Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison

Article *in* International Journal of Information Technology · February 2019

DOI: 10.1007/s41870-019-00294-x

CITATIONS
6

READS
6,074

3 authors, including:

Darshan Tank
Gujarat Technological University
12 PUBLICATIONS **68** CITATIONS

SEE PROFILE

Nirbhay Chaubey
Gujarat Technological University
50 PUBLICATIONS **270** CITATIONS

SEE PROFILE

Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison

Darshan Tank, Akshai Aggarwal & Nirbhay Chaubey

International Journal of Information Technology
An Official Journal of Bharati Vidyapeeth's Institute of Computer Applications and Management

ISSN 2511-2104

Int. j. inf. tecnol.
DOI 10.1007/s41870-019-00294-x

Springer

Int. j. inf. tecnol.
https://doi.org/10.1007/s41870-019-00294-x

ORIGINAL RESEARCH

Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison

Darshan Tank[1] · **Akshai Aggarwal**[2] · **Nirbhay Chaubey**[3]

Received: 14 June 2018 / Accepted: 4 February 2019

Abstract Virtualization is technological revolution that separates functions from underlying hardware and allows us to create useful environment from abstract resources. Virtualization technology has been targeted by attackers for malicious activity. Attackers could compromise VM infrastructures, allowing them to access other VMs on the same system and even the host. Our article emphasize on the assessment of virtualization specific vulnerabilities, security issues and possible solutions. In this article, a recent comprehensive survey on virtualization threats and vulnerabilities is presented. We also described taxonomy of cloud-based attacks on the virtualized system and existing defense mechanisms intended to help academia, industry and researchers to gain deeper and valuable insights into the attacks so that the associated vulnerabilities can be identified and subsequently required actions would be taken. We provide an exhaustive comparison of various techniques proposed by researchers to resolve virtualization specific vulnerabilities. To guide future research, we discussed generalized security measures and requirements to be taken to achieve secure virtualized implementations. At the end, we shed some light on cloud shared responsibility model to decide which roles cloud service providers and cloud service customers play in cloud security. The aim of this article is to deliver researchers, academicians and industry with a superior understanding of existing attacks and defense mechanisms on cloud security.

Keywords Defense mechanisms · Cloud shared responsibility model · Hypervisor · Security issues · Security measures · Taxonomy · Virtualization · Virtual machine · Vulnerabilities

1 Introduction

Cloud computing is currently influencing many daily activities and has many exclusive properties that make it very valuable. Regrettably, many of those properties make security a unique interest [1]. Cloud service providers and customers must well aware of these security concerns and must have developed new technologies to address them. Different types of cloud computing service models provide different levels of security services. IaaS (Infrastructure as a Service) is the lowest level services in cloud service model, with PaaS (Platform as a Service) and SaaS (Software as a Service) the next two services above. As we move upward in the stack, each service model inherits the capabilities of the model beneath it, as well as all the inherent security concerns and risk factors. As we ascend the stack, IaaS has the least levels of integrated functionality and the lowest levels of built in security [2].

Virtualization is a key enabler of the key attributes of cloud computing: Service-based, Scalable and elastic, Shared services, Metered usage. Virtualization supplies a foundation to deliver infrastructure as a service over the

✉ Darshan Tank
dmtank@gmail.com

Akshai Aggarwal
akshai.aggarwal@gmail.com

Nirbhay Chaubey
nirbhay@ieee.org

[1] L E College (Diploma), Gujarat Technological University, Ahmedabad, Gujarat, India

[2] School of Computer Science, University of Windsor, Windsor, Canada

[3] S S Agrawal Institute of Computer Science, Gujarat Technological University, Ahmedabad, Gujarat, India

Published online: 27 February 2019

cloud. Virtualization allows the effective allocation and adjustment of multiple VMs with one physical host machine beneath or the movement of one VM among different hosts [3]. Virtual Machine Monitor (VMM) technology offers significant benefits in terms of functional isolation and performance isolation, live-migration-enabled load balance, fault tolerance, portability of applications, and higher resource utilization. However, the design, implementation, and deployment of virtualization technology have also opened up novel threats and security issues which, take on new forms in relation to it [4].

Infrastructure as a service allows us to get access to machines and install our own operating systems, but without having the security. Thus, it is important to address the security issues and problems in cloud systems and to find a solution for the widespread acceptance of these solutions [5]. Virtualization security addresses the security issues faced by the components of a virtualization infrastructure/environment. The initial discovery of vulnerabilities in virtualization environment is essential for virtualization accomplishment and to defend against attacks that may cause information leakage or virtual machine (VM) escape [3]. There may be many attack pathways, such as prebuilt virtual machines/virtual appliances comprising malicious code, erroneously configured virtual firewalls or networking, erroneously configured hypervisor, and data leakage through offline images. In fact protecting virtual machines can be more difficult than protecting physical machines. Attacking a single physical host could possibly give the attacker access to confidential data stored in many different virtual servers [6].

Various tools and techniques are used to implement cloud based virtualization. The overall function of these systems is to manage the provisioning of virtual machines for a cloud providing infrastructure-as-a-service. There exist commercial and open source solutions. The major open source IaaS cloud management platforms are Eucalyptus, OpenNebula, Nimbus, CloudStack and OpenStack. These various open source projects provide an important alternative for those who do not wish to use a commercially provided cloud [7]. The commercial solutions are Hyper-V, VMware, ESX, etc. It is observed that the open source solution such as OpenStack provides more flexibility and development support than the other commercial solutions. Nevertheless, open source solutions suffer from a lack of documentation and are more difficult to accomplish. The hypervisors, such as Hyper-V, KVM, Xen and VMware vSphere are used with this open source solution. Hypervisor uses different architectures, although it is limited to hardware-assisted virtualization mode. The Windows-based Hyper-V delivers a notably different architecture than the Linux based hypervisors. Xen and KVM are based on open source modification of the Linux kernel, whereas VMware uses custom build functions [8]. Xen hypervisor uses PV of separate management domain; controls the VMs, access to user defined block and network drivers. KVM considered as a key module that employs most of the Linux features. VMs services and cloud service providers offer more powerful and anchor ecosystem of cloud services. User provides their VMs and cloud provider leads them often without the knowledge of the guest operating system. Cloud providers, security-as-a-service based on VM introspection and ensures the best security [8].

With the use of virtualization, cloud computing brings about not only convenience and efficiency benefits but also creates new vulnerabilities and threats on a virtualization based cloud system [9]. Until and unless the virtualization environment is secured, the security of cloud cannot be guaranteed. The identification and implementation of strategies for the evaluation of all the aspects that may influence the security of a cloud computing environment are extremely necessary for the protection of sensitive data stored by cloud infrastructures. Our contributions in this paper are: (1) provide taxonomy of cloud-based attacks on virtualized system and existing defense mechanisms; (2) present various security issues disclosed in recent years in cloud virtualization components and perform a comparative analysis of various techniques proposed by the researchers to solve virtualization specific vulnerabilities in cloud computing; (3) furnish security measures or requirements to be taken to handle various security concerns.

Cloud virtualization threats and vulnerabilities are major obstacles in the adoption of cloud computing paradigm. The rest of the paper is organized as follows. In Sect. 2, we review the work related to recent virtualization vulnerabilities and virtualization security threats. Section 3 outlines the virtualization security concerns in cloud computing. Section 4 presents a classification of virtualization security attacks in cloud computing. In Sect. 5, virtualization security attacks on different virtualization elements containing hypervisor, virtual machines and guest operating system images in cloud computing are particularized. We present a comparative analysis of various techniques proposed by the researcher to solve virtualization specific vulnerabilities in cloud computing. Section 6 deals with virtualization security measures and requirements to be taken to handle various security concerns. Section 7 investigates cloud shared responsibility model to determine which roles cloud service providers and cloud service customers play in cloud security. Finally, Sect. 8 discusses the conclusion remarks and future research areas.

2 Related work

Security issues in cloud computing have received broad attention recently, and many researchers have studied security issues in the virtualization layer. In a virtualized environment, each of the VMs is detached from the rest of the system by the hypervisor or Virtual Machine Monitor (VMM). A strong accomplishment can break this confinement and thus point to various concerns respecting the confidentiality, integrity, or availability of the VMs [3]. Many of the virtualization vulnerabilities are unique to the cloud platform and can hardly be addressed by existing techniques. The number of virtualization security vulnerabilities disclosed is increasing year by year and more researchers are focusing on this field. The VMM is a key issue in virtualization security. The VMM is a software module that controls all the virtual machines and their connection with the hardware. The main duty of the VMM is the management and isolation of each running VM and is also responsible for the creation and management of each virtual resource. The interconnection complexities and more entry points in the VMM can encourage a large number of attack vectors [10].

Zhang et al. [11] proposed a method of Rootkit detection based on KVM by using virtualization technology. Wojtkowiak [12] outline 259 new virtualization vulnerabilities over the last 5 years and new attack types (e.g. Hyperjacking, hypervisor escape, VM attacks). Pearce et al. [4] showed in their work the hypervisor vulnerability, along with breaking the security of the Xen and KVM (Kernel-based Virtual Machine). Gupta and Kumar [13] discuss the prospect of secure system isolation and presented issues that arise from strong virtualization and from weak implementation of core virtualization, but the necessary associated test procedures are not specifically implemented. Perez-Botero et al. [14] presented a thorough analysis of the codebase of two popular open-source Hypervisors (Xen and KVM), and vulnerability reports associated with them. Perez-Botero et al. [14] proposed a characterization of Hypervisor Vulnerabilities comprised of three dimensions: the trigger source, the attack vector, and the attack target. Moyo and Bhogal [15] investigated security issues in cloud computing and states that virtual machines could use side-channeling to extract private cryptographic keys which are used by other VMs on the same server. Kazim and Zhu [16] described security issues in cloud virtualization components such as hypervisor, virtual machines and guest disk images.

Wang et al. [17] explored a shared memory based cross-VM side channel attacks in IaaS cloud. Hussain et al. [18] presents a novel multilevel classification model of different security attacks across different cloud services at each layer. They have also identified attack types and risk levels associated with different cloud services at these layers. Zhang and Lee [19] analyzed inside-VM and outside-VM vulnerabilities. They showed that a VM can get infected with malware or OS rootkits at runtime and can take complete control of the VM and significantly compromise its security state. The threats from the host OS and co-located VMs are hard for customers to defeat. Wu et al. [20] proposed an access control model that can prevent virtual machine escape (PVME) by adapting the BLP (Bell-La Padula) model (an access control model developed by Bell and LaPadula). Geeta et al. [21] discussed a comprehensive survey on the state-of-art techniques in data auditing and security. Challenging problems in information repository auditing and security are presented. Dubey et al. [22] made an attempt to do a SWOT analysis of a cloud computing environment. A critical and detail analysis is done by mapping its Strengths (S), Weakness (W), Opportunity (O), and Threat (T) in different ways. Zhang and Lee [23] proposed a flexible architecture, CloudMonatt, to monitor and attest the security health of customers' VMs within a cloud system. Ravi Kumar et al. [24] explored the different data security issues in cloud computing in a multi-tenant environment and proposed methods to overcome the security issues.

During the study, we observed that while some of the vulnerabilities exist in conventional computing environments and can be discovered by existing techniques, many others have definite properties connected to virtualized systems, such as software emulated hardware logic and an opponent's capability to command the implementation flow of a few virtual hardware that cannot simply be addressed. Out of the four main hypervisor offerings, which take up 93% of the total market share, two are closed-source (VMWare and Hyper-V) and two are open-source (Xen and KVM) [25]. Our study focused mainly on Xen and KVM (Kernel-based Virtual Machine) because Microsoft Hyper-V and VMW are closed-source commercial software, which makes it hard to interpret the internal logic of the VMMs and analyze their vulnerabilities [3].

3 Virtualization vulnerabilities

Virtualization assigns a logical name for a physical resource and then provides a pointer to that physical resource when a request is made. Virtualization provides a means to manage resources efficiently because the mapping of virtual resources to physical resources can be both dynamic and facile. Virtualization is dynamic in that the

mapping can be assigned based on rapidly changing conditions, and it is facile because changes to a mapping assignment can be nearly instantaneous [2]. These are among the different types of virtualization that are characteristic of cloud computing:

- *Access* A client can request access to a cloud service from any location.
- *Application* A cloud has multiple application instances and directs requests to an instance based on conditions.
- *CPU* Computers can be partitioned into a set of virtual machines with each machine being assigned a workload. Alternatively, systems can be virtualized through load-balancing technologies.
- *Storage* Data is stored across storage devices and often replicated for redundancy.

As the enabling technology, virtualization plays an important role in cloud computing by providing the capability of running multiple operating systems and applications on top of the same underlying hardware [3]. Virtualization is the process of converting a physical IT resource into a virtual IT resource. A key use of virtualization technology is server virtualization, which uses a software layer called a hypervisor to emulate the underlying hardware [26]. Increased flexibility can increase security risk. Cloud virtualization infrastructure can be undermined by different assaults at the hypervisor, virtual machines and guest disk images [27].

Virtualization is primarily used in cloud computing systems to detach user environments. At present virtualization is chiefly used in datacenters to strengthen computers and to grow the use of the datacenter's capacity [28].

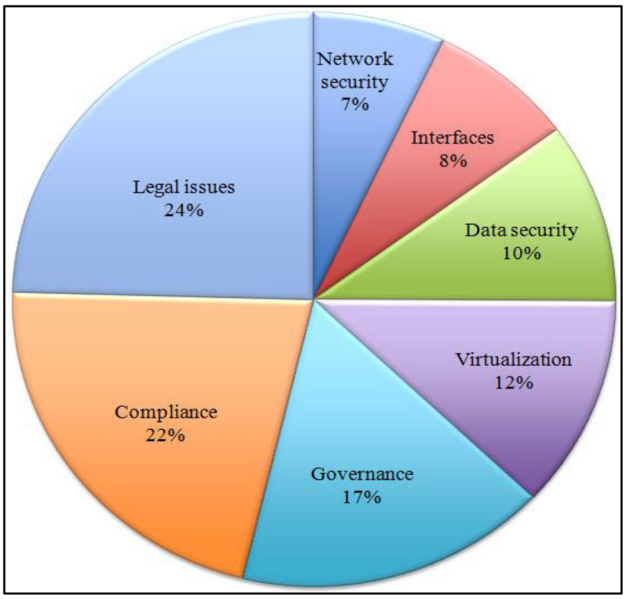

Fig. 1 Pie chart for security concerns with grouped categories [20]

As shown in Fig. 1, the technical issue more intensively evaluated (12%) is virtualization, followed by data security, interfaces, and network security. Virtualization is one of the main novelties employed by cloud computing in terms of technologies employed, considering virtual infrastructures, scalability and resource sharing, and its related problems represent the first major technical concern [29].

4 Taxonomy of cloud-based attacks on the virtualized systems

To secure a cloud environment, current security threats in a cloud environment need to be identified and taken care off while delivering services in cloud for ensuring high level of security towards familiar or derivable attacks [13]. Figure 2 shows the taxonomy of the possible attacks on a cloud environment. The attack taxonomy not only describes existing threats on cloud security, but also provides various defense mechanisms to protect the cloud environment from such attacks.

While there are many threats over the virtualized system, we have categorized threats into Hypervisor-based attacks, VM-based attack, and VM image attacks. Figure 3 shows the taxonomy of attacks on various virtualization components in cloud computing. Our taxonomy covers the cloud-based attacks on the virtualized systems at infrastructure as a service layer.

Table 1 shows three categories of cloud-based attacks on the virtualized system; (1) Hypervisor-based, (2) VM-based and (3) VM image. We have identified possible sub-attacks at these components and existing security schemes to provide security to virtualized environment.

Spiteful programs in distinct virtual machines can achieve required access permissions to log keystrokes and screen updates across virtual terminals that can be exploited by attackers to gain sensitive information. Live virtual machine images can be simply duplicated to form new virtual machine image files, which after-effects in VM image sprawl issue, in which a massive number of virtual machines formed by cloud customers may be left unseen.

The pie chart in Fig. 4 presents the security concerns on virtualization platform. We have gone through a number of peer-reviewed papers published in reputed international journals and conferences on security concerns surrounding virtualization and conclude in the form of pie chart. The three major categories identified are hypervisor-based attacks, VM-based attacks, and VM image attacks. Our analysis shows that the highest percentage of attacks could be exploited on hypervisors followed by VMs and VM images in virtualized environments.

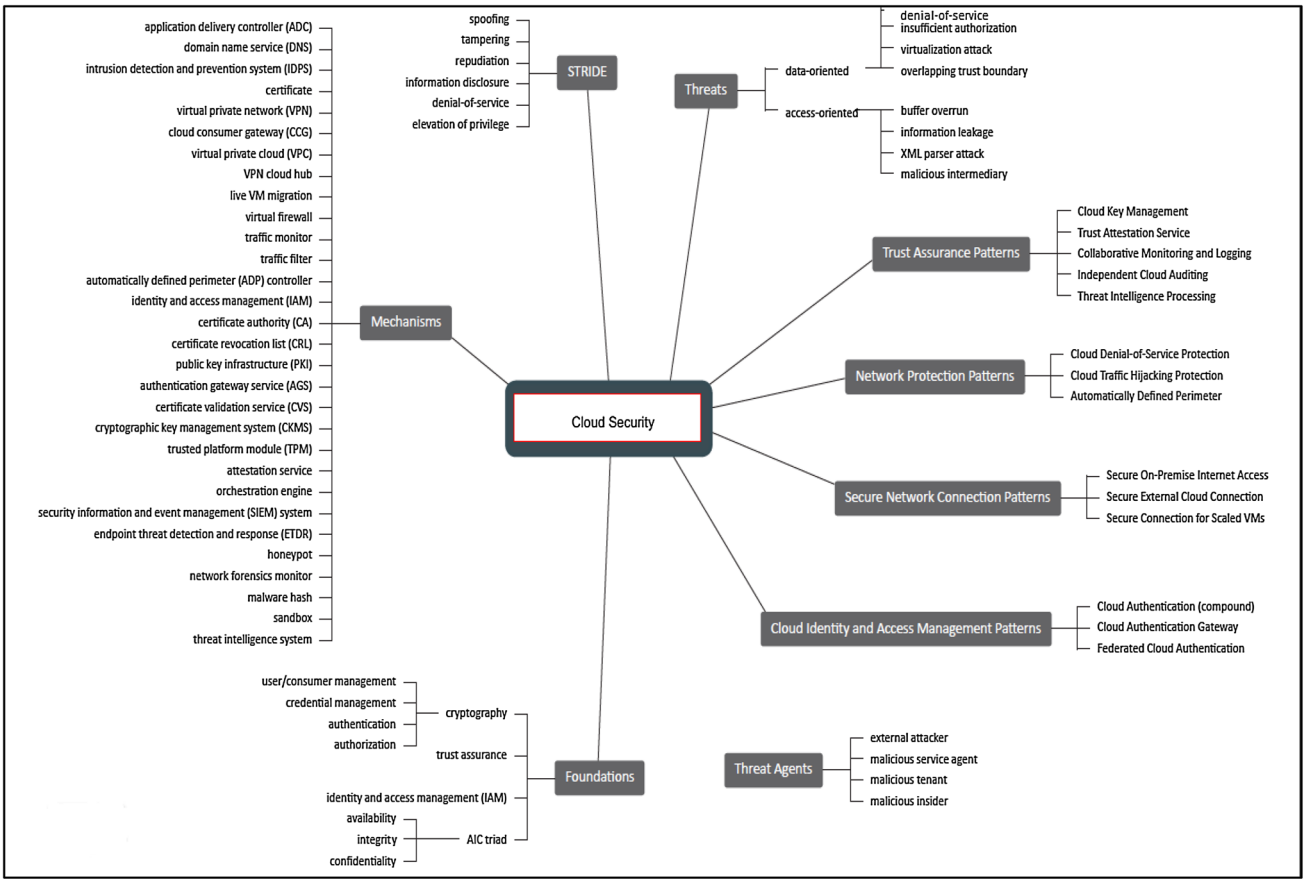

Fig. 2 Taxonomy of security in cloud environment (retrieved from http://cloudschool.com)

5 Virtualization security issues

We have analyzed and identified security issues discovered in recent years in distinct cloud virtualization elements, such as a hypervisor, virtual machines, and guest disk images [16]. A hypervisor-based attack is an exploit in which an intruder takes advantage of vulnerabilities in the program used to allow multiple operating systems to share a single hardware processor. A compromised hypervisor can allow the hacker to attack each virtual machine on a virtual host. Larger software stacks and greater numbers of APIs, along with a lower degree of security assurance in the code, increase the risk [30]. We highlight the following attacks in virtualized environments.

5.1 VM escape

Virtual machines are designed to support strong isolation between the host and the VMs [31]. But the vulnerabilities in the operating system running inside the VM can aid attackers to insert a malicious program into it. When that program is run, VM breaks the isolated boundaries and starts communicating with the operating system directly bypassing the VMM layer. Such an exploit opens the door to attackers to gain access to the host machine and launch further attacks.

5.2 Hyperjacking

Hyperjacking is an attack in which a hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine (VM) host. The point of the attack is to target the operating system that is below that of the virtual machines so that the attacker's program can run and the applications on the VMs above it will be completely oblivious to its presence [32].

5.3 VM sprawl

VM sprawling occurs when a large number of virtual machines exist in the environment without proper management or control. Since they retain the system resources (i.e., memory, disks, network channels etc.) during this

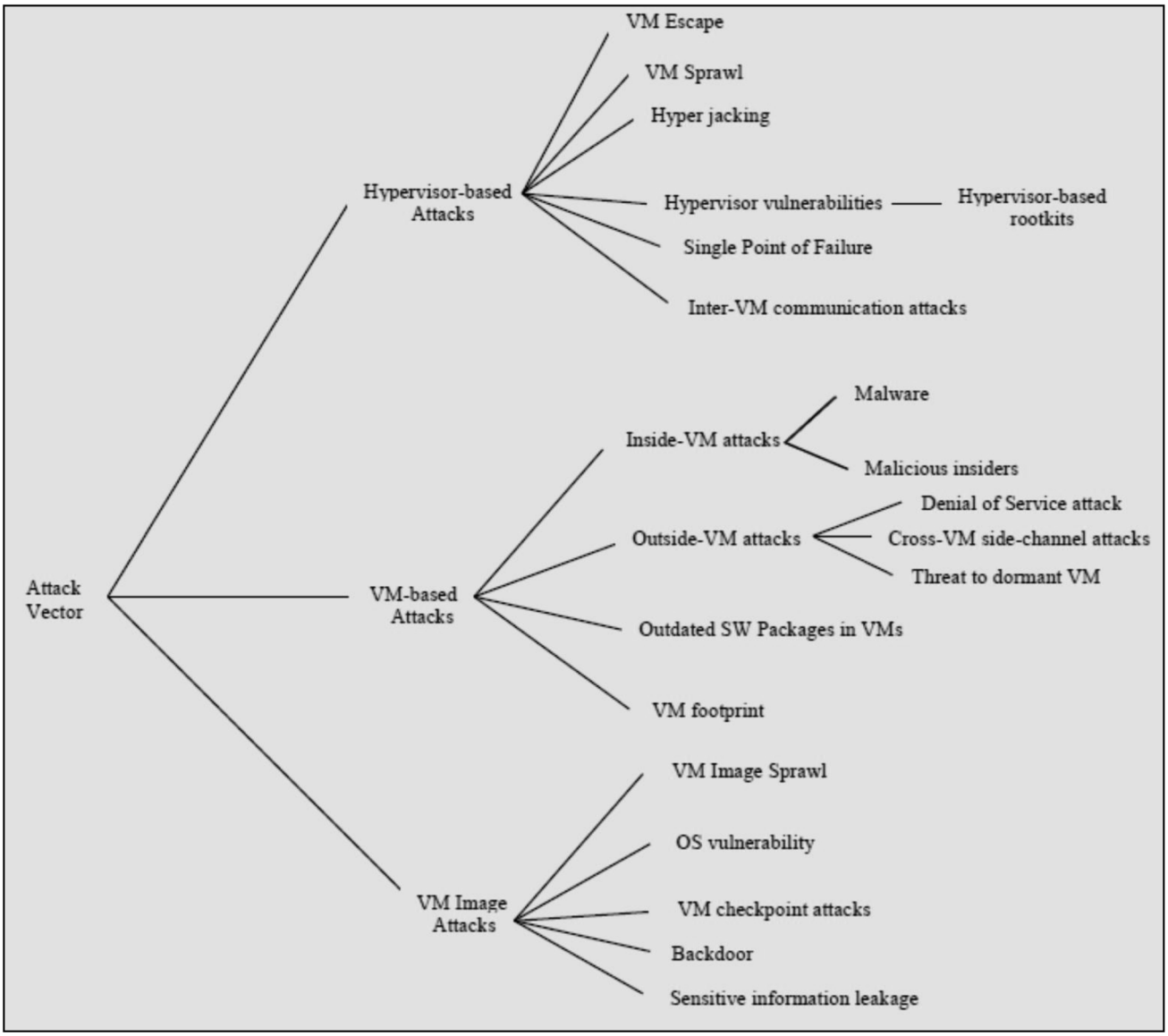

Fig. 3 Taxonomy of cloud-based attacks on the virtualized system

period, these resources cannot be assigned to other VMs, and they are effectively lost.

5.4 Hypervisor vulnerabilities

A hypervisor or VMM is formed to run numerous guest VMs and applications simultaneously on a single host machine and to provide separation among the guest VMs [33]. Despite the fact that hypervisors are anticipated to be vigorous and secure, they are accessible to attacks. If attackers gain command of the hypervisor, all the VMs and the data accessed by them will be under their full control to utilize. One more reason hackers contemplated the VMM a possible target, is the greater control provided by the bottom layers in the virtualized system. Compromising a VMM also helps to gain control of the underlying physical system and the hosted applications. Some of the well-known attacks (e.g., Bluepill, Hyperjacking, etc.) insert VM-based rootkits that can install rogue hypervisor or modify the existing one to take complete control of the environment. Since hypervisor runs underneath the host OS, it is difficult to detect these sorts of attack using regular security measures.

5.5 Single point of failure

Existing virtualized environments are based on the hypervisor technology that controls the access of the VMs to physical resources and is important for the overall functioning of the system. Therefore, failure of the hypervisor

Table 1 Cloud-based attacks on the virtualized system and existing defense mechanisms

S. no.	Attacks	Sub-attacks	Existing defense mechanisms
1	Hypervisor-based attacks	VM Escape attack	Designing secure hypervisors [47, 48]
		HyperJacking, BLUEPILL, Vitriol, SubVirt and DKSM attacks	Protecting hypervisor integrity [49, 50]
		VM Sprawl	Reducing hypervisor attack surface [43–53]
		Hypervisor vulnerabilities	Intrusion Detection System [54]
		Hypervisor-based rootkits	Properly configuring the interaction between guest machines and host VM [55]
		Single Point of Failure	By encrypting VMsR
		Inter-VM communication attacks	Hypersafe [56]
2	VM-based attacks	Inside-VM attacks	Introspecting VMs [57, 58]
		Malware	Virtual Machine Monitor-Based Lightweight Intrusion [59]
		Malicious insiders	Building a MAC-based security architecture for the Xen open-source hypervisor [60]
		Outside-VM attacks	Co-Residency Detection in the Cloud via Side-Channel Analysis [11]
		Denial of Service (DoS) attacks	A Security-Aware Scheduler for Virtual Machines on IaaS Clouds [61]
		Cross-VM side-channel attacks	Using anti-viruses, anti-spyware programs in guest OS to detect any suspicious activity [62]
		A threat to dormant VM	Using encryption and hashing of VMs state before saving
		Outdated SW Packages in VMs	
		VM footprint	
3	VM Image attacks	VM Image Sprawl	Managing VM images [63]
		VM checkpoint attacks	Encrypting the checkpoints or using SPARCR [64]
		OS vulnerability	Enforcing policies to manages issues of unnecessary images [65]
		Backdoor	
		Sensitive information leakage	

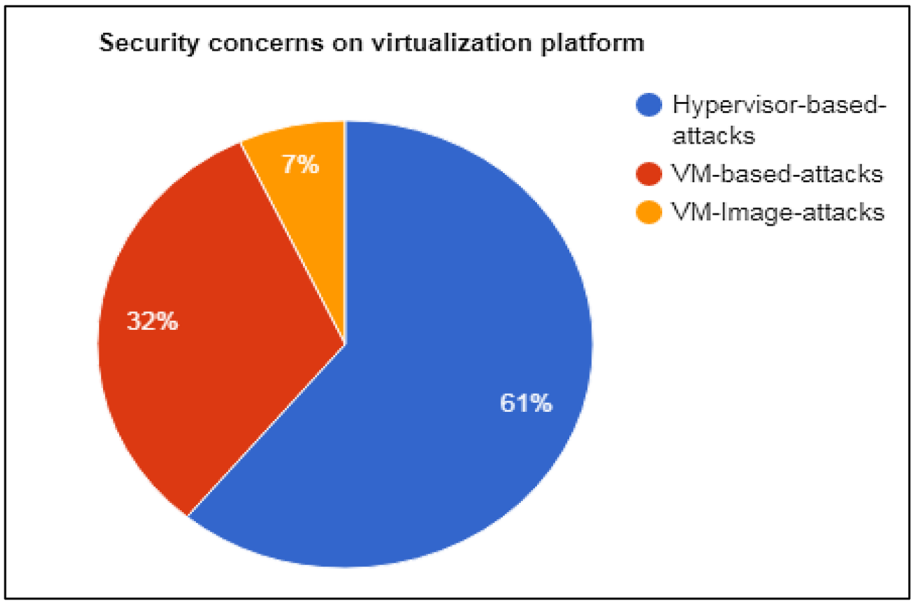

Fig. 4 Pie chart for security concerns on a virtualization platform

due to overused infrastructure or software faults leads to the collapse of the overall system.

5.6 Inside-VM attack

VM can get infected with malware or OS rootkits at runtime. Such attack can take complete control of the VM and significantly compromise its security state [23].

5.7 Outside-VM attack

Attacks from the host OS and co-located VMs are known as outside-VM attacks [23]. Outside-VM attacks are hard for customers to defeat. A malicious VM can potentially access other VMs through shared memory, network connections, and other shared resources. For example, if a malicious VM determines where another VM's allocated memory lies, then it could read or write to that location and interfere with the other's operation [34].

5.8 Cross VM side channel attack

To maximize resource utilization, multiple VMs are usually placed on the same physical server in the Cloud environment and this co-resident placement is a potential threat to cross VM side channel attack [35]. The basic idea is: a malicious VM penetrates the isolation between VMs, and then access the shared hardware and cache locations to extract confidential information from the target VM [36].

5.9 Outdated SW packages in VMs

Outdated software packages in virtual machines can pose serious security threats in the virtualized environment [37]. Because of the low cost and the ease of creation, users tend to create new virtual machines for different tasks, branch new virtual machines based on the old ones, snapshot machines or even rollback machines to an earlier state [38]. These operations may have serious security implications, for example, a machine rollback operation may expose a software bug that has already been fixed.

5.10 VM footprint

VM footprinting is the technique used for gathering information about target VM like OS installed, packages installed and services running etc. It refers to one of the pre-attack phases; tasks performed prior to doing the actual attack [39].

5.11 VM image sprawl

Live virtual machine images can be simply duplicated to form new virtual machine image files, which after-effects in VM image sprawl issue, in which a massive number of virtual machines formed by cloud customers may be left unseen. VM image sprawl consequences in enormous administration issues of VMs comprising the security patches [40].

5.12 VM checkpoint attacks

VM images are primarily online, and to patch these images, they will have to be started. This will add to the computation cost of cloud service provider. An attacker can approach VM checkpoint available in the disk that carries VM physical memory contents and can reveal delicate data of VM state [40].

As we saw in previous section, virtualization domain of cloud computing has a much greater attack surface than any other domain. Different types of cloud computing service models provide different levels of security services. Cloud users get the least amount of built in security with an Infrastructure as a Service provider, and the most with Software as a Service provider [2]. A comparative analysis of various techniques proposed by researchers to solve virtualization specific vulnerabilities in cloud computing environment is indicated in Table 2. Comparative analysis will help cloud users to identify what security mechanisms are required and mapping those mechanisms to controls that exist in their chosen cloud service provider. When cloud users identify missing security elements in the cloud, they can use that mapping to work to close the gap [2].

6 Virtualization security measures and requirements

The standard bodies in computing security have issued guidelines on security in cloud computing. These guidelines cover different aspects of virtualization security. National Institute of Standards and Technology (NIST) guide mentions security issues and recommendations for securing virtualization environment, whereas the Cloud Security Alliance (CSA) guide discuss security issues related to virtualization in the cloud and provide recommendations for secure virtualization environments [40]. European Network and Information Security Agency (ENISA) guide focuses on security measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, human resources and their management and vetting, hardware and software

Table 2 Comparative analysis of various techniques proposed by the researchers to solve virtualization specific vulnerabilities in cloud computing

Author	Virtualization specific security issues	Impact on cloud system	Counter-measures/possible solutions	The focus of the work	Limitations	Future work
Sabahi [66]	Virtualization, Data Leakage, Data Remanence	Exposure of Confidential Data	Hypervisor-based virtualization technology, VM Security Monitor, VM Reliability Monitor	Virtualization technology, Reduce the workload, Distributed security systems	More complexity	–
Lee and Yu [67]	Breaches due to software defects	Compromise of all guest VMs	Proposed a new Virtualization Introspection System (VIS) to detect, prevent the cloud ecosystem from potential malicious attacks and to protect the host as well as VMs	KVM-based Cloud Systems	Limited to protection based on established rules, have false positives and negatives, require more sophisticated analysis	Adopt a new analysis method, GK-trail, which would produce models in the form of an extended final state machine
MA and CD [68]	Advanced persistent attacks such as a stealthy rootkit, Trojan, DoS and DDoS attack	Disrupt the normal operation of cloud infrastructure	Hypervisor-based Intrusion Detection and Prevention System Open source Host-based Intrusion Detection System OSSEC	To detect real-time intrusions including stealthy self-hiding rootkits and DoS attack	–	VMI technique as Out-of-the-Box intrusion detection technique, to measure the efficiency of VMI based detection approach and to verify the detection as well as prevention capability of intrusion
Raina and Ng [69]	VM Sprawl, Security of Offline, Dormant, Pre-Configured and Active VMs, Resource Exhaustion, Hypervisor Security, Unauthorized Access to Hypervisor, Risk Due to Cloud Service Provider API	The risk to confidentiality, integrity, and availability VMs with unknown configurations can quickly proliferate, consuming resources and degrade overall system performance	- Enforces effective controls - Encrypt data stored on virtual and cloud servers - Develop policies to restrict storage of VM images and snapshots - Cryptographic checksum protection to detect unauthorized changes to VM images and snapshots	Identification and management of security risks specific to virtualization technologies	–	–

Table 2 continued

Author	Virtualization specific security issues	Impact on cloud system	Counter-measures/possible solutions	The focus of the work	Limitations	Future work
Kazim and Zhu [70]	The Hypervisor, virtual machines, and disk images	Occupy system resources, launch a DoS attack, leak sensitive data, provide attacker root access to the host machine	Proper configuration, Encrypting the VMsR, Hypersafe, Using encryption and hashing of VMs state, Encrypting the checkpoints, Enforcing policies	Virtualization security	–	–
Wang et al. [17]	Cross-VM Side Channel Attacks based on shared physical memory and exploits the vulnerabilities of balloon driver	Obtain sensitive information	–	Cross-VM Side-Channel Attacks	–	To transmit data by a novel side channel
Siddappa [71]	Security for the Virtual machines and their required resources	Sharing the logical resources and data security	Security supervisor	Challenges of virtualization security, vulnerabilities, the impact of virtualization on cloud services	–	The flexibility of including the latest technique and other solutions
Zhu et al. [3]	Virtualization security vulnerabilities in different VMMs documented by XSA, CVE, and NVD	Performance deterioration, service intervention, information leakage and control flow hijacking at the hypervisor level	By extending symbolic execution methods and designed a detection framework for virtualization platforms which can detect bugs in virtualization implementations	Analyses of the known vulnerabilities in KVM and Xen Differences between vulnerabilities in virtualization and traditional software vulnerabilities To analyze the characteristics of security vulnerabilities and develop a systematic approach to detect them accurately	Current bug finding tools can detect common flaws in software implementation. Many virtualization vulnerabilities can hardly be addressed by existing techniques	Conformity inspection of the virtual hardware Resource availability vulnerability detection based on the framework
Donaldson et al. [72]	Virtualization, VM escape, security of virtual machines	An attacker could potentially gain control of all the systems Allowing capricious code from the virtual OS to be run on the host system	By performing a penetration test to evaluate the security of virtualization systems	To test the security of a virtualized environment	Complexity, hardware limitations and wide attack surface of virtualization	To evaluate the effectiveness of the methodology for use in the penetration testing process

Table 2 continued

Author	Virtualization specific security issues	Impact on cloud system	Counter-measures/possible solutions	The focus of the work	Limitations	Future work
Dildar et al. [73]	Hypervisor attack	Allows the cybercriminal to possess the accessibility and authorization over the hypervisors The operating system files can be modified or removed by cybercriminals	Proposed the Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS)	To determine competent approaches for defending the hypervisor attacks in cloud computing	–	–
Mishra et al. [74]	Malicious network traffic in a cloud environment	Spoofing attacks, VM attacks	Proposed a robust and learning based security approach Malicious Network Packet Detection (MNPD)	To detect network intrusions in the cloud	It cannot detect those unseen attacks which exhibit very different behavior than learned attack patterns	To provide an extended framework for doing the detailed investigation of attacks by performing memory introspection at VMM of VM hosted servers

redundancy, strong authentication, efficient role-based access control and federated identity management [41].

Virtualization security is the concerted measures, procedures, and processes that assure the conservation of a virtualization environment. It addresses the security issues encountered by the elements of a virtualization infrastructure and procedures through which it can be alleviated or stopped [42]. Virtualization security is a wide conception that comprises a number of different techniques to assess, implement, monitor and administer security within a virtualization environment. Typically, virtualization security may comprise processes such as:

- Execution of security controls and procedures granularly at each VM.
- Securing VMs, virtual network and other virtual appliance with attacks and vulnerabilities surfaced from the underlying physical device.
- Assuring control and authority over each VM.
- Formation and execution of security policy across the environment

In order to protect the virtualization environment in the cloud, the authority must implement definite security measures. The following measures must be endorsed for a secure cloud execution [40].

- Protected network
- Deactivating the non-essential features
- Detach unutilized hardware devices
- Backup of VM images
- Hardened configurations
- Patch management
- Solidifying of VMs
- Auditing

7 Cloud shared responsibility model

Cloud always comes as a shared responsibility model between a cloud service provider and cloud customers using this service [43]. Cloud service customers must know how the cloud will impact their privacy, security, and compliance. Cloud service customers must understand how their cloud service provider delivers a secure solution. Cloud service customers must consider their new role in cloud security. Some cloud service customers mistakenly believe that when they migrate to the cloud, their cloud security responsibilities also shift. As shown in Fig. 5, the shared responsibility model is a method for determining which roles cloud service providers and cloud service customers play in cloud security.

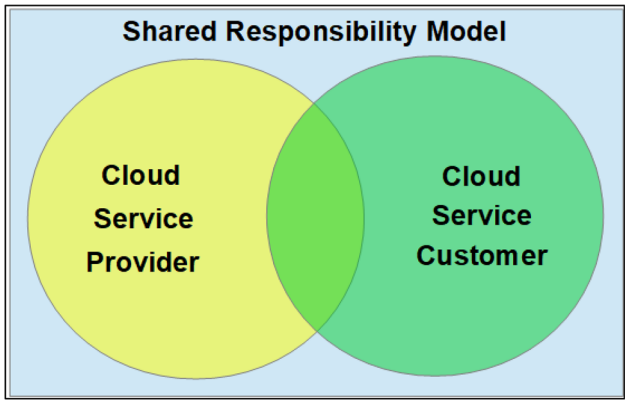

Fig. 5 Cloud shared responsibility model

The shared responsibility model outlines that providers are responsible for security of the cloud, and customers are responsible for security in the cloud [24]. Cloud service providers and customers must work together to meet overall objectives of the cloud security.

When an enterprise runs and manages its own IT infrastructure on premises, within its own data center, it is responsible for the security of that infrastructure, as well as the applications and data that run on it. When an organization moves to a public cloud computing model, it hands off some, but not all, of these IT security responsibilities to its cloud provider. Each party, the cloud service provider and cloud user is accountable for different aspects of security and must work together to meet cloud security objectives [44].

Microsoft Azure's guidance on the shared responsibility model states, "The importance of understanding this shared responsibility model is essential for customers who are moving to the cloud. Cloud service providers offer considerable advantages for security and compliance efforts, but these advantages do not absolve the customer from protecting their users, applications, and service offerings." Cloud users' responsibilities generally increase as they move from SaaS to PaaS to IaaS. In IaaS, the cloud service provider supplies and is responsible for securing basic - cloud infrastructure components, such as virtual machines, disks and networks. IaaS users, on the other hand, are generally responsible for the security of the operating system and software stack required to run their applications, as well as their data [44]. Cloud consumers must always ensure the security of the endpoints that are used to access cloud services. In the IaaS model, the cloud user is responsible for network security and, if necessary, communication encryption.

With PaaS and SaaS, this accountability is transferred from the cloud consumer to the provider, since the provider has the appropriate security technologies in place. The cloud service provider must ensure the physical security of the cloud system [45]. A schematic is shown in Table 3 highlighting the various functional components exposed in the IaaS delivery model in cloud computing.

The key to understanding where to place security mechanisms is to understand where physically in the cloud resources are deployed and consumed, what those resources are, who manages the resources, and what mechanisms are used to control them. Those factors help us gauge where systems are located and what areas of compliance we need to build into our system [2]. Table 4 lists the different service models and lists the parties responsible for security in the different instances.

Basically, cloud computing furnishes a break-up of a cloud user's roles and responsibilities from those of a cloud service provider's. By subscribing a particular service delivery model, a cloud user implicitly agrees to relinquish certain level of access to and control over resources [46]. Out of the three models, IaaS supplies nearly all acquiescence to a cloud user. This model presents opportunities for customizing operating procedures with the ability to on-demand provision IT infrastructure delivered by virtual machines in cloud.

8 Conclusion and future research

Virtualization involves the use of an encapsulating software layer (Hypervisor or Virtual Machine Monitor) which surrounds or underlies an operating system and provides the same inputs, outputs, and behavior that would be expected from an actual physical device. As virtual machine is not dependent on the state of the physical hardware, multiple virtual machines may be installed on a single set of hardware. The decoupling of physical and logical states gives virtualization inherent security benefits. Virtualization maps the virtual machines (VMs) to physical resources but poses security concerns as users relinquish physical possession of their computation and data.

Each different type of cloud service delivery model creates a security boundary at which the cloud service provider's responsibilities end and the cloud customer's responsibilities begin. Any security mechanism below the security boundary must be built into the system, and any security mechanism above must be maintained by the cloud customer. Virtualized systems introduce important security gaps that need to be taken into account when deploying strong and secure virtualized infrastructure. The multi-tenant nature of virtualized systems must be appropriately managed to provide strong isolation between tenants operations. Cloud virtualization environment can be compromised by different attacks at hypervisor, virtual machines and VM images. We have identified attack scenarios at these components and different existing security schemes that provide security to virtualization

Table 3 Cloud security responsibilities of cloud service provider and cloud service customer at IaaS delivery model

Responsibility	At IaaS delivery model	
Data governance		CSC
Endpoints		CSC
User access management		CSC
Identity infrastructure		CSC
Network and firewall configuration		CSC
Data/communication encryption and data integrity authentication		CSC
Network traffic protection		CSC
Operating system security		CSC
Software stack		CSC
Middleware, applications, interfaces and data		CSC
Access control and activity monitoring		CSC
Virtual network, virtual machines		
Governance, and compliance requirements	CSP	CSC
Network controls and network interfaces	CSP	CSC
Hosts	CSP	
Facilities and data center	CSP	
Physical security of data center	CSP	
Processing and memory		
Hypervisors, servers, data storage and networking	CSP	
Physical security of the cloud service	CSP	
Disaster and Incident response	CSP	

CSP cloud service provider, *CSC* cloud service customer

Table 4 Security responsibilities by service model

Model type	Infrastructure security management	Infrastructure owner
Public	CSP	CSP
Private/community	CSC	CSC
Private/community	CSC	CSP
Private/community	CSP	CSC
Private/community	CSP	CSP
Hybrid	CSP and CSC	CSP and CSC

environment. In order to keep the cloud secure, a security mechanism must be designed to detect, prevent or recover from such security threats.

This paper has analyzed the critical threats that exist in a cloud environment from both the cloud service providers' and customers' perspectives that should be taken care off while buying or delivering services in cloud for ensuring high level of security towards leading or derivable attacks. This paper provides a basis to understand issues related to virtualization security. We provide a security attack statistics and its impact on the virtualization environment. We present a variety of security concerns associated with virtualization components. Our taxonomy of cloud-based attacks on the virtualized systems supports practitioners at an early stage of the design of mitigation mechanisms by identifying relevant attacks which threaten their VMs. We perform a comprehensive comparative analysis on various techniques proposed by research analysts to solve virtualization specific vulnerabilities in cloud computing environment. These security issues must be addressed exhaustively for the widespread acceptance of cloud computing paradigm. We discussed virtualization security measures and requirements to be taken to achieve secure virtualization implementations. Furthermore, we examined cloud shared responsibility model to determine which roles cloud service providers and cloud service customers play in cloud security. Lack of understanding of the break-up of responsibilities in our view often results in wrong beliefs of what cloud computing can or cannot deliver.

In summary, the paper has analyzed various vulnerabilities leading to threats and has provided taxonomy of various attacks possible on cloud with possible defensive solutions. The article will assist both academia and industry to understand the challenges on security over a cloud

environment and the ways to solve them for secure cloud services in the near future. Our future work will be concerned to detect and mitigate potential security threats targeting customers' VMs in cloud computing and to protect customers' virtual machines in the IaaS delivery model.

Acknowledgements We would like to thank the anonymous reviewers for their valuable feedback and constructive suggestions which have helped to improve the quality and presentation of this article. We also express our gratitude to Dr. O P Vyas for initiating the early discussions on virtualization security issues which led in part towards the completion of this work. Finally, we are also thankful to Dr. Vipul K Dabhi and Dr. Savita Gandhi for their continuous support and encouragements throughout the preparation of this article.

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):17:1–17:39. https://doi.org/10.1145/2431211.2431216
5. Asad S, Fatima M, Saeed A, Raza I (2017) Multilevel classification of security concerns in cloud computing. Appl Comput Inf 13(1):57–65. https://doi.org/10.1016/j.aci.2016.03.001
6. Granneman (2012) Virtualization vulnerabilities and virtualization security threats. https://searchcloudsecurity.techtarget.com/tip/Virtualization-vulnerabilities-and-virtualization-security-threats
7. Sempolinski P, Thain D (2010) A comparison and critique of Eucalyptus, OpenNebula and Nimbus. https://doi.org/10.1109/CloudCom.2010.42
8. Nagar N, Suman U (2016) Analyzing virtualization vulnerabilities and design a secure cloud environment to prevent from XSS attack. Int J Cloud Appl Comput 6(1):1–14. https://doi.org/10.4018/IJCAC.2016010101
9. Kaur A, Gupta G, Bhathal GS (2017) Role of virtualization in cloud computing. Global J Eng Sci Res 4(7):143–150. https://doi.org/10.5281/zenodo.835421
10. 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
11. Zhang Y, Juels A, Oprea A, Reiter M (2011) Homealone: Co-residency 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
12. Wojtkowiak A (2012) Protection for virtual environments ? IBM Virtual Server Protection. IBM Corporation
13. 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
14. 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
15. 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
16. 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/10.1007/978-3-319-25988-8
17. Wang Z, Yang R, Fu X, Du X, Luo B (2016) A shared memory based cross-VM side channel attacks in IaaS cloud. In: 2016 IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp 181–86. http://ieeexplore.ieee.org/document/7562068/
18. Hussain SA, Fatima M, Saeed A, Raza I, Shahzad RK (2017) Multilevel classification of security concerns in cloud computing. Appl Comput Inform 13(1):57–65. https://doi.org/10.1016/j.aci.2016.03.001
19. Zhang T (2017) Detection and mitigation of security threats in cloud computing. PhD Thesis, Electrical Engineering Department, Princeton University, Princeton, NJ, p 257. Retrieved from http://palms.ee.princeton.edu/node/479
20. Jiang Wu, Zhou Lei, Shengbo Chen, Wenfeng Shen, (2017) An Access Control Model for Preventing Virtual Machine Escape Attack. Future Internet 9 (2):20. https://doi.org/10.3390/fi9020020
21. Geeta CM et al. (2018) Data auditing and security in cloud computing: issues, challenges and future directions. Int J Comput (IJC) 28(1):8–57.
22. Dubey S, Verma K, Rizvi MA, Ahmad K (2018) SWOT Analysis of Cloud Computing Environment. In: Aggarwal V, Bhatnagar V, Mishra D (eds) Big Data Analytics. Advances in Intelligent Systems and Computing, vol 654. Springer, Singapore. https://doi.org/10.1007/978-981-10-6620-7_71
23. Zhang T, Lee RB (2018) Design, implementation and verification of cloud architecture for monitoring a virtual machine's security health. IEEE Trans Comput 67(6):799–815. https://doi.org/10.1109/tc.2017.2780823
24. Ravi Kumar P, Herbert Raj P, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Proc Comput Sci 125:691-697. ISSN: 1877-0509. https://doi.org/10.1016/j.procs.2017.12.089
25. 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
26. Rouse (2016) What is virtualization? Definition from WhatIs.com. Retrieved from https://searchservervirtualization.techtarget.com/definition/virtualization
27. Zhu SY, Hill R, Trovati M (2015) Guide to security assurance for cloud computing, computer communications and networks book series (CCN). Springer International Publishing, ISBN: 978-3-319-25986-4, 978-3-319-25988-8
28. Gonzalez N, Miers C, Redígolo F et al (2012) J Cloud Comp 1:11. https://doi.org/10.1186/2192-113X-1-11
29. Kabir MH, Islam S, Hossain S (2015) A detail overview of cloud computing with its opportunities and obstacles in developing countries. Int J Eng Sci Invent 4(4):52–63
30. Rouse (2015) What is hypervisor attack? Definition from WhatIs.com. https://whatis.techtarget.com/definition/hypervisor-attack. Accessed 10 Mar 2018
31. Adla, Vishrutha (2013) Comparing performance of HyperV 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

32. From Wikipedia, the free encyclopedia (2017) Hyperjacking—wikipedia. https://en.wikipedia.org/wiki?curid=45523767. Accessed 17 May 2018
33. 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
34. Hyde D (2009) A survey on the security of virtual machines. A project report written under the guidance of Prof. Raj Jain. https://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/. Accessed 11 Nov 2017
35. Zhu SY, Hill R, Trovati M (2015) Guide to security assurance for cloud computing. Springer, Switzerland. https://doi.org/10.1007/978-3-319-25988-8
36. Xiong H, Zheng Q, Zhang X, Yao D (2013) CloudSafe: securing data processing within vulnerable virtualization environments in the cloud. In: 2013 IEEE conference on communications and network security (CNS), National Harbor, MD, 2013, pp 172–180. https://doi.org/10.1109/cns.2013.6682705
37. Schwarzkopf R, Schmidt M, Strack C, Freisleben B (2011) Checking running and dormant virtual machines for the necessity of security updates in cloud environments. In: 2011 IEEE third international conference on cloud computing technology and science, Athens, pp 239–246. https://doi.org/10.1109/cloudcom.2011.40
38. Schwarzkopf R, Schmidt M, Strack C, Martin S, Freisleben B (2012) Increasing virtual machine security in cloud environments. J Cloud Comp (2012) 1:12. https://doi.org/10.1186/2192-113X-1-12
39. Himanshu (2017) Technology redefine: footprinting [Blog post]. https://technologyredefine.blogspot.com/2017/09/footprinting_17.html. Accessed 23 Jan2018
40. 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/10.1007/978-3-319-25988-8
41. Catteddu D (2010) Cloud computing: benefits, risks and recommendations for information security, In: Serrão C, Aguilera Díaz V, Cerullo F (eds) Web Application Security. IBWAS 2009. Communications in Computer and Information Science, vol 72. Springer, Berlin, Heidelberg, pp 17–17. https://doi.org/10.1007/978-3-642-16120-9_9
42. What is Virtualization Security? Definition from Techopedia. https://www.techopedia.com/definition/30243/virtualization-security. Accessed 23 Mar 2018
43. Jeena R, Kumar SS, Sudhan SKHH (2014) Efficient and secure techniques for protecting data in the cloud. In: International conference on information communication and embedded systems (ICICES2014), Chennai, 2014, pp 1–5. https://doi.org/10.1109/icices.2014.7033771
44. Rouse (2017) What is shared responsibility model? Definition from WhatIs.com. https://searchcloudcomputing.techtarget.com/definition/shared-responsibility-model. Accessed 14 April 2018
45. Gresser (2017) Who is responsible for cloud security? https://securityintelligence.com/who-is-responsible-for-cloud-security/. Accessed 24 Jan 2018
46. YungChou (2010) Cloud Computing Primer for IT Pros—Yung Chou on Hybrid Cloud. https://blogs.technet.microsoft.com/yungchou/2010/11/15/cloud-computing-primer-for-it-pros/. Accessed 15 Nov 2017
47. McCune JM, Li Y, Qu N, Zhou Z, Datta A, Gligor V, Perrig A (2010). TrustVisor: efficient TCB reduction and attestation. In IEEE symposium on security and privacy, Berkeley/Oakland, CA, pp 143–158. https://doi.org/10.1109/SP.2010.17
48. Vasudevan A, Chaki S, Jia L, McCune J, Newsome J, Datta A (2013) Design, implementation and verification of an extensible and modular hypervisor framework. In: IEEE symposium on security and privacy, Berkeley, CA, pp. 430–444. https://doi.org/10.1109/SP.2013.36
49. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-low integrity. In: IEEE symposium on security and privacy, 380–395. https://doi.org/10.1109/SP.2010.30
50. Azab AM, Ning P, Wang Z, Jiang X, Zhang X, Skalsky NC (2010) HyperSentry: enabling stealthy in-context measurement of hypervisor integrity. In: ACM conference on computer and communications security, 38–49. https://doi.org/10.1145/1866307.1866313
51. Butt S, Lagar-Cavilla HA, Srivastava A, Ganapathy V (2012) Self-service cloud computing. In: ACM conference on computer and communications security, ACM, New York, NY, USA, 253–264. https://doi.org/10.1145/2382196.2382226
52. Keller E, Szefer J, Rexford J, Lee RB (2010) NoHype: virtualized cloud infrastructure without the virtualization. In: ACM international symposium on computer architecture, ACM, New York, NY, USA, 350–361. https://doi.org/10.1145/1815961.1816010
53. Szefer J, Keller E, Lee R, Rexford J (2011) Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM conference on computer and communications security, Chicago. ACM, pp 401–412. https://doi.org/10.1145/2046707.2046754
54. Ye X et al (2016) An anomalous behavior detection model in cloud computing. In: Tsinghua Science and Technology 21(3):322–332. https://doi.org/10.1109/TST.2016.7488743
55. Szefer J, Keller E, Lee R, Rexford J (2011) Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM conference on computer and communications security, Chicago. ACM, pp 401–412. https://doi.org/10.1145/2046707.2046754
56. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-low integrity. In: IEEE symposium on security and privacy, pp 380–395. https://doi.org/10.1109/SP.2010.30
57. Jiang X, Wang X, Xu D (2007) Stealthy malware detection through VMM-based out-of-the-box semantic view reconstruction. In: ACM conference on computer and communications security, ACM, New York, NY, USA, 128–138. https://doi.org/10.1145/1315245.1315262
58. Payne BD, Carbone M, Sharif M, Lee W (2008) Lares: an architecture for secure active monitoring using virtualization. In: IEEE symposium on security and privacy, Oakland, CA, pp. 233–247. https://doi.org/10.1109/SP.2008.24
59. Azmandian F, Moffie M, Alshawabkeh M, Dy J, Aslam J, Kaeli D (2011) Virtual machine monitor-based lightweight intrusion detection. ACM SIGOPS Oper Syst Rev 45(2): 38–53. https://doi.org/10.1145/2007183.2007189
60. Sailer R, Jaeger T, Valdez E, Caceres R, Perez R, Berger S, Griffin J, van Doorn L (2005) Building a MAC-based security architecture for the Xen open-source hypervisor. In: Annual computer security applications conference (ACSAC), Washington, DC 859, pp 10–285. https://doi.org/10.1109/CSAC.2005.13
61. Afoulki Z, Rouzaud-Cornabas J (2011) A security-aware scheduler for virtual machines on IAAS clouds. Technical Report RR-2011-08, LIFO, ENSI de Bourges. http://www.univ-orleans.fr/lifo/prodsci/rapports/RR/RR2011/RR-2011-08.pdf. Accessed 4 June 2018
62. Rueda S, Sreenivasan Y, Jaeger T (2008) Flexible security configuration for virtual machines. In: Proceedings of the 2nd ACM workshop on computer security architectures, New York. ACM, pp 35–44. https://doi.org/10.1145/1456508.1456515

63. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing security of virtual machine images in a cloud environment. In: ACM workshop on cloud computing security (CCSW '09). ACM, New York, NY, USA, 91–96. https://doi.org/10.1145/1655008.1655021
64. Gofman M, Luo R, Yang P, Gopalan K (2011) Sparc: a security and privacy aware virtual machinecheckpointing mechanism. In: Proceedings of the 10th annual ACM workshop on privacy in the electronic society, Chicago. ACM, pp 115–124. https://doi.org/10.1145/2046556.2046571
65. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing security of virtual machine images in a cloud environment. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago. ACM, pp 91–96. https://doi.org/10.1145/1655008.1655021
66. Sabahi F (2012) Secure virtualization for cloud environment using hypervisor-based technology. Int J Mach Learn Comput 2(1):39–45. https://doi.org/10.7763/IJMLC.2012.V2.87
67. Lee S, Yu F (2014) Securing KVM-based cloud systems via virtualization introspection. In: Proceedings of the annual Hawaii international conference on system sciences, pp 5028–5037. https://doi.org/10.1109/HICSS.2014.617
68. Ajay Kumara MA, Jaidhar CD (2015) Hypervisor and virtual machine dependent intrusion detection and prevention system for virtualized cloud environment. In: 2015 international conference on telematics and future generation networks, TAFGEN 2015, pp 28–33. https://doi.org/10.1109/TAFGEN.2015.7289570
69. Cloud Security Alliance (2015) Best practices for mitigating risks in virtualized environments, pp 1–35. https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf. Accessed 19 May 2018
70. Kazim M, Zhu SY (2018) 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. pp 51–63. https://doi.org/10.1007/978-3-319-25988-8
71. Kumar NLU, Siddappa M (2016) Ensuring security for virtualization in cloud services. In: International Conference on Electrical, Electronics, Communication. Computer and Optimization Techniques (ICEECCOT), Mysuru, pp. 248–251. https://doi.org/10.1109/ICEECCOT.2016.7955224
72. Donaldson S, Coull N, Mcluskie D (2018) A methodology for testing virtualisation security. In: International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), London, pp. 1–8. https://doi.org/10.1109/CyberSA.2017.8073397
73. DIldar MS, Khan N, Abdullah JB, Khan AS (2017) Effective way to defend the hypervisor attacks in cloud computing. In: 2017 2nd international conference on anti-cyber crimes, ICACC 2017, pp 154–59. https://doi.org/10.1109/Anti-Cybercrime.2017.7905282
74. Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Out-VM monitoring for malicious network packet detection in cloud. ISEA Asia Security and Privacy (ISEASP), Surat, pp 1–10. https://doi.org/10.1109/ISEASP.2017.7976995