securely erase the data user has to overwrite the data after erasing it. Second, user has to encrypt the data with their confidential key to prevent reconstructing.
Mobility	As the data is present in a mobile server it raises a important security issue called data leakage	Modern encryption techniques like Digital signatures &Homomorphic encryption, integrity algorithms can be applied by the host hypervisor
Scaling	A single affected machine can replicate to the other VMs .	Virtual machine introspection can be used for analyze the content of the VM-allocated memory space by hypervisor

		from outside.
VM Sprawl	The number of virtual machines outflows from the administrator threshold	Need for new VMs should be analyzed and under-utilized VMs should be archived.

5 Conclusion and Future Work

Cloud Computing is a new concept and users get a lot of benefits from it. And it is mainly based on Virtualization technology. But there are several challenges and related security issues. Most of the security solutions are focused on hypervisor which is also known as Virtual Machine Monitor (VMM). VMM is the component that drives virtualization. Virtualization adds an extra layer which makes opportunities for attackers. This paper studies different issues of virtualization. It's a security risk and different mechanisms to overcome them and make the environment less vulnerable to risk.

Cloud computing cannot completely replace traditional computing. There are many security issues that are still to discover. And the solutions need to be more secure. The existing security solution should be periodically reviewed.

References

[1] Scarfone, K., Souppaya, M. and Hoffman, P. (2010). Guide to Security for Full virtualization Technologies. *National Institute of Standards and Technology*, USA.

[2] Szefer, J. et al. (2011). Eliminating the Hypervisor Attack Surface for a more Secure Cloud. *Proceedings of the 18th ACM conference on Computer and communications security*, 401-412.

[3] Ranjith, P., Chandran. P. and Kaleeswaran, S. (2012). On Covert channels between Virtual Machines. *Journal in Computer Virology*, 8: 85-97.

[4] Joshi, N. and Vashapriya, J. N. (2013). Analytical Survey of Security in Virtualized Enviornment. 66-71.

[5] Gallagher, P. R. (1991). A Guide to Understanding Data Remanence in Automated Information Systems. *https://irp.fas.org/nsa/rainbow/tg025-2.htm*.

[6] Wang, Z. and Jiang, X. (2010). HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity. In *IEEE Symposium on Security and Privacy,* 380-395.

[7] Sunitha, K. (2014). A Survey on Securing the Virtual Machines in cloud Computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 2: 17.

[8] Studnia, I. et al. (2012). Survey of Security Problems in Cloud Computing Virtual Machines. Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012). Cloud and security:threat or opportunity, Rennes, France. 61-74.

[9] Chen, L. et al. (2011). Researches on detecting malware based on virtual machine. İn *6th International Conference on Computer Sciences and Convergence Information Technology*, 659-665

[10] Reuben, J. S. (2007). A Survey on Virtual Machine Security. *http://www.cs.umd.edu/class/fall2017/cmsc414/readings/vm-security.pdf*

[11] Hashizume, K. et al. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4:5.

[12] Kirch, J. (2007). Virtual machine security guidelines. *The center for Internet Security*.

[13] Almutairy, et al. (2019). A Survey on Security Challenges of Virtualization Technology in Cloud Computing. *International Journal of Computer Science & Information Technology*, 11(3).

[14] Jyothi, A. and Indira, B. (2019). An Automated VM Security Framework for Live Migration. *https://1library.net/title/an-automated-vm-security-framework-for-live-migration*, 8:2029-2037.

[15] Joseph, L. and Mukesh, R. (2018). Effects of Malware Attacks on Virtual Machine Snapshots in a Private Cloud Setup a Survey. *Journal of Advanced Research in Dynamical and Control System,* 5: 332-340.

[16] Nadiah, M. et al. (2019). A Taxonomy of Virtualization Security Issues in Cloud Computing Environments. *Indian Journal of Science and Technology,* 12(3): 1-19.
[17] Kazemi, U. and Boostani, R. (2018). Analysis of Scalability and Risks in Cloud Computing. *İnternational Journal of Academic Research in Computer Engineering,* 2(1): 24-33.
[18] Qaisar, S. and Khawaja, K. F. (2012). Cloud computıng: network/securıty threats and countermeasures. *İnternational Journal of Contemporary Research in Business,* 3(9): 1323-1329.