Computer Systems Science & Engineering
DOI:10.32604/csse.2022.019547
Article

Tech Science Press

Extensive Study of Cloud Computing Technologies, Threats and Solutions Prospective

Mwaffaq Abu-Alhaija[1], Nidal M. Turab[1,*] and AbdelRahman Hamza[2]

[1]Department of Networks and Information Security, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, 19328, Jordan
[2]Department of Computer Science, Information Technology, Al-Ahliyya Amman University, Amman, 19328, Jordan
*Corresponding Author: Nidal M. Turab. Email: N.turab@ammanu.edu.jo

Received: 16 April 2021; Accepted: 23 May 2021

Abstract: Infrastructure as a Service (IaaS) provides logical separation between data, network, applications and machines from the physical constrains of real machines. IaaS is one of the basis of cloud virtualization. Recently, security issues are also gradually emerging with virtualization of cloud computing. Different security aspects of cloud virtualization will be explored in this research paper, security recognizing potential threats or attacks that exploit these vulnerabilities, and what security measures are used to alleviate such threats. In addition, a discussion of general security requirements and the existing security schemes is also provided. As shown in this paper, different components of virtualization environment are targets to various attacks that in turn leads to security issues compromising the whole cloud infrastructure. In this paper an overview of various cloud security aspects is also provided. Different attack scenarios of virtualization environments and security solutions to cater these attacks have been discussed in the paper. We then proceed to discuss API security concerns, data security, hijacking of user account and other security concerns. The aforementioned discussions can be used in the future to propose assessment criteria, which could be useful in analyzing the efficiency of security solutions of virtualization environment in the face of various virtual environment attacks.

Keywords: Cloud computing environment; paravirtualization; full virtualization; cloud virtualization security; hypervisor; virtual machines

1 Introduction

Information Technology (IT) area has faced numerous and newly emerged security issues, especially for organizations relying on virtual environments in their business. Cloud computing is viewed as one of the most promising technologies in IT, fundamentally able to deal with various issues. While the concepts and technology of cloud computing are becoming developed and widespread, more and more service providers are interested in the prospects of cloud computing in using and processing information [1]. Identified with key characteristics as flexibility, infrastructure scalability, support for wide range network access, location independence, reliability, cost effectiveness, and sustainability; cloud computing is projected as an evolutionary step in computing technologies nowadays [2].

With virtualization technology as the key technology of cloud computing, it has been recognized and developed quickly. This innovative technology is transforming abstract infrastructure and resources such that multiple logical resources are available to users on a single server in isolated form through virtual machines (VMs) and Virtual Networks (VNs). Various benefits that can be provided by the 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.

The major conceptualized benefits of virtualization are to make it simpler to control and operate, as well as to reduce the cost of operation and ownership of the equipment, alongside with ease of management, less downtime, quicker disaster recovery, and centralization of control. One distinctive advantage of virtualization is sharing: it allows multiple guest operating systems to co-reside and share the same physical resources without interfering with each other. Another distinctive advantage of virtualization is isolation, where failure in any VM will not affect the performance or efficiency of other VMs running on the same host [3].

Whereas creating significant increase in IT agility, flexibility, and scalability, allowing workload mobility, enhanced performance, hardware resources availability, and automated operations, security issues are also gradually emerging with virtualization of cloud computing. Its threat degree is far higher than the traditional unrelated environments; cloud-computing industry, for it increases the vulnerability of the system to attacks as all cloud users, and possibly attackers, who share with each other its resources.

Virtualization technology complicates security, as there are many new vulnerabilities, risks and threats appearing. The task of securing virtualization in cloud computing is a crucial portion to elevate the safety of the widely deployed traditional cloud computing [4].

Security in cloud computing has always been a great concern for IT sector, that is why most researches are in cloud computing security. Due to the sharing of physical resources like processor caches, or by the mechanism implemented in the virtualization layer itself, cloud virtualization is at risk of various security threats [2]. The efficiency and effectiveness of old protection mechanisms are being reconsidered, as the characteristics of this innovative deployment model entirely are different from those of old cloud architectures. Security means and approaches in traditional IT are still useful. However, cloud computing presents different security threats to organizations than traditional infrastructure due to service deployment method, operations and enabling technologies. Regrettably, security integration into these services often makes it is more and more difficult to provide more considerable solution to the security issues [2]. So in recent years, this problem is attracting increased attention from theorists and equipment developers.

The remainder of this paper is arranged as follows. Section 2 introduces the concept of cloud virtualization. The problem statement and the related research questions are highlighted in Section 3. The various types of cloud virtualizations and their security threats and presented in Section 4. The paper is concluded in Section 5.

2 Virtualization Architecture

The term Virtualization is defined as the use of a software layer that lies beneath the operating systems which will be deployed on the same server (hardware settings) while providing the same resources that would be demanded from physical hardware. The software playing this role is called Hypervisor or Virtual Machine Monitor (VMM), with the purpose of providing an environment to the hosted operating system with the look and feel of the original host system. Moreover, the Hypervisor or Virtual Machine Monitor (VMM) detaches the hardware state; i.e., virtual machines are not bound by the state of the physical hardware; hence, multiple virtual machines can be installed on a single server/computer. A hypervisor is an extremely privileged software that runs either alone or can underlay the operating system; it is implemented to be "an efficient, isolated duplicate of the physical machine", where a single hypervisor can run multiple guest systems [5].

Virtualization architecture is a theoretical model, which determines the interrelationships among particular components involved in delivering virtual machines with the same functionality as the physical ones, such as operating systems, network resources, servers, and storage spaces. The virtual environment enables the virtual machine to isolate data from other virtual machines. In other words, a program running in one virtual machine cannot see programs running on other virtual machines.

In general, the virtualization is based on a hypervisor. The hypervisor isolates operating systems and applications from physical hardware, whereas the host machine runs multiple Virtual Machines (VMs) as guests that are sharing the physical resources of the system, such as processors, memory, network bandwidth, and so forth. Besides coordinating access to the hardware resources, the Virtual Machine Monitor (VMM) also protects access between the various VMs. When the host machine starts the VMM, it loads all the VMs and their associated OSs and allocates memory, CPU, network adapter, and disk storage between them as required.

The virtual machine monitor differs from an emulator. Whereas an emulator intercepts all commands, a virtual machine monitor intercepts sensitive instructions (which interface with the VMM operations). The non-sensitive instructions are executed directly on the hardware setup. A Virtualization architecture can be categorized into two types: Type 1: Native or Bare Metal Architecture and Type 2 is Hosted hypervisor Architecture [6]. Fig. 1 below illustrates both architectures.

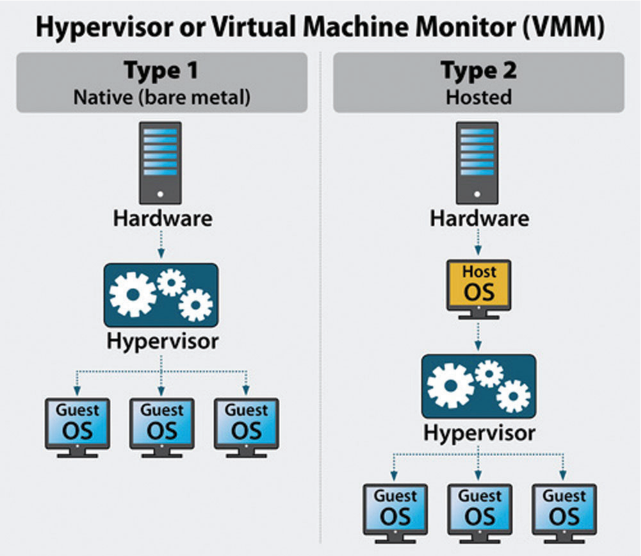

Figure 1: Hypervisor Architectures: Type 1 *vs*. Type 2

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 top of the OS, hence the Hypervisor is hosted as a program on an existing operating system. This OS-based architecture entirely enables the user to control multiple guests OSs, or VMs installed on the hardware. On the other hand, in the Bare Metal architecture, a software is installed directly on the hardware setup of the physical machine, positioned between the hardware and the guest operation system allowing the hypervisor to run directly on the host hardware. Like the hosted architecture, VMs and higher layer applications are installed above the hypervisor.

Hosted virtualization is useful for software developers when creating and testing software on legacy applications, and on different operating systems that developers do not really have physically. Also, it enables laptop or desktop computers, usually considered to have low resources compared with servers, to run two or more VMs, where those VMs represent different operating systems and desktop configurations. For example, one VM might run a Windows 10 desktop, while another VM might run a Linux. However, it has some severe disadvantages due to controlling the virtual machines by operating systems directly. Therefore, it turns out to be more straightforward for an attacker to inject malicious attacks or DoS attacks to 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 [7].

Bare-metal virtualization satisfies the requirements for IT admins looking to maximize the use of physical server resources by running two or more VMs on the same system. Admins who use bare-metal virtualization gain the benefits of VM logical isolation, mobility and performance.

Every layer of cloud computing services can be virtualized in a cloud-computing environment. Such virtualizations include three essential services. The first is Software as a Service (SaaS) in which the users run applications on the virtual environment, the application can be accessed through different hardware form the side. Another is Platform as a Service (PaaS) where PaaS delivers to users with multiple programming languages, libraries, services, and tools supported by the provider. Lastly, Infrastructure as a Service (IaaS) provides on-demand virtual computing services and provides access to computing resources in a virtualized environment [5].

3 Problem Statement and Research Questions

The rapid expansion of cloud computing and virtualization technology complicates cloud infrastructure and have introduces a new set of security threats. Virtualization technology has made security in cloud environments a complex issue, where lots of new vulnerabilities and threats are constantly appearing.

Being the core of cloud virtualization, many security issues and vulnerabilities in the virtual environment are related to the hypervisor or VMM as the enabler of dynamic allocation and modification of multiple VMs on a single physical host machine. The Hypervisor is attracting the main concerns, because it has the supervisory duties (creation, management, isolation of the VMs). Nonetheless, most virtualization vulnerabilities are distinct and ever-increasing in the virtual environment. The volume of the virtualization research studies is increasing due to the expansion of the market demand. Accordingly, the vulnerabilities revealed by security analysts and hackers are tremendously mounting [8].

Vulnerabilities in the virtualization layer frequently affects performance causing degradation and interruption of service, data leakage, and even hijacking of control flow at the VMM level. Many of these vulnerabilities can be detected by existing software analysis techniques, nonetheless, some flaws as and can hardly be mitigated by the existing solution alone [7].

Over the past few years, researchers [8–10] are focusing their attention on some basic research questions; primarily in identifying the vulnerabilities and risks of virtualization in cloud computing environments, recognizing potential threats or attacks that exploit these vulnerabilities, and what security measures are used to alleviate such threats.

A few essential research questions are currently the basis of any research on virtualization in cloud environments, and most research involves Systematic Literature Review in order to fully explore virtualization security issues. The following research questions have been highlighted in most research nowadays:

Q1. What are the main vulnerabilities and risks of virtualization in cloud computing environments?

Q2. What are the potential threats or attacks that exploit virtualization vulnerabilities?

Q3. What are the major security techniques and approaches used to alleviate the security risks?

The following section aims at addressing these research questions, providing elaborative discussions on the various vulnerabilities that face cloud computing environments, the potential threats that exploit these vulnerabilities, and the techniques proposed to mitigate each of these threats.

4 Virtualization Types and Attacks

Virtualization enables researches, and companies to build a complete virtual computer system infrastructure including operating systems, storage devices, and networking components on a single physical server hardware.

Server virtualization is not the only available virualization type there is other virtualiation types such as: application virtualization, storage virtualization, network function virtualization, and desktop virutalization.

4.1 Application Virtualization

Application virtualization is the process of installing an application on a single server in a way that this virtual application can be operated on diverse range on multiple systems. From the end user prospective, this virtualized application works exactly like a native application installed on a real physical machine. Another promising feature is portability, application virtualization allows applications to run in environments that do not planned for the original application. For example, Wine allows Microsoft Windows applications to run on Linux [11].

Application virtualization resides in the Ring 3 of the VM x86 architecture that deals with four privileges levels also known as Ring 0, 1, 2 and 3 [12] as shown in Fig. 2 below.

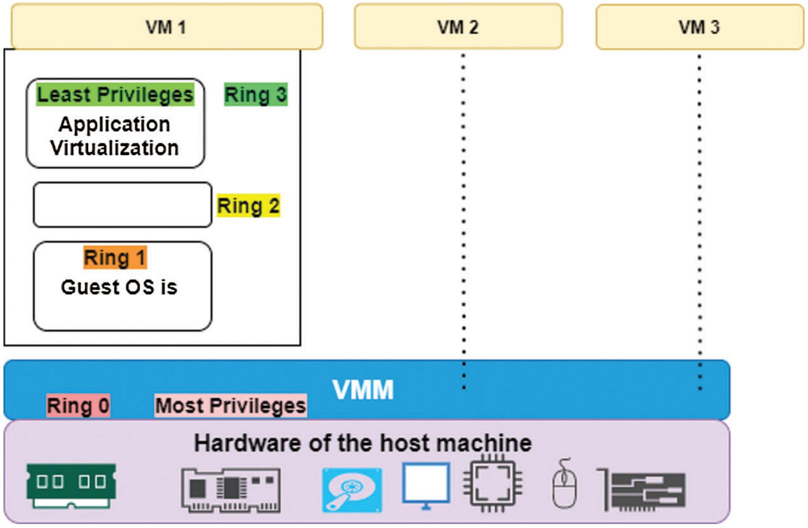

Figure 2: Application virtualization and privileges levels

In its 120-page report, Markets and Markets [13] expected that the Application virtualization market size expected to grow to 4.4 billion$ by 2023 while it was 2.2 billion$ in 2018, at a Compound Annual Growth Rate (CAGR) of 14.0% during the estimated period.

Some examples of application virtualization include:

- **VMware ThinApp**: allowing traditional web applications to run on innovative operating systems, Isolating applications from their underlying operating systems [14].
- **Microsoft App-V**: App-V allows real-time deployment of applications to any client from a virtual application server. With no post local installation [15].
- **PACE Suite:** is an application virtualization tool for: creating MSI, MSIX, Appx, App-V and ThinApp packages and deploy them for Windows OS [16]
- **Ericom Connect:,** Multi-platform remote administration solution used supports wide range network, from any device, via a unified management console [17].
- **DxEnterprise:** is an application virtualization technology, which is available for cross both Windows and Linux environments Operating systems. For cloud environments DEX can run on both Amazon Web Services (AWS) and Microsoft Azure [18].
- **Evalaze:** is an application virtualization technology which is available for different version of Windows operating system [19].
- **AppStream 2.0** is a streaming application built on AWS that benefits from existing architecture, data center and network. It is a fully managed non-persistent application and desktop streaming service [20].

4.2 Network Function Virtualization

In traditional network infrastructure, there exists different hardware appliances (firewalls, switches, routers gateways, etc.) to perform different roles in the network. Network Virtualization Function (NVF) is the implementation of Network Functions (NFs) over software rather than hardware. This software is executed on physical hosts (not necessary network devices) such as Windows and/or Linux based hosts. Which provide virtualized switches, virtualized routers and virtualized firewalls and even virtualized entire network such as ISP. NVF provides easiest flexible and scalable network functions deployment [21]. The market size of NVS is expected to grow to USD 39.3 billion$ by 2023, it was about 12.9 billion$ in 2019, at a Compound Annual Growth Rate (CAGR) of 22.90% during the estimate period [13].

The existing Internet infrastructure was designed on the best-effort class of traffic. Currently, Internet must support multiple classes of traffic with different quality of service (QoS) demands that differ from best-effort demands. Here Network virtualization is a suitable way to overcome QoS limitations over the Internet. In NVF the Internet service provider (ISP) is replaced by two separate business model entities: infrastructure provider (InP) and service provider (SP) [22]. InP manages and deploys the physical infrastructure resources through programmable interfaces to different SPs. SPs creates and aggregates virtual networks (VNs) by aggregating resources from multiple InPs.

VNF poses security threats associated that are the combination of that associated with physical networking and on virtualization technologies. NVF new emerging threats may affect the system that were not possible in the traditional network configuration. We will list most NFV threats, attacks, and possible ways to mitigate them.

4.2.1 Distributed Denial of Service Attacks

The problem of DDoS attack is that resources are not unlimited, and the fact it is hard to distinguish normal traffic from attacking traffic. In typical type of DDoS attack, an attacker assorts a large scale of bot-nodes on the Internet to perform attacks on Virtual Network (VN). The IP identity of the attacker can be hidden by spoofing legitimate IP address of the targeted network [23].

Unified Threat Management (UTM), Intrusion Prevention System (IPS), Web Application Firewall (WAF) are some mitigation techniques of DDoS.

4.2.2 VM Escape

VM Escape occurs when an attacker intends to violate this isolation by utilizing arbitrary codes that make a VM become free from the hypervisor control. VM Escape attacks are possible due to the improper isolation between hypervisors and VNF. The attacker gains access to the hypervisor management API and then penetrates through the hypervisor to cause harmful impact [24]. Possible mitigation of VM Escape are:

- Using hypervisor inspection by NFV providers [25].
- Separating the VM traffic from the management traffic.
- VMs may be grouped according to functionalities into segments, each of which is equipped with a dedicated firewall [26].
- Using blind hypervisor architecture, that limits the hypervisor access to protected areas, in order to prevent an escaped VM from accessing other VMs [27].

4.2.3 Malicious Insider

In this kind of attacks, legitimate users from inside the organization use their privileges to violate the privacy and access data of other users. Insider attacks make data modification on network elements and consequently, unauthorized changes to NE configuration [28].

User/guest authorization, accounting, and VM system activity monitor are good mitigation techniques.

4.2.4 Side Channel Attack

Side Channel attacks take advantage of shared resources such as shared memory resources between VMs. A cache side channel attack results in side channel causes leakage of sensitive data. In side-channel attacks, attackers infer information in an indirect manner, e.g., measuring the frequency at which a VM is paused. Cache side channel attack can be mitigated using different techniques [29]:

- Hardware-based Solutions: in which cache portions are created by isolating cache portion from each other, and each CPU core is assigned a separate cache portion.
- Hypervisor-based Solutions: where changes at the hypervisor level are required.

4.3 Storage Virtualization

Storage virtualization is the technology of hypothesizing physical data storage resources and represent them virtually as a joint and central resource. Pooled storage devices from different vendors. The storage virtualization engine combines the capacity from multiple storage arrays and storage media, aggregates them, manages and presents them as storage resource to end users and applications [30].

There are multiple ways storage can be applied to a virtualized environment [31]:

- Host-based storage virtualization: A host, or group multiple hosts, presents virtual drives of a set capacity to the guest machines.
- Array-based storage virtualization different types of physical storage used as storage tiers.

- Network-based storage virtualization: is the most used virtual storage today. A network device connects to all storage devices in Storage Area Network (SAN) and presents the storage as a virtual pool.

In the next section, we will list most Storage Virtualization threats, attacks, and possible ways to mitigate them.

4.3.1 Attack from VM to Virtual Storages

Once a VM is hijacked, it will have access to a virtual storage, to which other VMs are also attached. Another issue of this attack is the VMs (even while turned off) have in external site-storage, and if an infected VM is restored back on a clean VMM it will infect it [32]. VM isolation is good mitigation strategy.

4.3.2 Confidentiality Attacks

With confidentiality attacks, attacker attempts to read information from a storage system that he is not authorized to. This could be because of weak authentication techniques. Also, covert (side) channel attack may lead to this form of attacks. Good access and auditing techniques and polices are good countermeasures of this attack. Also, encrypting the storage is another good mitigation technique [33].

4.3.3 Integrity Attacks

Poor authorization leads to integrity attacks to alter information in a virtual storage. Data alteration may include creating, changing, writing, and deleting. Strong integrity techniques are good mitigation against this attack [34].

4.3.4 Denial-of-Service (DoS) (i.e., Availability) Attacks

A DoS attack attempts to make virtual storage unavailable. The storage capacity is finite and can be exhausted by huge amount of suspicious requests. Using backups or versioning and DoS mitigation techniques mentioned in NVF section are good mitigation techniques [28,35].

4.4 Desktop Virtualization

Desktop Virtualization, also called Virtual Desktop Infrastructure (VDI), is desktop operating system images run within virtual machines (VMs) that resides on physical server and are delivered to end point clients over a network. Those endpoints may be PCs, Laptops, tablets or thin clients. The entire virtualized desktop operating system appears to end user to be running locally, but is in fact running on the server hosts VM [36].

VDI have similar merits of a virtualized infrastructure, as the end users share the same physical resources and suffering from lack of partitioning and isolation. Furthermore, the centralized management and distribution make the VDI a single point of attack and require clients to exchange data locally [37].

4.4.1 Remote Access Trojans (RAT)

If a malicious software is installed on victim's devices, all data on the VDI and all communications passed on the mobile device may become exposed. Different activities on the Victim VDIs can be recorded and controlled by the attacker such as Keylogging, Screen Scraping and stored password [38] Intrusion detection system is a good mitigation tool, in addition to user awareness not to download any software to their devices from untrusted sources.

4.4.2 Man-in-the-Middle (MitM)

The Man-in-the-Middle (MitM) attack has always been a concern for VDI devices that are not on trusted networks. To defeat against MitM, the mitigation is to adopt SSL as an end-to-end encryption between end devices.

4.5 Server Virtualization

Server Virtualization is a technology, which enables the creation of different virtual servers on a single physical platform. Without server virtualization, each individual server requires physical resources such as CPU, Disk, Memory and network interface(s); but this is not necessary with server virtualization, as all virtual servers share the same physical resources.

There exist several types of server virtualization, namely Full Virtualization, ParaVirtualization, and Hardware-Assisted Virtualization. These types of server virtualization although different in implementation, share the same security threats with similar impact.

In full virtualization, guest operating systems and software are run on top of virtual hardware and abstracted from physical resources. VMs that do not need to be modified to work with different operating systems [39]. Full virtualization is illustrated in Fig. 3.

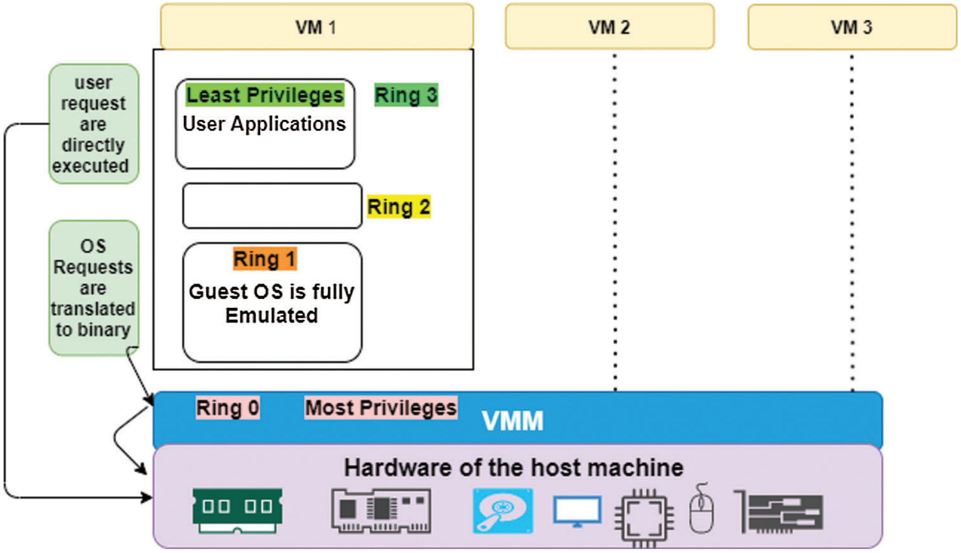
VM 1
VM 2
VM 3
user request are directly executed
Least Privileges
Ring 3
User Applications
Ring 2
OS Requests are translated to binary
Ring 1
Guest OS is fully Emulated
Ring 0
Most Privileges
VMM
Hardware of the host machine

Figure 3: Full virtualization

ParaVirtualization is a lightweight version of the virtualization technique where the hypervisor disclosures hypercalls that can be directly called by a guest OS (that must be modified prior to installation) to simulate privileged instructions that are cannot be virtualized. The hypercalls invoke modified guest OS services through known APIs and implement a virtualized version of system calls. In term of performance and lower overhead, ParaVirtualization operates better than full virtualization, but it requires major changes to the guest operating system [5]. ParaVirtualization is illustrated in Fig. 4.

Hardware-Assisted virtualization is efficient full virtualization using hardware capabilities of the host machine processors. It provides a new execution mode that allows VMM to run in a new privileged mode. It makes hardware extension available to the guest OS. Besides, it requires less OS changes than paravirtualization [37]. Hardware-Assisted Virtualization is illustrated in Fig. 5.

Server virtualization implemented in any of the three variations, namely Full Virtualization, ParaVirtualization, and Hardware-Assisted Virtualization, are threatened by the same security attacks especially those aiming at the virtual machine. VM jumping, Malicious Insider, VM Detection and VM Sprawl are a few of these threats. The following subsections present these threats along the proper means to mitigate the risk posed by these attacks.

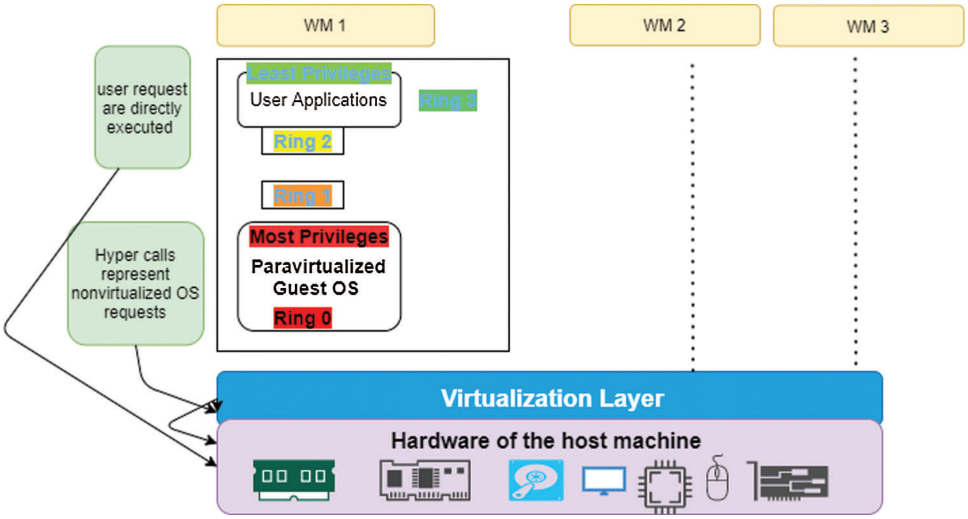

Figure 4: ParaVirtualization

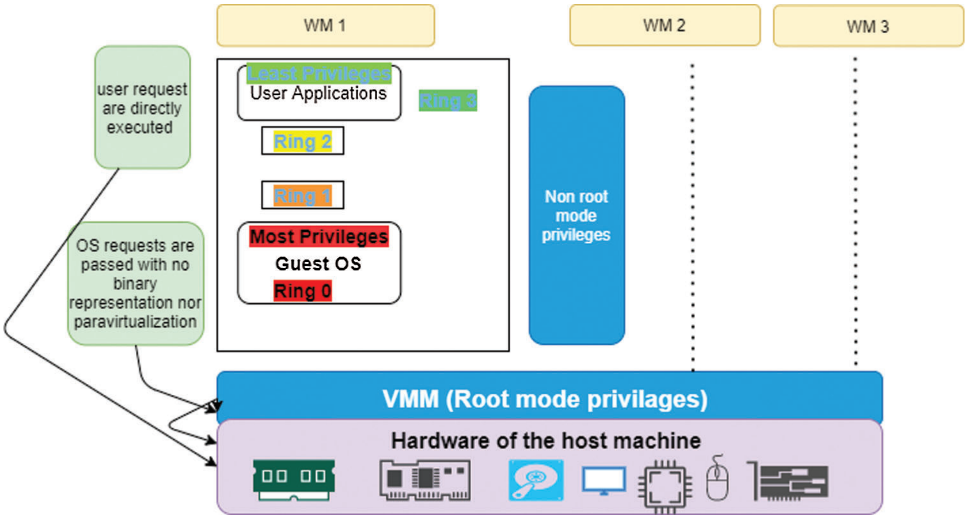
WM 1
WM 2
WM 3
user request are directly executed
OS requests are passed with no binary representation nor paravirtualization
Least Privileges
User Applications
Ring 3
Ring 2
Ring 1
Most Privileges
Guest OS
Ring 0
Non root mode privileges
VMM (Root mode privilages)
Hardware of the host machine

Figure 5: Hardware-assisted virtualization

4.5.1 VM Escape

The attacker utilizes exploit to run code on a VM it to break its control out and interact directly with the hypervisor. Which in turn gives the attacker direct access to the host operating system and all other virtual machines (VMs) running on that server VM segregation, strong authentication procedures, good identity management, and logging procedure are recommended techniques to mitigate VM Escape [40].

4.5.2 VM Jumping

Also known as VM guest hopping, VM jumping exploits weakness in the hypervisor that allows a virtual machine (VM) to be accessed from another VM. In other words, the attacker can jump from one VM to another VM and threaten its availability and integrity. In addition, attacker can gain access to the host server. Grouping of similar traffic and separating groups from each other is good countermeasure, additionally; using VALN between VMs is helpful to mitigate VM Jumping [40].

4.5.3 VM Based Rootkit (VMBR)

VMBR installs a virtual-machine monitor underneath an existing operating system and installs a malicious operating system into VM [41]. Introspecting and Virtual Machine Monitor-Based Lightweight Intrusion are good mitigations of such an attack.

4.5.4 VM Sprawl

This attack occurs when the number of VMs grows rapidly and gets out of control (that is why it is sometimes considered as phenomena). Knowing the right size for VMs according to users' needs and available resources and deploying good VM management are good practices to minimize VM Sprawl [1].

4.5.5 Resource Hogging (VM Poaching)

This threat occurs when a guest OS takes up more CPU, memory, storage or network other than that allocated to it at the expense of other guest OSs [42]. Patching the guest OS and regular resources monitoring are successful mitigation of VM poaching.

4.5.6 Malicious Insider

A malicious insider intentionally misuses the authorized access to VM resources, this threat can be mitigated through good authorization techniques and applying auditing policy.

4.5.7 VM Migration

VM migration is when a VM is migrated from one server to another, for better efficiency and productivity. This process can be live and non-live VM migration. Live migration poses security threats such as DoS, Man-in-the-Middle-Attack, overflow attack and Reply attack. Cryptography, Authentication, Integrity and Authorization are recommended mitigation techniques [43].

4.5.8 VM Detection

For an attacker, detecting a target system that runs inside a certain is important. The attacker may try to exploit the detected VM to know vulnerabilities of the discovered VMM. The use of session key authentication to control guest-host and host-guest communication is a good mitigation [44].

5 Security Solutions for Virtualization

As explained in the previous section, each of virtualization layers can be exposed to more than one attack. These attacks against virtualization environment may result in major security risks and could compromise the entire cloud infrastructure, and the theft of stored data and system hacking. Fig. 6 summarizes the virtualization types and their attacks as shown previously.

Different security solutions have been proposed in different articles and researches to mitigate security attacks against virtualization environment. These security solutions can mitigate or at least minimize the effect of those attacks on virtualization environments.

Unauthorized users should be prevented from accessing the virtualization hardware, thus access control should be applied to each VM. OpenID is an identity management for online usage and can be integrated with an open source Cloud platform OpenStack to provide identity management [45]. Another research in Rueda et al. [46] proposed using SELinux, XEN and IPsec tools to impose Mandatory Access Control (MAC) policies at VM, while relying on the OS and network layers to secure all communications between different VMs. Furthermore, another the security requirements of virtualized environment is to apply some vulnerability assessment for the used virtualization tools.

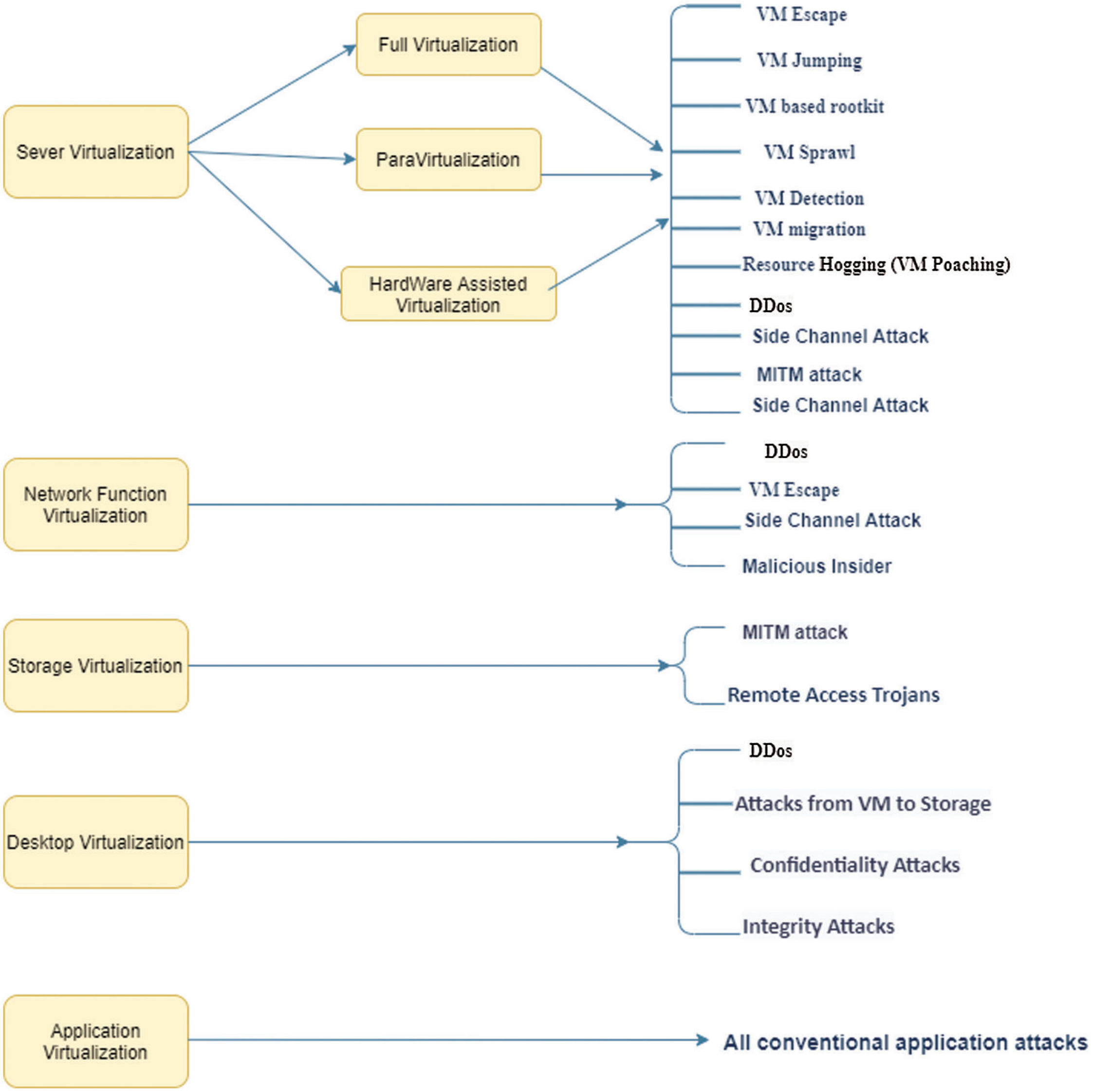

Figure 6: Virtualization types and their security issues

Hypersafe [47] is used for hypervisor security, as Hypersafe maintains code integrity of the Hypervisor preventing code modification by locking down the write-protected memory pages. Consequently, the Hypervisor is secured against the control-flow hijacking attacks. In addition, it prevents insider attackers from performing VM Escape attack. Consequently, proper configuration of the interaction between guest machines and the host OS is important. Furthermore, it is essential to strengthen the hypervisor by separating the administrative duties and roles, thus restricting the hypervisors administrator privileges to modify, create, modify or delete hypervisor logs.

Other protection practices and tools are useful such as anti-viruses, Host Intrusion Prevention System (HIPS), anti-spyware, firewall, web application protection, and log monitoring in the guest OS. Vigilant is proposed in Pelleg et al. [48] to identify guest OS faults that utilizes virtualization and machine learning methods, it necessitates no monitoring agent in VMs. To ensure the integrity of OS, Advanced Cloud Protection System (ACPS) was proposed in Lombardi et al. [49], ACPS monitors and protects the guest

VMs by monitoring of executable system files is to check the behavior of virtual environment. Virtual introspection techniques is used to deploy guest monitoring machine in system seamlessly of the attacker on guest VM. Hence any suspicious activity on the guest OS can be blocked.

Cloud admin must check and ensure that the removal of all data from previous or destroyed disks. When migrating VMs from one old physical machine to new one. Encryption and other cryptographic techniques must employed to protect the backup VM images. Furthermore, to protect VM images from storage attacks, Cloud provider must encrypt the complete VM images when it is in idle state.

SPARC deals with security issues resulting from VM checkpoint attacks. SPARC enables users to select applications that they want to barrier so sensitive applications and processes can't be escaped from inspection.

6 Conclusions

Cloud Computing is the innovative name for the old concept of computing services to a remote location. In cloud computing, Infrastructure as a Service (IaaS) provides logical separation between data, network, applications and machines from physical constrains of real machine.

As the virtualization environment is secured, the security of cloud is maintained. Even though different virtualization methods exist, bare metal virtualization method is the most recommended and thus used in server virtualization. This paper explains general architecture of bare metal virtualization including security aspects of its various components. Cloud virtualization environment can be targeted by different attacks at hypervisor, virtual machines, guest operating system, network virtualization and storage virtualization.

In this paper, we provide an overview of cloud security in all those various aspects, and the attack scenarios of these components. We then present data, API concerns, account hijacking, and related security concerns. Furthermore, the main differences between traditional networking services and cloud services are compared from a security perspective.

The whole picture of virtualization security in Cloud computing is provided through tight analysis of security requirements, attacks and solutions. Many security solutions have been developed to combat the vulnerabilities in virtualization. Traditional security mechanisms such as intrusion detection software and firewall on components of virtualization such as the hypervisor and the guest OS are the most basic forms of security involve implementing. Also, security on how images of VMs are transported, stored and managed is very important due to mobility of VMs. To add additional layer of security, infrastructure security of virtualization is used. The hypervisor is supposed to be secure from assaults and efficiently isolate the VMs, yet potential security flaws are evident. VM Escape out is the most serious of all the assaults mentioned due to the fact the escaped VM would be free to compromise all the other co-resident VMs. Other assaults that focus on stealing facts via side-channels can be mitigated by adding noise to the side-channel. Solving the problem of hypervisor security is a vital step in imparting a secure cloud surroundings for agencies and buyers to utilize.

It has been concluded that each of the virtualization layers can be exposed to more than one attack. Consequently, different security solutions will need to implemented and embedded in the cloud environment to mitigate security attacks against virtualization environment. Possible scenarios may include Hypersafe to maintain the hypervisor code integrity, Host Intrusion Prevention System (HIPS), Vigilant to identify guest OS faults, Advanced Cloud Protection System (ACPS) to monitor and protect the guest VMs or SPARC to deal with VM checkpoint attacks. Addressing these security aspects will help in the future lead headed for more general research to secure cloud virtualization environment. As future work, an assessment criteria can be proposed from which could be useful in analyzing the effectiveness of security solutions of virtualization environment against various virtual environment attacks.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Chen, M. Xian, J. Liu and H. Wang, "Research on virtualization security in cloud computing," *IOP Conf. Series: Materials Science and Engineering*, Chennai, India. vol. 991, 2020.

[2] G. Shanmugasundaram, V. Aswini and G. Suganya, "A comprehensive review on cloud computing security," in *2017 Int. Conf. on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, Coimbatore, India, 2017.

[3] N. Almutairy, K. Al-Shqeerat and H. Al Hamad, "A taxonomy of virtualization security issues in cloud computing environments," *Indian Journal of Science and Technology*, vol. 12, no. 3, pp. 1–19, 2019.

[4] J. Saravanan and P. Saravanan, "A Concept of security and vulnerability attacks, protection process in virtualization for cloud computing," *JAC: A Journal of Composition Theory*, vol. 13, no. 5, pp. 153–161, 2020.

[5] S. M. Jain, Virtualization basics. In: *Linux Containers and Virtualization*. New York, USA: Apress, pp. 1–14, 2020.

[6] F. Siebenlist, "Challenges and opportunities for virtualized security in the clouds," in *SACMAT '09: Proc. of the 14th ACM Symp. on Access Control Models and Technologies*, ACM, NY, USA, pp. 1–2, 2009.

[7] N. Khan and A. Al-Yasiri, "Identifying cloud security threats to strengthen cloud computing adoption framework," *Procedia Computer Science*, vol. 94, pp. 485–490, 2016.

[8] G. Zhu, Y. Yin, R. Cai and K. Li, "Detecting virtualization specific vulnerabilities in cloud computing environment," in *2017 IEEE 10th Int. Conf. on Cloud Computing (CLOUD)*, Hawaii, United States, 2017.

[9] Y. Yadav and C. Krishna, "Two-level security framework for virtual machine migration in cloud computing," *i-Manager's Journal on Information Technology*, vol. 7, no. 1, pp. 34–44, 2017.

[10] T. Zhang and R. Lee, "Monitoring and attestation of virtual machine security health in cloud computing," *IEEE Micro*, vol. 36, no. 5, pp. 28–37, 2016.

[11] G. Hunt, R. Olinsky and M. Fortin, "Application compatibility with library operating systems," *Google Patents*, Patent No: US 9, 891, 939 B2, 2018. [Online]. Available: https://www.freepatentsonline.com/y2012/0227061.html.

[12] C. Horne, "Understanding full virtualization, paravirtualization and hardware assist," White paper, VMware Inc., 2007.

[13] MarketsandMarkets, "Application Virtualization Market," San Francisco, USA, 2004. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/application-virtualization-market-263424909.html.

[14] VMWare, "ThinApp," 2008. [Online]. Available: https://www.vmware.com/products/thinapp.html.

[15] Z. Yang, S. Zhou, J. Zu and D. Inman, "High-Performance piezoelectric energy harvesters and their applications," *Joule*, vol. 2, no. 4, pp. 642–697, 2018.

[16] Softpedia, "PACE Suite," 2014. [Online]. Available: https://www.softpedia.com/get/Authoring-tools/Authoring-Related/PACE-Suite.shtml.

[17] Ericom, "Ericom Connect," 2020. [Online]. Available: https://www.ericom.com/connect-feature-matrix.asp.

[18] DxEnterprise, "DH2i," 2020. [Online]. Available: https://dh2i.com/dxenterprise/.

[19] Rorymon, "Evalaze Application Virtualization," 2016. [Online]. Available: https://www.rorymon.com/blog/evalaze-application-virtualization-2-1/.

[20] S. Narula, A. Jain and Prachi, "Cloud computing security: Amazon web service," in *Computer Science Fifth Int. Conf. on Advanced Computing & Communication Technologies*, Haryana, India, 2015.

[21] A. Alwakeel, A. Alnaim and E. Fernandez, “A survey of network function virtualization security,” in *Southeast Conf. 2018*, Florida, USA, 2018.

[22] P. Jeyabharathi and S. Kaliappan, “Optimal resource allocation using software defined network for wireless IOT application using RBFNN,” *Tierärztliche Praxis*, vol. 40, pp. 1343–1354, 2020.

[23] A. Jakaria, W. Yang, B. Rashidi, C. Fung and M. Rahman, “Vfence: A defense against distributed denial of service attacks using network function virtualization,” in *2016 IEEE 40th Annual Computer Software and Applications Conf. (COMPSAC)*, Atlanta, USA, 2016.

[24] S. Lal, T. Taleb and A. Dutta, “NFV: Security threats and best practices,” *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[25] I. Faynberg and S. Goeringer, “NFV security: Emerging technologies and standards,” *Guide to Security in SDN and NFV: Springer*, pp. 33–73, 2017.

[26] A. Alnaim, A. Alwakeel and E. B. Fernandez, “A Misuse pattern for compromising VMs via virtual machine escape in NFV,” in *Proc. of the 14th Int. Conf. on Availability, Reliability and Security*, Canterbury, United Kingdom, pp. 1–6, 2019.

[27] Y. Dong and Z. Lei, “An access control model for preventing virtual machine hopping attack,” *Future Internet*, vol. 11, no. 3, pp. 11–82, 2019.

[28] A. Dutta and E. Hammad, “5G Security challenges and opportunities: A system approach,” *IEEE 3rd 5G World Forum (5GWF)*, vol. 1, pp. 109–114, 2020.

[29] A. Litchfield and A. Shahzad, “Virtualization technology: Cross-VM cache side channel attacks make it vulnerable,” *in Australasian Conf. on Information Systems*, Australia, 160601356, 2016.

[30] F. Guthrie, S. Lowe and K. Coleman, *VMware I. vSphere Storage*. New Jersey, USA: John Wiley & Sons, 2013.

[31] M. Abu-Alhaija, “Cyber security: Between challenges and prospects,” *ICIC Express Letters Part B: Applications*, vol. 11, no. 11, pp. 1019–1028, 2020.

[32] R. Hörmansederand and M. Jäger, “Cloud security problems caused by virtualization technology vulnerabilities and their prevention,” *IDIMT-2014 Networking Societies-Cooperation and Conflict*, vol. 43, pp. 373–383, 2014.

[33] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan *et al.,* “Integrating encryption techniques for secure data storage in the cloud,” *Transactions on Emerging Telecommunications Technologies*, vol. 1, pp. e4108, 2020.

[34] A. Singh, S. Awasthi and M. Wajid, “Data storage security issues in cloud computing,” in *ICCBI 2019: Proc. of the Int. Conf. on Computer Networks, Big Data and IoT*, Madurai, India, pp. 177–187, 2018.

[35] S. Olarig and J. Martineau, “System and method of detecting and countering denial-of-service (DOS) attacks on an NVME-of-based computer storage array,” *Google Patents*, U.S. Patent No. 10,686,833. 16, 2020.

[36] M. Pearce, S. Zeadally and R. Hunt, “Virtualization: Issues, security threats, and solutions,” *ACM Computing Surveys (CSUR),* article, vol. 45, no. 17, pp. 1–39, 2013.

[37] N. Ahmad, “Cloud computing: Technology, security issues and solutions,” in *2017 2nd Int. Conf. on Anti-Cyber Crimes (ICACC)*, Abha, KSA, pp. 30–35, 2017.

[38] P. Calle-Romero, P. Lema-Sarmiento, P. Gallegos-Segovia, G. León-Paredes, P. Vintimilla-Tapiaand *et al.,* “Virtual desktop infrastructure (VDI) deployment using opennebula as a private cloud,” in *Int. Conf. on Applied Technologies*, Quito–Ecuador, pp. 440–450, 2019.

[39] D. Barrett and G. Kipper, “Server virtualization,” in *Virtualization and Forensics*, Elsevier Inc., Amsterdam, 2010.

[40] A. Chaudhuri, H. Ferrer, H. Prafullchandra and J. Sherry, “Best practices for mitigating risks in virtualized environment,” *Cloud Security Alliance, Tech Rep*, pp. 1–35, 2015.

[41] S. King and P. Chen, “SubVirt: Implementing malware with virtual machines,” *2006 IEEE Sym. on Security and Privacy (S&P'06)*, California, USA, vol. 14, pp. 313–327, 2006.

[42] D. Tank, A. Aggarwal and N. Chaubey, “Cyber security aspects of virtualization in cloud computing environments: Analyzing virtualization-specific cyber security risks,” in *Quantum Cryptography and the Future of Cyber Security, IGI Global*, Hershey, USA, pp. 283–299, 2020.

[43] A. Mishra, N. Gupta and B. Gupta, “Security threats and recent countermeasures in cloud computing,” in *Modern Principles, Practices, and Algorithms for Cloud Security, IGI Global*, Hershey, USA, pp. 145–161, 2020.

[44] P. Ferrie, "Attacks on more virtual machine emulators," *Symantec Technology Exchange*, vol. 55, pp. 369–386, 2007.

[45] R. Khan, J. Ylitalo and A. Ahmed, "OpenID authentication as a service in OpenStack," in *2011 7th Int. Conf. on Information Assurance and Security (IAS)*, Malacca, Malaysia, pp. 372–377, 2011.

[46] S. Rueda, Y. Sreenivasan and T. Jaeger, "Flexible security configuration for virtual machines," in *Proc. of the 2nd ACM Workshop on Computer Security Architectures*, Alexandria, USA, pp. 35–44, 2008.

[47] Z. Wang and X. Jiang, "Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity," in *2010 IEEE Sym. on Security and Privacy*, California, USA, pp. 380–395, 2010.

[48] D. Pelleg, M. Ben-Yehuda, R. Harper, L. Spainhower and T. Adeshiyan, "Vigilant: Out-of-band detection of failures in virtual machines," *ACM SIGOPS Operating Systems Review*, vol. 42, no. 1, pp. 26–31, 2008.

[49] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113–1122, 2011.