Hypervisor Vulnerabilities and Some Defense Mechanisms, in Cloud Computing Environment

Dina Mohsen Zoughbi, Nitul Dutta

Abstract: Cloud computing is the most important technology at the present time, in terms of reducing applications costs and makes them more scalable and flexible. As the cloud currency is based on building virtualization technology, so it can secure a large-scale environment with limited security capacity such as the cloud. Where, Malicious activities lead the attackers to penetrate virtualization technologies that endanger the infrastructure, and then enabling attacker access to other virtual machines which running on the same vulnerable device. The proposed work in this paper is to review and discuss the attacks and intrusions that allow a malicious virtual machine (VM) to penetrate hypervisor, especially the technologies that malicious virtual machines work on, to steal more than their allocated quota from material resources, and the use of side channels to steal data and Passing buffer barriers between virtual machines. This paper is based on the Security Study of Cloud Hypervisors and classification of vulnerabilities, security issues, and possible solutions that virtual machines are exposed to. Therefore, we aim to provide researchers, academics, and industry with a better understanding of all attacks and defense mechanisms to protect cloud security. and work on building a new security architecture in a virtual technology based on hypervisor to protect and ensure the security of the cloud.

Keywords: Cloud security, Defense mechanism, Hypervisor vulnerabilities, Security issues, Virtualization.

I. INTRODUCTION

Cloud computing is the way for many Internet providers to choose. The ability to run multiple virtual machines (VMs) on a single hardware platform through virtualization is the primary technology that makes the cloud possible.Cloud computing contains many features that provide it with unique value, but these features expose it to security concerns as users of cloud computing must be fully aware of these concerns and work to address them.

Cloud computing uses three different services [1]Models SaaS (Software as a Service), PaaS (Platformas a Service), IaaS (Infrastructure as a Service).

Each of these models has its own security problems.

1- SaaS Software or services in their own cloud environment or a request from a third-party Amazon to host them. Therefore, it is difficult for usersto make sure

that all that is needed are safetymeasures. Customer data is stored on the infrastructure of SaaS providers or it may be stored in a third-party public cloud environment. In this case, the data may be stored with data or other SaaS unrelated to applications related to other customers.

Revised Manuscript Received on November 26, 2020.

* Correspondence Author

Dina Mohsen Zoughbi, Department Computer Engineering, Marwadi Education Foundation's Group of Institutions, Rajkot, India.Email:dina.zoughbi108402@marwadiuniversity.ac.in

Dr. Nitul Dutta, Department Computer Engineering, Marwadi Education Foundation's Group of Institutions, Rajkot, India.

Email: nitul.dutta@marwadieducation.edu.in

In addition, data can be copied to other locations in different cities or even different countries to support the high availability of solutions. Hence, there will be potential vulnerabilities to data and app breaches. In this model, clients do not have enough information to know how their data is stored and also lack the ability to control it.

2- PaaS Security Issues: In PaaS (most of them are developers in this case) they have some of the app building controls are at the top of the platform. Therefore, PaaS is more flexible SaaS and brings more security concerns. Security vulnerabilities in application code can be exploited and put the application at risk safety.

3- IaaS Security Issues: IaaS has several security issues based on the cloud model and location (public, private, hybrid, community). Public cloud has a high risk while private cloud appears to have less security issues. When the cloud data environment is passed through a number of third-party infrastructure devices, there is a possibility that the data is being routed by the hacker's infrastructure. In addition, the physical security of cloud infrastructure is very important and any harm can affect the entire virtual machine environment. [2]

Virtualization is one of the major components of cloud computing technology. However, this leads to major security problems. one of the major security issues is that the host machine itself is completely isolated this has not been fully achieved in the current security plans. Virtualization modifies devices by applying a physical device underneath or placing a single mobile virtual machine between two different hosts [3]. Virtual Machine Monitor (VMM) technology or what is known as hypervisor provides many characteristics, the most important of which are functional isolation, ability to transfer and migrate data, [4] workload balance and avoidance of errors. However, this leads to increasing security concerns and problems resulting from this development. The infrastructure exists to work as a provider to access hardware and enable operating systems, but this does not provide security. Hence, security problems must be studied and solutions sought on a large scale many security vulnerabilities have been exposed in virtual environments that contain vulnerabilities in isolation. There are also vulnerabilities in virtualization software that are being compromised by a malicious user. For example, a hacker exploited a computer vulnerability to run malicious code. The importance of virtualization in addressing security problems or issues that the virtual environment is exposed to. [4] Where detection of vulnerabilities and protection from attacks are among the necessary tasks to accomplish virtual simulations as these attacks may cause information leakage.

The difficulty lies in protecting virtual devices, where Hacking a single physical host may give the hacker access to data that is stored in virtual servers. [5] therefore Virtualization technology has caused new security concerns. About 70% of cloud consumers believe that security issues are one of their problems. The main challenges in IaaS 'main open source cloud management platforms are Eucalyptus, OpenNebula, Nimbus, CloudStack and OpenStack. For those who do not want to use commercial cloud, these projects offer an important alternative.

Open source solutions are weak in terms of documentation and verification. Hypervisors are used as Hypervisors use different architectures, although only hardware-based virtualization is used. Linux-Based Hypervisors Software. XEN and KVM(Kernel Virtual Machine) are based on an open source mod for the Linux kernel, while [6] XEN hypervisor PV is used in fields based on discrete management; To manage and control virtual machines, and through a user, they can access a group of virtual machines.

KVM is the basic open source module capable of using most of Linux's features. It is able to provide a more robust ecosystem for virtual machines and cloud services. The cloud service provider is running user-supplied VMs without the knowledge of the guest OS. In addition to the fact that cloud computing provides convenience and many benefits, it also causes many weaknesses and threats to the computing system [7]. Where to ensure cloud security, a virtual environment must be secured. This comprehensive study evaluates all aspects that may affect the security of a cloud computing environment in order to protect the data stored by cloud infrastructures.

Our contribution to this paper is: (1) Classification of attacks in the cloud; (2) View security issues and find solutions to solve vulnerabilities in cloud computing virtual machines; (3) Take security measures to protect the cloud environment.

II. VIRTUALIZATION COMPONENTS

Virtualization is the basis of the manufacturing of cloud computing. In terms of cost, virtualization technology is a tool for effectively improving and developing the performance of IT enterprise applications, but it causes some security risks through application delivery challenges. [8] Thus, virtual servers are able to play an important role in virtual technology in terms of significant cost savings. Whereas, the guest OS is an operating system that resides on a virtual machine. In addition, there is an administration layer called a controller or virtual machine manager (VMM) or hypervisor that controls all the virtual machines present in the virtual environment. Hypervisor is one of the most important virtualization technologies, [9] as multiple operating systems are called guests, virtual machines have the advantage of working simultaneously on the host "my computer". The hypervisor is preparing a platform for guest operating systems that runs by default and also "monitors the implementation of the guest operating system.

Servers only function is to run guest operating systems, so the hypervisor is installed.

III. VIRTUALIZATION VULNERABILITIES

Virtualization has the advantage of providing a highly efficient resource management tool because virtual resources are available for both physical and dynamic resources. There are several issues with IaaS, PaaS, and SaaS that have made the cloud environment vulnerable. However, it is not considered a modern security issue.

Virtualization technology has caused complex security issues in the cloud and led to many new vulnerabilities, threats, and breaches. Where the importance of multiple virtualization is in running multiple operating systems on one physical device without interfering with each other. It plays a "significant" role in operating systems, even though they are running on the same server. Therefore, the malicious party might have a chance to exploit the vulnerabilities and attack the virtualization layer in order to gain access to the virtual networks.

The biggest problem, when one virtual machine is hacked, and this causes a security issue for all the virtual machines on the physical server, causing other virtual machines to be compromised and accessed by the host. [10]

IV. TAXONOMY OF CLOUD-BASED ATTACKS ON THE VIRTUALIZED SYSTEM

In order to protect and secure the cloud environment, security threats must be classified and dealt with, while providing services in the cloud in order to have the highest level of security against attacks. [11] So, so we classified the threats in Hypervisor-based attack, VM-based attack, and VM image attacks. Figure 1 illustrates the categories of attacks on the basis of various types of virtualization in cloud computing. Our classification covers cloud-based attacks on virtual systems in the infrastructure as a service layer.

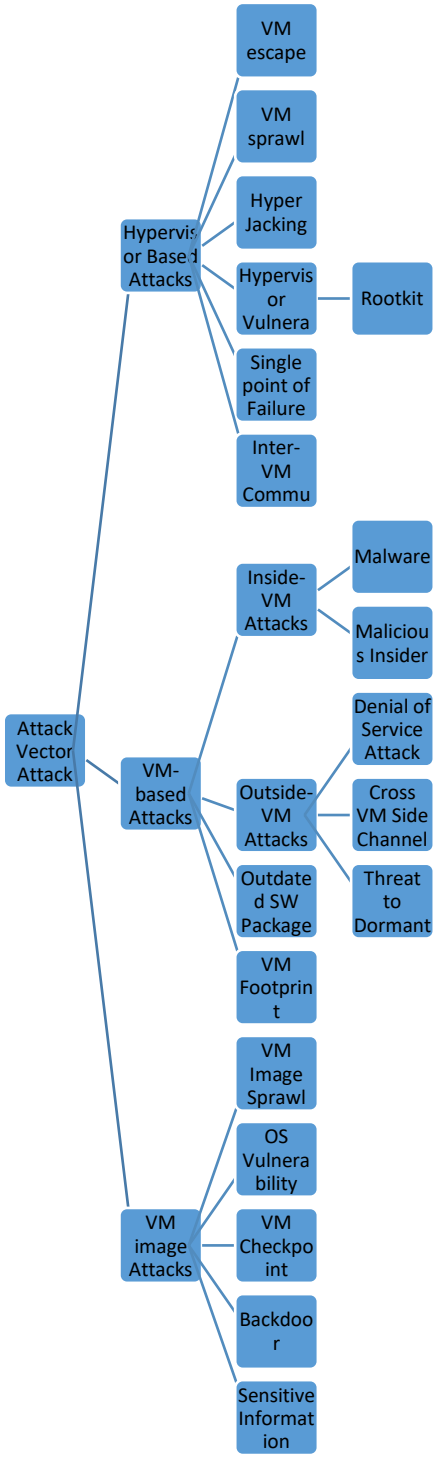

Fig. 1Taxonomy of cloud-based attacks on the virtualized systems.

V. VIRTUALIZATION SECURITY ISSUES

A hypervisor-based attack is an attack that exploits vulnerabilities in the program by a hacker that works to share multiple operating systems with a single processor of devices. Hacked hypervisor allows a hacker to attack every virtual machine on a virtual host. [12] More programs and larger numbers of APIs, but the security guarantee in the code is less, and this leads to increase in risks and damages [13]. We highlight the following attacks in hypervisor-based virtual environments.

A. VM escape

Virtual machines are designed to allow the host and VMs to be strongly isolated [14]. But the operating system vulnerabilities that run within the VM will help attackers to inject a malicious program into it. When this software is running, the VM violates the isolated limits and Contact begins with the operating system bypassing the VMM layer directly. Such an exploit opens the door for attackers to gain access to and conduct more attacks on the host computer.

B. Hyper jacking

Hyper jackingIt is an attack in which a hacker takes malicious control of the hypervisor that creates the virtual environment within a virtual machine (VM) host. Where the purpose of the attack is to target the operating system below that of the virtual machines so that the software of the attacker may runs and its existence will be completely obvious to the applications on the VMs above it. [15]
Hypervisor Hyper jacking is categorized into 3 types:
1. Injecting under the original Hypervisor a rogue Hypervisor.
2. Obtaining full control of the initial Hypervisor.
3. On top of the Hypervisor, running a rogue Hypervisor.

C. VM sprawl

When a large number of virtual machines reside in the system without proper monitoring or control, VM sprawl occurs. Because during this (retrieved from http:/cloudschool.com) they retain the device resources (i.e. memory, disks, network channels, etc.)
Such resources can't be distributed to other VMs over time, and they are essentially lost.

VI. BACKGROUND ON HYPERVISORS

The market for virtualization consists of mature (e.g. VMware and XEN) and rising (e.g. KVM and Hyper-V) members. Of the four main offerings of Hypervisor, which make up 93% of the overall market share [16].
Two are closed sources (VMware and Hyper-V) and two (XEN and KVM) are open sources. Recent surveys [16, 17] show that there is a large and rising number of different hypervisor brands deployed in data centers, with multiple hypervisor strategies becoming the norm. Vulnerabilities and VMware Generic Code exposures (CVEs) are often from an external viewpoint. It does not constitute a sample collection that is representative. We agreed, therefore, to concentrate on XEN and KVM.
With 81 % and 51 % of data centers respectively, knowing their vulnerabilities could help millions of users around the world, considering the effect of XEN and KVM on the virtualization sector. Below, we summarize XEN, KVM, and the different hypervisor designs' architectural features.

A. XEN:

XEN,which has been in use since 2003, is well known open source hypervisor. Whereas, XEN is a Model 1 hypervisor (exposed metal), running directly on top of devices and controlling all host resources, as shown in Figure 1.

It also contains a different virtual machine called Dom0, which performs everything (such as startup and shutdown) Guest Relay (VMs) behavior of the Virtual Machine Manager. Domo VM is a completely custom and familiar Linux kernel for XEN deployment. Dom0 displays devices that have been simulated by connecting a copy of the system emulator.

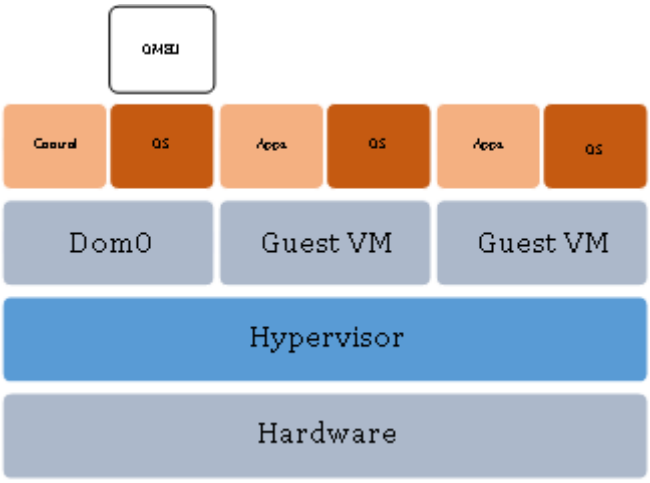

Fig. 2XEN Architecture

B. KVM:

KVM is a fairly recent open-source project, dating back to the 2008 acquisition of Qumranet by Red Hat. Many inequalities with XEN can be described from Figure 2. As a separate user process, each guest VM runs and has a corresponding process.

An instance of QEMU interface emulation running with it. The Hypervisor itself resides inside a host operating system as a module, making KVM a Type-II (hosted) Hypervisor.

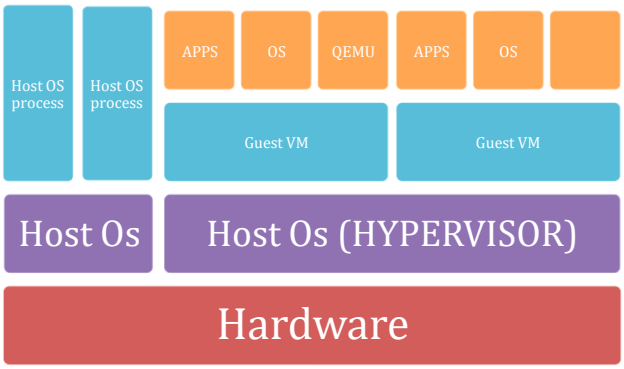

Fig. 3KVM Architecture

VII. HYPERVISOR VULNEABILITIES:

To run multiple guest VMs and applications simultaneously on a single host machine and to provide separation between guest VMs, a hypervisor or VMM is created [18]. They are open to attacks, despite the fact that hypervisors are supposed to be vigorous and stable. When attackers take control of the hypervisor, [19] all the VMs and data accessed by them will be completely controlled for their use. The greater control offered by the bottom layers in the virtualized framework is another reason that hackers considered the VMM a potential target. To compromise a VMM also allows the underlying physical structure and the hosted applications to gain power. some of the well-known attacks (e.g., Bluepill, Hyperjacking, etc.) inject rootkits based on VMs that can mount or change the current rogue hypervisor to take full control of the environment. Since the hypervisor runs under the host OS, it is difficult to detect these types of attacks using periodic security measurements. [19]We conducted a search of a host of vulnerability databases for KVM and XEN-related publications. As of 15 July 2012, 59 vulnerabilities have been identified in XEN and 38 in the KVM, according to the CVE reports. Effective exploitation of the vulnerability leads to an attack that could harm the security, reliability, or availability of a hypervisor or a guest VM device.

deeper understanding and identification of various vulnerabilities

Symmetric Multiprocessing (SMP):Hypervisors can host SMP capable guest VMs, leading to the possibility of parallel scheduling of two or more vCPUs belonging to a single VM to the physical CPU cores. This operation mode adds complexity to the guest VM state management and requires additional precautions when determining the Current Privilege Level (CPL) of a vCPU (e.g., Ring 0 or Ring 3).

SMP vulnerabilities arise from assumptions made by Hypervisor code that only apply to single-threaded processes.

a. Soft MMU (memory management unit):It is not possible to grant direct access to the MMU to guest VMs, as this would enable them to access Hypervisor memory and other co-hosted VMs. The soft MMU is managed by a hypervisor to maintain a table of shadow pages for each guest VM in the absence of a VRAP MMU, such as Extended Page Tables (EPT). The soft MMU intercepts any page mapping change that is invoked by a virtual machine to adjust shadow page tables accordingly. Soft MMU implementation vulnerabilities are dangerous because they can lead to data disclosure in random address spaces, such as the memory segment of a shared hosted VM guest or the memory portion of a hypervisorIn the special case of CVE-2010-0298, when a guest VM memory is accessed on behalf of the guest VM code, the KVM memory is accessed by the KVM. emulator often uses the Ring 0 privilege level. One disenfranchised, provided that the MMIO instruction is emulated, (Episode 3) an application running inside the VM Access to the MMIO region(such as frame-up et secure) can be utilized to trick the KVM into executing a malicious instruction that Modi-Fi outperforms that kernel of the VM's own space.

(Episode 3) A program running inside a virtual machine can use MMIO zone access (for example, Frame Clipboard) to trick a KVM into executing a malicious command that modifies the kernel space memory of the same virtual machine

b. Hyper calls: in the OS universe, hyper calls are similar to machine calls. Although VM Exits are architecture-wide (e.g. AMD64, x86), hyper calls are wide to Hypervisor (e.g. XEN, KVM) and provide a procedural interface from which guest VMs can request Hypervisor privileged behavior. It is possible to use Hyper calls to query CPU operation, control Hard Disk partitions, and generate virtual interrupts. An attacker who controls a guest VM may present Hyper call vulnerabilities, with a way to attain expanded privileges over the properties of the host system. Case in point, CVE-20093290 mentions the reality that KVM used to allow MMU hyper calls to be given by unprivileged (Ring 3) guest callers. Since the MMU command structures must be passed by their physical address as an argument to those hyper calls, they only make sense when issued by a mechanism called Ring 0. The Ring 3 callers could also transfer random addresses as arguments to the MMU hyper calls without access to the physical address space, which would either crash the guest VM or, read or write on kernel-space memory segments in the worst case scenario.

c. VM Management: The collection of basic administrative operations that a Hypervisor must support is made up of VM Management features. Guest VM configuration is expressed in terms of their allocated virtual machines, dedicated PCI machines, big memory quotas, topologies and goals for virtual CPUs, etc. The Hypervisor must then be able to start, pause and stop VMs that are true to the cloud provider's configuration declarations. These tasks are initiated by XEN's Dom0 and KVM's libvirt toolkit [12]. when booting up a VM, kernel images need to be decompressed into memory and interpreted by the management domain.
CVE-2007-4993 indicates that XEN's Para virtualized image bootloader used exec) (statements from Python to process the user-defined configuration file of the custom kernel, leading to the ability to execute arbitrary python code within Dom0. A malicious user might trick Dom0 into issuing a command that would cause the destruction of another co-hosted domain by modifying the configuration file to include the line shown in Listing (substituting I'd with the ID of the victim domain).

d. Remote Management Software: Typically, these pieces of software are web applications that run as a background process and are not required for the proper execution of the World Virtualized. Generally, their objective is to facilitate the administration of the Hypervisor through user-friendly web interfaces and network-facing virtual consoles. Vulnerabilities can be exploited from anywhere in these bundled applications and can lead to complete control of the virtualized world.CVE-2008-3253, for example, describes a Cross-Site Scripting attack on a remote administration console that, after stealing authentication cookies from a victim, exposed all of XEN's VM management behavior to a remote attacker.

VIII. HYPERVISOR SECURITY:

There is information theft through side channels, or performance-based attacks to slow down targeted VMs, in addition to the functions of HYPERVISOR as attack vectors, which we have previously learned about, and a malicious VM may try to compromise a hypervisor. This is known as Escape from the VM.

1) Hyper Safe [20], Hypervisor Control Flow Integrity, is designed to offer Hypervisor control flow integrity. The Trusted Platform Module (TPM) offers safe storage, safe validation, as well as cryptographic hashes and signatures [21] on a hardware-based module. TPM will incorporate the hypervisor load time, but the challenge is to incorporate the runtime. in Hyper Safe, two strategies have been suggested to address the problem of runtime verification.

a) In Hyper Safe, the first approach is to enforce a memory lock that is non-bypass able. Memory file locking prohibits any unauthorized file writing from happening. The method of unlocking is structured to avoid any alteration of the code and data of the hypervisor. This approach prevents malicious code from being inserted into the control flow of the hypervisor and is implemented as a complement to the XEN Hypervisor [20].

b) In Hyper Safe, the second approach is called restricted cursor indexing, in order to apply a switching layer to all indicators. Use the method of shutting down memory previously discussed, pre-calculate control flow objectives and then store them in a table. Ensures that the control flow diagram is accompanied by calls and return goals. it is implemented as a compiler extension, so no modifications to the hypervisor code are necessary. [20]

2) Hypervisor Integrity ***Checking Another approach:***is called Hyper Sentry [1] to protect the hypervisor. To provide stealth and in-context integrity testing of the hypervisor, Hyper Sentry uses a software component that is separated from the hypervisor. This approach does not add a higher and more privileged layer, but instead uses the software integrity portion with existing hardware and firmware and isolates it from the hypervisor by using TP [22]

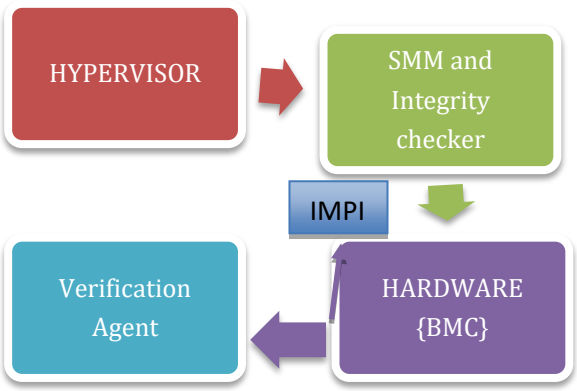

Fig. 4Hyper Sentry architecture

3) Return-Oriented Hypervisor Programming Attack an attack using return-oriented programming (ROP) can be used to launch a successful XEN hypervisor attack [23].

The purpose of the ROP attack is to change the data that governs the level of VM privilege in the hypervisor. An attacker can escalate their VMs to a privileged state in this way.

IX. RELATED WORK:

Recently, cloud computing security concerns have attracted broad attention, and several researchers have researched security problems in the virtualization layer. In a virtualized world, the hypervisor or Virtual Machine Monitor (VMM) detaches each of the VMs from the rest of the device. Many of the flaws in virtualization are special to the cloud platform and current approaches can hardly fix them. year by year, the number of reported virtualization security vulnerabilities is growing and more researchers are concentrating on this area. A main concern in virtualization protection is the VMM. The VMM is a software module which controls all virtual machines and their hardware connections. The VMM is primarily responsible for managing and isolating each running VM and is also responsible for developing and managing each virtual resource. A large number of attack vectors can encourage interconnection complexities and more entry points in the VMM [6]. Zhang et al. Zhang et al. [7] suggested a KVM-based Rootkit identification approach using virtualization technology. Wojtkowiak [10] explains 259 new virtualization vulnerabilities and new forms of attacks (e.g. hyperjacking, hypervisor escape, VM attacks) during the last 5 years. Pearce et al. [4] demonstrated the hypervisor vulnerability in their work, along with breaking the XEN and KVM (Kernel-based Virtual Machine) protections.

Perez-Botero et al. [24] provided an in-depth codebase study of two common open-source hypervisors (XEN and KVM) and related vulnerability reports. A classification of hypervisor vulnerabilities comprised of three dimensions was proposed by Perez-Botero et al. [24]: the trigger source, the attack vector, and the attack target. Moyo and Bhopal [25] discussed cloud computing security concerns and claimed that virtual machines could be used Side channeling to extract cryptographic private keys that are used on the same list by other VMs. Security problems in cloud virtualization components such as hypervisors, virtual machines and guest disk images were identified by Kazim and Zhu [4] Security problems have been identified in components of cloud virtualization such as hypervisor, virtual machines and guest disk images. During the analysis, we found that although some of the vulnerabilities occur in traditional computing environments and can be discovered through existing techniques, many others have unique virtualized system-related properties, such as hardware logic emulated through software and the ability of an adversary to monitor the implementation flow of a few virtual hardware that can't simply be addressed. Of the four major hypervisor products that account for 93% of the overall market share, two are closed-source (VMWare and Hyper-V) and two are open-source (XEN and KVM) [26]. Our analysis focused primarily on XEN and KVM (Kernel-based Virtual Machine) since Microsoft Hyper-V and VMW are commercial closed-source applications, which makes it difficult to understand and evaluate the internal logic of the VMMs [3]. Other works have provided classifications at various levels of security concerns, such as network, host or application [23]. Our job, as one of its contributions, aims to categorize various attack vectors. In addition to cloud computing, researchers have researched the categorization of kernel-level rootkits to enable potential detection. [20]

X. CONCLUSION:

Virtualization is an important technology in the cloud that enables the sharing of the same physical devices by multiple guest devices. The default visualization, however, requires the use of an encapsulated software layer (Hypervisor or Virtual Machine Monitor) covering the operating system or centered on it and providing the same input, output and actions anticipated from an actual physical computer. Various attacks against hypervisors, virtual machines, and VM images can compromise the cloud simulator environment. We defined attack scenarios on these components and different existing security systems that provide virtualization security.

We conducted a detailed code base analysis of two common hypervisors, XEN and KVM, in this report. Our work will help to better identify the security needs of a particular user based on our observations and identify the range of solutions that can be introduced to resolve them.

Lastly, Hypervisor should be safe from attacks and separate virtual machines effectively, but possible security vulnerabilities are obvious. The addition of noise to the side channel may mitigate other attacks based on data theft through side channels. A significant move in providing a safe cloud environment for businesses and consumers to benefit from the solution to the hypervisor security problems.

REFERENCES:

1. Alameri I, Radchenko G (2017) Development of student information management system based on cloud computing platform. Journal of Applied Computer Science & Mathematics 11:9–14. https://doi.org/10.4316/JACSM.201702001
2. Sosinsky B (2011) Cloud computing bible. https://doi.org/10.1145/358438.349303
3. Zhu G, Yin Y, Cai R, Li K (2017) Detecting virtualization specific vulnerabilities in cloud computing environment. In: IEEE international conference on cloud computing, CLOUD 2017-June, pp 743–48
4. Pearce M, Zeadally S, Hunt R (2013) Virtualization: issues, security threats, and solutions. ACM Comput Surv 45(2):17:1–17:39https://doi.org/10.1145/2431211.2431216
5. Sempolinski P, Thain D (2010) A comparison and critique of Eucalyptus, OpenNebula and Nimbus. https://doi.org/10.1109/CloudCom.2010.42
6. Wu J, Lei Z, Chen S, Shen W (2017) An access control model for preventing virtual machine escape attack. Future Int 9:2. https://doi.org/10.3390/fi9020020
7. Zhang Y, Juels A, Oprea A, Reiter M (2011) Homealone: Coresidency detection in the cloud via side-channel analysis. In: IEEE symposium on security and privacy (Oakland), Oakland, CA, pp 313–328. https://doi.org/10.1109/SP.2011.31
8. G. Rowel, "Virtualization: The next generation of application delivery challenges," 2009.
9. G. Texiwill, Is Network Security the Major Component of Virtualizat
10. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2010), doi:10.1016/j.jnca.2010.07.006

11. Gupta S, Kumar P (2013) Taxonomy of cloud security. Int J Comput Sci Eng Appl 3(5):47–67. https://doi.org/10.5121/ijcsea. 2013.3505
12. Kazim M, Zhu SY (2015) Virtualization security in cloud computing. In: Zhu S, Hill R, Trovati M (eds) Guide to security assurance for cloud computing. Computer communications and networks. Springer, Cham. https://doi.org/10.1007/978-3-31925988-8
13. Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Virtualization security for cloud computing service, Cloud and Service Computing (CSC), 2011 International Conference on, p. 174 – 179, Publisher:IEEE
14. Rouse (2015) What is hypervisor attack? Definition from WhatIs.com. https://whatis.techtarget.com/definition/hypervisorattack. Accessed 10 Mar 2018
15. . Adla, Vishrutha (2013) Comparing performance of Hyper-V and VMware considering network isolation in virtual machines. Masters thesis, Dublin, National College of Ireland. http://trap. ncirl.ie/id/eprint/907. Accessed 25 Mar 2018
16. From Wikipedia, the free encyclopedia (2017) Hyperjacking—wikipedia. https://en.wikipedia.org/wiki?curid=45523767. Accessed 17 May 2018
17. Nexenta Hypervisor Survey. http://www.nexenta.com/corp/nexentahypervisor-survey.
18. M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing," IEEE Transactions on Consumer Electronics, 56(1), 2010, pp. 134–140.
19. Is the Hypervisor Market Expanding or Contracting? http://www.aberdeen.com/Aberdeen-Library/8157/ AI-hypervisor-server-virtualization.aspx.
20. M. Kim, H. Ju, Y. Kim, J. Park, and Y. Park, "Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing," IEEE Transactions on Consumer Electronics, 56(1), 2010, pp. 134–140
21. Jansen WA (2011) Cloud hooks: security and privacy issues in cloud computing. In: 2011 44th Hawaii international conference on system sciences, Kauai, HI, 2011, pp 1–10. https://doi.org/10.1109/hicss.2011.103
22. X. Jia, R. Wang, J. Jiang, S. Zhang, and P. Liu, "Defending Return-oriented Programming Based on Virtualization Techniques," Security and Communication Networks, 6(10), 2013, pp. 1236–1249.
23. R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal. A survey on security issues in cloud computing. arXiv, http://arxiv.org/abs/1109.5388, September 2011.
24. Perez-Botero D, Szefer J, Lee RB (2013) Characterizing hypervisor vulnerabilities in cloud computing servers. Published in SCC@ASIACCS, 3-10. https://doi.org/10.1145/2484402. 2484406
25. Moyo T, Bhogal J (2014) Investigating security issues in cloud computing. In: Eighth International Conference on Complex, Intelligent and Software Intensive Systems, Birmingham, pp. 141–146. https://doi.org/10.1109/CISIS.2014.21
26. Patil S (2017) Digital forensics technique for detection of attack and previous data restoration in cloud environment. 6:427–433. https://doi.org/10.23956/ijarcsse/V7I6/0125

AUTHORS PROFILE

Dina Mohsen Zoughbi, Received her bachelor degree in Information and Communication Technology Engineering from Tartous University, Syria in 2018, Her research interest includes Hypervisor vulnerabilities and mitigation techniques in cloud computing environment, she is perusing Master of Cyber Security in Computer Engineering Department from Marwadi Education Foundation's Group of Institutions, Rajkot, India

Dr. Nitul Dutta, Received his bachelor degree in Computer Engineering from Dibrugarh University, India in 1996, M. Tech in computer engineering from Tezpur University, India in 2002, PhD degree in Communication from Jadavpur University, India in 2011, then Post Doctoral Fellowship from University Jana Wyżykowskiego, Poland. His main research interest in network field of expertise is Computer Network in general and Mobile IPv6 based Network in particular. also working in Cognitive Radio Networks (CRN) and Delay-Disruption Tolerant Networks (DTN) , Routing and Mobility management in WLN. Currently vice-Chair of Computational Intelligence Society, Gujarat Section (from 2016). • Technical Activity Chair of IEEE Gujarat chapter and coordinator of technical activity for students. • Reviewer of IEEE TMC, IEEE Communications Letters and Springer WPC journal. IEEE Senior Member (ID: 90702992) since 2017. He is currently head of Computer Engineering Department, at Marwadi Education Foundation's Group of Institutions, Rajkot, India.