ISSN (Print): 0974-6846
ISSN (Online): 0974-5645
Indian Journal of Science and Technology, *Vol 12(3), DOI: 10.17485/ijst/2019/v12i3/139557, January 2019*

A Taxonomy of Virtualization Security Issues in Cloud Computing Environments

Nadiah M. Almutairy[1], Khalil H. A. Al-Shqeerat[1] and Husam Ahmed Al Hamad[2]

[1]Department of Computer Science, Qassim University, Saudi Arabia;
nm.almutairy@qu.edu.sa, kh.alshqeerat@qu.edu.sa
[2]Department of Computer Science, Amman Arab University, Jordan; hhamad@aau.edu.jo

Abstract

Objectives: To identify the main challenges and security issues of virtualization in cloud computing environments. It reviews the alleviation techniques for improving the security of cloud virtualization systems. **Methods/ Statistical Analysis:** Virtualization is a fundamental technology for cloud computing, and for this reason, any cloud vulnerabilities and threats affect virtualization. In this study, the systematic literature review is performed to find out the vulnerabilities and risks of virtualization in cloud computing and to identify threats, and attacks result from those vulnerabilities. Furthermore, we discover and analyze the effective mitigation techniques that are used to protect, secure, and manage virtualization environments. **Findings:** Thirty vulnerabilities are identified, explained, and classified into six proposed classes. Furthermore, fifteen main virtualization threats and attacks are defined according to exploited vulnerabilities in a cloud environment. **Application/Improvements:** A set of common mitigation solutions are recognized and discovered to alleviate the virtualization security risks. These reviewed techniques are analyzed and evaluated according to five specified security criteria.

Keywords: Challenges, Cloud Computing, Security, Taxonomy, Virtualization

1. Introduction

Cloud computing has been developed to enable the Information Technology world for utilizing computer resources efficiently and more proficiently[1]. The cloud users have an advantage of unlimited computing power available on demand, in which they can access and pay for services when need it. Users will be able to accomplish computing services without the need for any significant investment in information technology infrastructure[2]. Cloud computing is an efficient way to increase the capacity dynamic scalability or add capabilities using virtualization resources, platform, infrastructure and software as service that can be accessed over the internet[3]. To improve the utilization of cloud resources we use Virtual Machines (VMs). The virtual machine is a virtual computer similar to a physical computer in which application or operating system can be installed and run[4].

Virtualization is an innovative technology, which is significantly expanding in the Information Technology industry. It provides multiple logical resources on a single server. Various benefits that can be provided by the virtualization are hardware utilization, resources protection, remote access, and other resources[5]. 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.

Two significant benefits that can be provided by a virtual machine are resources sharing and isolation[6]. Traditionally, the physical machine dedicates available resources permanently to all applications that are running on the computer, and this may cause waste in some resources such as memory and storage space. Whereas, in the virtual environment, resources are shared among numerous VMs and entirely used on demand. Isolation means failure in any VM will not affect the performance

or efficiency of other VMs running on the same host. The virtual environment enables VM to isolate data from other VMs, i.e., a program runs in one VM cannot see programs that are running on other VMs.

Virtualization is used to match the customers' requirements for security, control, economy, scaling, speed, and so forth. It may affect the choice of cloud service provider. Furthermore, it empowers the cloud users to start up and shut down their resources rapidly, which can be in some applications has its advantage[7].

1.1 Virtualization Architecture

Virtualization architecture is a model, which determines the interrelationships among particular virtual components, such as an operating system, network resources, servers, and storage spaces. In general, the virtualization is based on a hypervisor. The hypervisor isolates operating systems and applications from system hardware, whereas the host can run multiple Virtual Machines (VM) as guests that sharing the physical resources of the system, such as processors, memory, network bandwidth, and so forth. Virtualization architecture might be divided into two types, hosted and bare-metal architectures as shown in Figure 1.

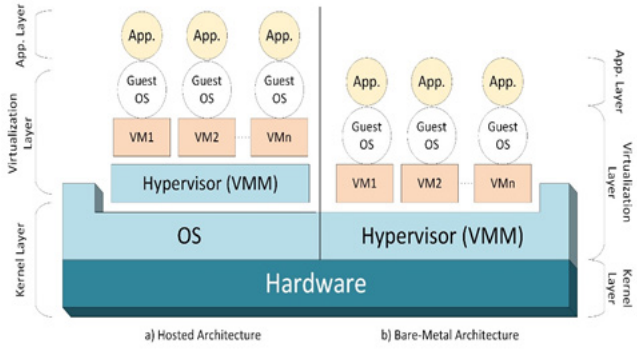

Figure 1. Hosted vs. bare-metal architecture.

In hosted architecture, first, an essential Operating System (OS) is installed on the host system, and then a hypervisor or VM monitor software is installed on the top of OS. This OS-based architecture entirely enables the user to control multiple guests OSs, or VMs installed on the hardware. Hosted virtualization architecture is substantially less complex to implement, and it is more useful for software development, running legacy applications, and supporting different operating systems. However, it has some severe disadvantages due to controlling the virtual machines by operating system directly[8]. 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 able to damage the virtual machines later. In the second architecture, the hypervisor runs directly on the host hardware. Like hosted architecture, VMs and higher layer applications are installed above the hypervisor.

The cloud-computing environment can be virtualized on every layer of cloud computing services, such as IaaS resources including virtualized storage, networking, and servers, or virtualized datasets, and development environments in PaaS, and any software application instances. The rapid expanding of cloud computing and virtualization technology make cloud infrastructure more complicated and have brought a series of security threats. This study aims to identify the main challenges and security issues of virtualization in cloud computing environments. Furthermore, it reviews the alleviation techniques for improving the security of cloud virtualization systems. The rest of the paper is organized as follows. The method used in this study is presented in the next section. The third section presents an overview of the security challenges and vulnerabilities. Then, we review the security threats and attacks on the virtual environment. Finally, some solutions and techniques proposed in the literature review to alleviate potential threats and attacks are discussed.

2. Methodology

A Systematic Literature Review (SLR) is performed to provide comprehensive summary of existing literature relevant to a research since it helps in collecting research evidence from current relevant studies. In SLR, we try to have as many researches as possible that answer our research questions and help us achieve objectives of the study.

2.1 Terminology

In this section, the main terms are defined and adopted as follows:

Challenge: something new, difficult, or complex, which requires great effort by user to determine and solve it.

Vulnerability: an occurrence of weakness in operation, in software, and in the infrastructure that can be

exploited by a party to perform malicious actions. The vulnerability can also be in the existence of an error in design or implementation that can cause unexpected, undesirable actions.

Risk: the potential that the vulnerability is exploited to cause a threat as well as the effect resulting from this serious event on the organization.

Threat: any circumstance or action that exploit one or more vulnerabilities to harm the assets.

Attack: an assault on the security of the system from a deep threat; which is an attempt to alter, expose, steal, destroy, disable or get unauthorized access to assets.

2.2 Research Questions

The research questions are the major core of a systematic literature review. In order to get existing studies, the following research questions have been formulated:

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?

3. Results and Discussion

In this step, we search for relevant work that satisfies the certain criteria. When we started to research, we made a great effort due to the wide scope of our research questions. After several trials, the search strategy was agreed upon. The keywords that are used during the research: challenge, vulnerability, risk, threat, attack, approach, solution, and framework. To be more precise, we used the virtualization term with keywords.

As we sometimes used AND or OR to be more accurate results, we used the keywords in the different databases such as ACM Digital Library, EBSCO, Google Scholar, IEEE Xplore, ISI Web of Science, ProQuest, ScienceDirect, Scopus, Springer Link, and Wiley Online. We did not restrict the results of the search based on publication year because we want to be as inclusive as possible. Therefore, for each database, we used the default settings for the start year of publication. Table 1 shows the number of results for each sources. We got 53324 of results after the search operation. After we remove based on title we had 35275 of results.

Table 1. Results before and after removal

Sources	The number of result	After removal
ACM Digital Library	6052	5224
EBSCO	2500	1489
Google Scholar	2000	1271
IEEE Xplore	20100	18248
ISI Web of Science	541	99
ProQuest	1171	700
ScienceDirect	5738	1865
Scopus	3051	1158
Springer Link	8771	3428
Wiley Online	3400	1793
Total	53324	35275

The important step in the process of selection a study is to identify exclusion and inclusion criteria. Studies that were excluded:

- None English research.
- That indicates to very specific and limited domain.
- That do not relate to virtualization security issues in cloud computing.
- That do not relate to mitigate the security issues of virtualization
- That is discussing cloud without relating it to virtualization security issues.
- That is discussing cloud without point to mitigation of security issues of virtualization.
- That is editorial papers prepared for special issues.
- We included all the studies that:
- Discuss virtualization vulnerabilities, risks, threats, or attacks in cloud computing environment.
- Propose the appropriate security techniques to mitigate the virtualization security issues.

The steps of the selection process are described below:

1. By using a SQL query, 21389 of results were discarded based on some keywords, such as storage security, management, VLAN, trust, industry, digital, E-Commerce, E-learning, mobile, and VM backup.
2. By reading the title, the abstract, and sometimes the conclusion of the remaining 13886 papers, we discarded 13486 papers.
3. By reading 400 of results completely, we left with 148 of results.

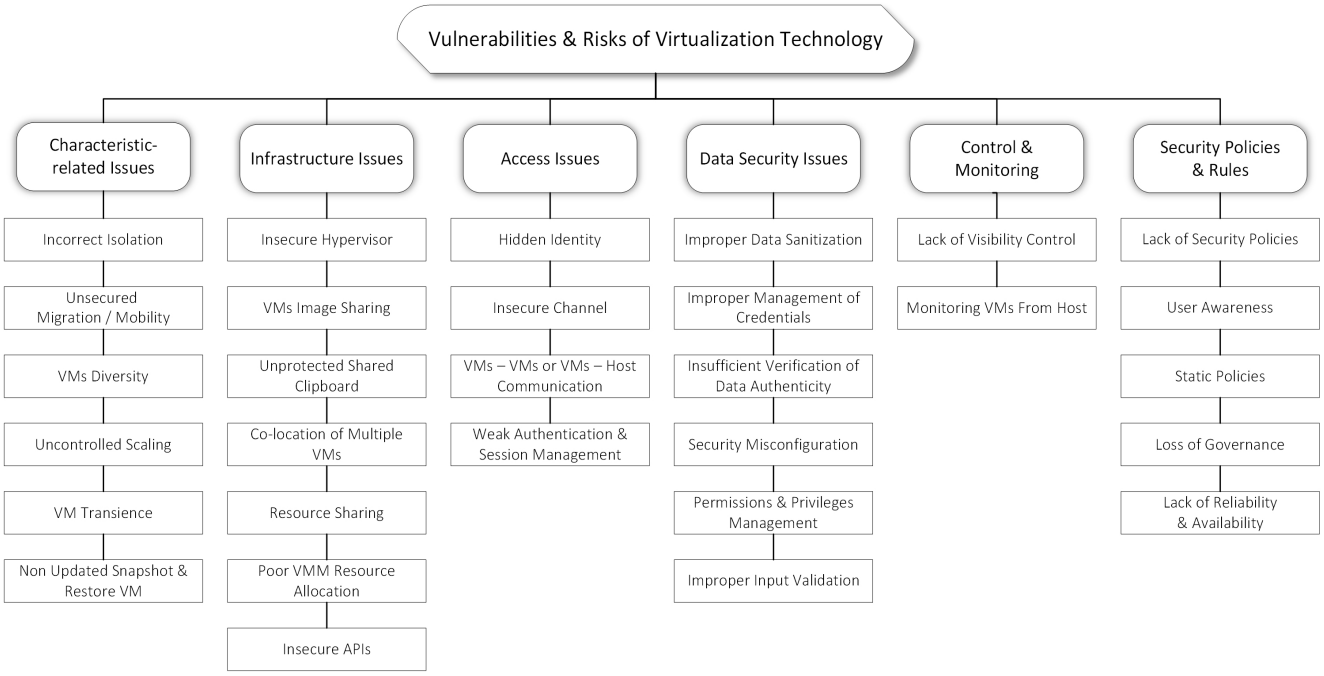

Figure 2. Security vulnerabilities and risks categories.

4. Taxonomy of Virtualization Challenges

Many vulnerabilities and risks are existing in current virtualization technologies that an attacker can exploit to penetrate the security and privacy systems in cloud computing environments. In this study, we have classified vulnerabilities into several categories regarding their characteristics and relevance to virtualization technology. Figure 2 shows these defined categories and its vulnerabilities and risks.

4.1 Virtualization Characteristic-Related Issues

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

Incorrect VM Isolation (VC1): The hypervisor is responsible for ensuring isolation between the different VMs[9]. The isolation between virtual machines prevents the VM from direct access to others' virtual disks, applications, or memory on the same host[10]. Isolation of virtual machine limits the scope of the attack. Furthermore, isolation of virtual machine makes more difficult for the attacker accessing resources and access unauthorized data on the physical machine[11]. Each VM is isolated from each other virtualized machines and its host physical system[12], so if one VM is break-down, it does not affect any of the other VMs on the same host. A violation of the isolation principal happens when the attacker uses a compromised VM for communicating with other VMs on the same host (Unauthorized communication). Moreover, violation of the isolation principal occurs when one VM affects other VMs located on the same host[13]. Therefore, a shared environment requires an accurate configuration for maintaining strong isolation.

Unsecured VM Migration/Mobility (VC2): Migration technique is one of many advantages of Virtualization. It enables the application to be transparently transmission from one host machine to another

without halting the virtual machine[14]. After migration, the application continues in execution without any loss of progress. VM migration is done by transmitting the application along with its VM's entire system state, including memory, the state of CPU, and sometimes disk too, to the destination host. VM migration offers many valuable advantages such as load balancing, and conserves energy.

Moreover, the migration of virtual machines is useful in case of hardware failure. It migrates the VM to another execution host and performs maintenance or repair operations on the source execution host[15]. Although migration technology introduced many advantages, it raises some security issues. Live migration is relatively a new term where its security issue is yet to be discussed. It is potential that the attacker may passively steal and snoop or actively modify confidential information during migration. Therefore, the transmission channel has to be protected and secured against different passive and active attacks.

VM Diversity (VC3): Many IT enterprises overcome the problem of security by enforcing homogeneity, as all devices must have the latest patching software. Virtualization can facilitate more efficient usage models that get the benefit of implementing older or unpatched versions of the software. This solution causes a set of challenges such as the need to maintain patches or provide other protection for different operating systems in addition to addressing the risk posed by the presence of many unpatched or old devices on the network[16].

Uncontrolled Scaling (VC4): Virtualization technology allows the creation of new virtual machines easily and quickly on demand. Scalability provides a very cost-effective way to handle business expansion and any additional resources of the server requirements. Users can have several particular purpose virtual machines, for example, for testing or viewing purposes. The growth in the number of VMs depends on the available space on the host. Generally, the scalability of cloud facilities gives greater availability[17]. The number of VMs can overgrow, and this makes management tasks more exacerbated, where all machines must be scanned, and patched for vulnerabilities[18].

VM Transience (VC5): In the physical computing environment, users have one or more devices that run online most of the time and are in a stable state. In contrast, VMs in a virtualized environment can come and go from the network intermittently[19] (i.e., it is never in a stable state).

If the computer is online most of the time, then it is more vulnerable to be attacked, since the offline server cannot be accessed. By enabling users to start and stop virtual machines remotely, attackers have no enough time in preparation for attacking the VM. Although VM transience limits the chance in which attackers can exploit for compromising the system, it makes security audits and maintenance more challenging because machines must be online when scanned or patched. Compromised VMs can infect other vulnerable machines and can go offline before detection.

Non-updated Snapshot & Restore VM (VC6): The ability of a virtual machine to recover from an error to a previously defined state is often considered a security benefit for restoring a guest VM to a pre-attack state. Most VMs pick a snapshot of the virtual disk content on a time interval or when changes are made[20]. Although the system can be restored smoothly and quickly, some security issues appear through a rollback system. If the VM restored to a compromised or unpatched state, this leads to exploit old vulnerabilities until updating state in the next cycle. Furthermore, the rollback can re-enable the security credentials that were previously disabled. The most severe risk through Rollback could reveal stream ciphers that were used for encryption and an attacker could easily acquire the original plaintext. So critical information is compromised, and if it is not detected, every encrypted data from this point on will not be safe[21].

4.2 Infrastructure Issues

The Infrastructure of virtualization includes any hardware and software components required to support virtualization purposes. Much vulnerability may arise from virtualization infrastructure.

Insecure Hypervisor (I1): Utilizing the hypervisor or virtual machine manager (VMM) to support many VMs on a single physical machine has become popular recently. It increases hardware usage and provides flexibility in system management. The hypervisor provides an abstraction layer to separate VMs from the physical hardware and isolates them from each other. It controls all aspects of the underlying VMs, including communicating with each other. This communication never goes to the real network[22]. On the other hand, the hypervisor must support a strong security base for VMs. If it is not secure, the attacker can gain control over the hypervisor and compromise any VMs running on it. Furthermore,

if an attacker exploits the vulnerable hypervisor, he can control the hypervisor, and get access to or redirect sensitive data[23].

VMs Image Sharing (I2): A VM image is a pre-packaged software template that contains the configuration files that are used to create VMs. The VM images provide an easy way for deploying and restoring virtual systems efficiently and quickly across numerous of physical servers[24]. Sharing VM images is commonly used in some environments of cloud computing as a quick method to get started. Users of cloud computing can create their VM image from scratch or can make utilization of existing images in the shared repository. For example, Amazon introduces a public image repository where legitimate customers can upload or download a VM image[25]. Although of these benefits or advantages, VM image introduces some risks that in turn effect on the security of the cloud computing. Therefore, the integrity of these images is an essential security requirement for services provided by cloud computing.

Unprotected Shared Clipboard (I3): A shared clipboard is a feature that allows data to be transferred among VMs on one side and between VMs and host on the other. The host can monitor the traffic between the underlying VMs because the network packets that come from or go to a virtual machine pass over the host. However, it may cause the hacked host to compromise all VMs operating on it. It can serve as a gateway to attack the system. Moreover, unprotected shared clipboard allows exchanging data between the cooperating malicious programs in VMs[26].

Co-location of Multiple VMs (I4): Co-location of multiple VMs is a presence of multiple VMs on the same host that share resources in order to ensure improved efficiency, flexibility, and thus reduced the operational cost[27]. Co-location of multiple VMs on a single server increases the surface of potential attack and the risk of VM-to-hypervisor or VM-to-VM.

Resource Sharing (I5): Cloud service providers need Virtualization technology to deliver their services in a scalable manner when sharing infrastructure, platforms, and applications. Although the ability to share hardware resources of one physical device among multiple isolated VMs to optimize hardware used and save cost, it may cause security vulnerabilities to the virtual environment. Sharing resources such as CPU, memory, storage space among VMs, may result in unauthorized communication between guests VMs[28]. In general, sharing resources reduces the security of connected VMs because an infected VM can access other VMs through resources they share. Organizations with permission to access the infrastructure can control the infrastructure or view other data[29], For example, the cloud services provider has different instances for each user but uses the same application code. Moreover, data of different customers will be loaded on the same database server, which leads to data leakage among these tenants[30], giving the attackers opportunity for hijacking user credentials, controlling and eavesdropping information of other users[31].

Poor VMM Resource Allocation (I6): The physical layer interacts with the virtual layer through the hypervisor or VMM, which allocates required resources to each VM on demand. The VM must be restricted to specific isolation. The VMM is responsible for preventing VMs from requesting more resources whereas the VM is missing its reserved resources[32]. Poor VMM resource allocation allows a VM to use resources that are not within its allocated resources, thus preventing the other VMs from using their resources, in some cases, this leads to denial of service.

Insecure APIs (I7): A cloud-computing provider provides infrastructure, software, and platform services to the users and enables them to access and manage services by the published Application Programming Interfaces (APIs) via Internet[33]. APIs may impose a variety of security issues such as improper authorizations, clear-text authentication, or data discovery during transmission, which affect the availability and security of the cloud services[34]. An attacker could use APIs to undermine the confidentiality and integrity of customers' data. He uses the token that used by customers to get access to the service through API for manipulating their data.

4.3 Access and Communication Security Issues

The user interaction with the cloud begins when he attempts to access cloud services. The user must first authenticate his identity before accessing cloud services. The communication process arises when the user and the cloud exchange data or services.

Furthermore, there are communications between VMs within the cloud that introduce vulnerabilities that may affect the host machine and all VMs running on it. An illegal user can exploit access and communication vulnerabilities related to access and communication security.

Hidden Identity (AC1): In physical computing environments, there is usually a custom identity correlated to a physical device such as MAC addresses, or device ID. It is used to differentiate between devices and determine who the owner of a machine is. This static method is not effective in virtual environments due to creating VMs dynamically or mobility of VMs that make it very difficult to identify or track the owner of a VM running on a particular physical host[35].

Insecure Channel (AC2): The cloud service providers use the Internet as a communication infrastructure to provide services to customers or transfer their data. An efficient and secure transmission channel is a critical component in a cloud environment and forms the basis for managing information and any related processes[36]. When transmitting the data from users to the cloud environment, the data must be sent using an encrypted secure transmission channel such as SSL/TLS. It protects network traffic against a potential interception attack.

VMs-VMs or VMs-Host Communications (AC3): In a cloud-computing environment, communication mechanisms in virtual networks are similar to those used in real networks. In the same way that physical devices are connected, virtual machines are connected and built on a network infrastructure of the host to connect to the public network[37]. VMs need to communicate and share data. If the connection does not meet critical security standards, they become a target for attacks. The virtual network uses virtual switches or bridges that connect the virtual network interface cards to the physical network interface card of the host machine to exchange data[38]. However, the virtual network traffics are visible for all VMs that share the same physical data-link, which potentially leads to security risk.

Weak Authentication and Session Management (AC4): Authentication is a mechanism used to determine whether something or someone is what or who it is declared to be. Authentication techniques protect the system against bad actors that masquerade as legitimate users, developers, or operator to read, delete, and modify data. In a virtual environment, the authentication mechanism applies to end users and to components of the system. Most of the widely utilized authentication methods are poor and may affect access and control policy. Sometimes, it is easy to break some authentication mechanisms that have weakness in their design, such as one-factor authentication mechanisms, to get access to the system[39].

4.4 Data Security Issues

The significant challenge in data security is how to share sensitive data in a virtual insecure environment-Data Security concerns about data protection from intentional modification by an unauthorized person.

Improper Data Sanitization (D1): Elasticity and resource pooling features allow a set of resources to be allocated to different users later. When the user accesses a memory service or storage space, he can recover data from another user who previously used the same storage space[40,41]. Sanitization is a method to clean or destroy data from a storage resource when it is available for other users[42]. In the public cloud, sometimes the data must be deleted entirely at the request of the client, including the log files and backup replicas prepared for recovery[43,44].

The data destruction might be complicated because many replicas of data can be distributed in many locations. Thus, it is difficult to guarantee a service provider can remove all copies of the backup[45]. Data sanitization is a significant task to discard appropriately physical resources and data that are sent to the trash. Improper data sanitization may expose the data to the risk, for example, may lead to data loss or data disclosure since hard disk may be disposed of without being wiped entirely or may not be destroyed due to continued use of other tenants[46].

Improper Management of Credentials (D2): Organizations need user credentials to control and allow the user to access his sensitive data. The deployment of the credential management system is an essential way to manage user credentials. Improper management of credentials indicates to weaknesses in the way used to manage the credentials such as lack of enforcement or verification of password strength[47]. This vulnerability is exacerbated in Virtualized environments that share unprotected transport channels, which may increase the number of actors who can sniff credentials during transmission.

Insufficient Verification of Data Authenticity (D3): If the system fails to verify the validity or origin of the data, it may accept invalid data. Lack of data authenticity might arise in different situations. It includes the poor design and implementation, such as the improper chosen of data-authenticity mechanisms, improperly verifying the signatures, cross-site request forgery, and improper or missing verification of integrity[47].

Security Misconfiguration (D4): Virtual systems often rely on many interoperating software components

that must be dynamically configured to support virtualization in many applications. The security configuration is vital for providing security to customers. Misconfiguration can compromise the security of users, applications, and the entire system. It arises when security settings are defined and maintained as a default setting[39]. The impact of virtualization vulnerabilities increases when a security configuration fails, mainly if the behavior of the virtual component depends on another component.

Permissions and Privileges Management (D5): Authentication mechanisms are used to verify the user identity and to enable the authorization policy. Thus, authorization policies are implemented using security measures to grant or deny access to resources. Improper permissions and privileges management refers to failure in privileges management, permissions, and other security features used for enforcing access control. In particular, it incorporates issues caused by implementing without the required privileges or assigning an incorrect privilege, dropping or reducing errors and preserved or insecure inherited permissions[44]. In virtualized environments, the complex nature of the privileges and the multiplicity of the layers of administrative required for a virtualized environment lead to emphasize this weakness, mainly when thinking about its dynamics, and scenarios where federations and migrations are in place.

Improper Input Validation (D6): It means the system does not check user input or fails to validate input. Therefore, the system may be exposed to and accept malicious input, which may cause the system to execute arbitrary code, or modify control flow[47].

4.5 Control and Monitoring

In a traditional network environment, the physical machines use the specific port on the monitored switch for connecting to the network. In a virtual environment, the deployment of the vast VMs can be appended to the same physical port on the network.

The communication between these virtual machines never goes through the physical port, i.e., they can communicate with each other, as they are part of one single virtual switch. The nature of the virtualization environment introduces some vulnerability that can be exploited by the attackers such as lack of visibility and monitoring VMs from the host.

Lack of Visibility (C1): The hypervisor is responsible for establishing communication between VMs located on the same host. Therefore, physical network security mechanisms, like network-based intrusion detection and prevention systems, cannot monitor the inter-VM traffic[24], because the traffic over a virtualized environment never goes through the physical network. This issue becomes a significant challenge as malicious activities of the VMs bypass the security monitoring tools. Some hypervisors enable network monitoring their capabilities not as strong as those in tools utilized to monitor the environment of the physical networks[17].

Monitoring VMs from the host (C2): The most significant issue is to secure the host rather than monitoring each VM individually, as long as the control point in the virtual environment is the host device. Inter-VMs traffic passes through the host, which manages these VMs. A breach of the host may lead to compromise all VMs running on it[48].

4.6 Security Policies and Rules

Security policies refer to the plans, practices, and rules that must be well defined, comprehensive, and clear for regulating access to the system or for addressing constraints on functions of the system and flow between them. Any vulnerability in these policies leads to different threats.

Lack of Security Policies (P1): It is needed to develop virtualization security policies, where virtual machine deployment, management, migration, and shutdown requirements are established securely. The lack of security policies may cause some vulnerability that lead to an unsafe environment for the host device, virtual machines, and virtual administration tools.

User Awareness (P2): Cloud service users are the weakest point in any information security because cloud service providers do not check the surrounding of their customers. Suspicious user accounts can give attackers an opportunity to do any malicious work without being identified. Furthermore, there are attack vectors for various social engineering that an attacker might use to trick a victim into entering a malicious site, and then gain access to the user's computer. From this point, it can monitor user actions and view the same data as the user sees and can steal user credentials to authenticate the cloud service itself. Security awareness is a security concern that is often overlooked[49]. The misuse of open cloud services by users often allows an attacker to access the system, so users should learn about different potential attacks and

how to avoid them to ensure that users understand and assume their responsibilities.

Static Policies (P3): VMs can be moved between physical environments as needed to get additional resources. Accordingly, baseline security policies of VMs must be transferred as they move from one environment to another. If the security policy of the VM does not conform to the new environment, VM becomes vulnerable[50]. Furthermore, when the VM moves, it loses its performance history and must re-evaluate its baselines.

Loss of Governance (P4): The cloud provider is responsible for data security while handling and storing it. Rules or policies must be clear between the cloud provider and individuals or enterprises. In many cases, the client essentially gives up control to the cloud service provider on many security-related issues, but sometimes the service providers themselves may not be trusted[51]. Furthermore, they unaware of any security or control mechanisms specified by the cloud provider[52]. The loss of control and governance can have a significant impact on the organization's strategy and consequently affect the ability to fulfill its mission and objectives. The loss of governance and control can also lead to a lack of data availability, integrity, and confidentiality[8]. Reducing processing and data storage costs is an essential requirement for any company, whereas data analysis always is a mandatory task for decision-making. Therefore, companies will not transfer their data to the cloud environment until they trust the security procedures by service providers.

Lack of Reliability and Availability of Service (P5): Reliability issues in virtualization can affect cloud performance. Collecting many VMs may cause performance problems[3]. Some challenges like limited CPU or I/O bottlenecks lead to performance problems. These problems occur more in virtualization environment more than in the traditional environment due to connecting the physical server to many VMs that compete to access critical resources. IT organizations should be able to monitor the usage of VMs and physical servers in real time. This capability avoids overuse of server resources and reallocates resources according to given business requirements[53].

5. Security Threats and Attacks

This section identifies common threats and potential attacks of virtualization security by performing a systematic literature survey.

VM Hoping/Guest jumping: An attacker is maliciously getting access to different virtual machines belonging to other customers[54]. He can monitor the target VM's resource utilization, and affect VM's integrity, availability, and confidentiality[55].

Malicious Insider: A malicious insider intentionally misuses the authorized access in a manner that negatively affects information systems[56,57].

Malicious VM image: A user may use a VM image that contains malicious code to create own VM. This image makes the entire system vulnerable to attack[58].

VM escape: An attacker gets access to the hypervisor and escapes from its control[59]. An infected VM can completely bypass the isolation between the VMs and the host[60]. Consequently, can get privileges to access the resources shared, with other VMs[61].

Hyper-jacking/VM-based Rootkit: Hyper-jacking attack inserts VM-based root kits to control the entire virtual environment[62].

Virtual memory Leak: A system failure may occur between the allocation and deallocation of the shared memory area in the hypervisor, which may lead to virtual memory leaks[63].

Theft-of-Service: Use cloud services or resources for a long time without being registered in a billing cycle or at the expense of another user[64,65].

VM sprawl/VM Spawl: Increase the number of VMs continuously, while some of them are in idle state, this may lead to waste the resources in the host machine[66].

VM poaching: It occurs when malicious VM exhausts resources and completely consumes the hypervisor against other VMs running in the same host[67].

Accounting, Service, and Traffic Hijacking: It occurs when the attacker gets access to users credential and becomes able to spy on their transactions, manipulate data, return falsified information and redirect them to illegal sites[68,69].

Cross-VM: It occurs when a malicious VM bypasses virtual isolation between VMs to attack other VMs in the same host[70]. It could exploit vulnerabilities in the OS guest or hypervisor to obtain confidential leakage data from other VMs through the side-channel attack[71,72].

Co-location/Co-resident: Unlike cross-VM attack, the attacker has a clear target VM and aims to co-locate own VM with victim VM on the same physical host. With co-residence, the attacker constructs covert side channels to obtain sensitive information from the victim[73].

Foot-printing: It occurs when an attacker intelligently collects information indicate to vulnerabilities of a victim platform operates in a virtualized environment. This information might be used to carry outmalicious activities on the system[74].

VM rollback attack: The attacker exploits the suspend/resume feature in a virtualized environment to attack VMs[75]. When the hypervisor suspends a victim VM at any points and makes a snapshot of its state, the attacker triggers a pre-defined infected snapshot to the VM at resume time. As a result of missing some security updates, an attacker could bypass certain security checks in the VM to achieve the attack target[76].

Data leakage/Data loss: Data leakage occurs when sensitive information falls into the wrong hands when it is audited, stored, processed, or even transmitted[77]. While Data loss occurs when data is lost due to loss of encryption key, accidental deletion, or natural disaster[78]. Table 2 shows security threats and correlates them with their exploited vulnerabilities in cloud computing environments.

Table 2. Mapping between threats and vulnerabilities

Threat	Vul.
VM Hoping/Guest jumping	I1, I3, I4, I5, VC1, VC2
Malicious Insider	P1, P4
Malicious VM image	I2
VM escape	VC1, VC2, I1, I4, I6, C1, C2, D4, D6
Hyper-jacking/VM-based rootkit	I1, I2, I3, AC3, VC2
Virtual memory leak	D1, I6
Theft-of-service attack	P4, D4, I1
VM sprawl/VM Spawl	VC2, VC3, VC4, I2, P4
VM poaching	I6
Accounting, service and traffic hijacking	D2, P4, P1, AC4, I7
Cross-VM attack	VC1, VC2, I1, I4, I5, I7, D1, D4
Co-location/Co-resident attacks	I4, VC1
Foot-printing attack	AC2
VM rollback attack	VC2, VC6, P1
Data leakage/Data loss	D1, P4, D5, AC4, P5, P1, I6, I1, I5, I7, AC3

6. Virtualization Security Solutions

Many types of research offer solutions in virtualization security. These solutions may be useful for centers and organizations interested in developing cloud security solutions and standards. In this section, we focus on some solutions covered in the literature survey. HyperSafe[61] is an approach proposed to provide control-flow integrity for the Type-I bare-metal hypervisors. This approach relies on two techniques. The first one protects code integrity of hypervisor by preventing memory pages from being manipulated at execution time. Authors have used Write Protect bit (WP bit) to check how the supervisor code acts with write-protection bits in page tables. The write-protection is skipped if the WP is off, otherwise, it is decided if the supervisor can write or not to the memory page. In order to allow the good updates to proceed, the WP bit is temporarily cleared right before each update and then re-enabled immediately after the update.

The other techniques protect control data by converting them into restricted pointer indexes. It extends the protection provided by the first technique from code integrity to control-flow integrity to prevent attacker form controlling the flow of the system. HyperSafe aggregates control data into target tables and then replaces them with a restricted pointer index.

A VM security monitoring model based on memory introspection has been proposed[79]. Security of host or VM can be recognized by using a hardware-based approach to obtain real-time physical memory of the host. Moreover, a VM Control Structure (VMCS) based approach is proposed for VM memory forensics. Based on the results of memory forensics of host/VM malicious behavior can be detected. These techniques were used to develop a prototype of a VM defense system that is called VEDefender, which incorporates a PCI device and a terminal program. The VEDefender prototype was implemented on top of kernel-based VM (KVM).

VEDefender is transparent to the guest machines, and it is hard to be accessed even from a compromised VM. It can gather and analyze data for discovering any malicious activity whether being on the host or guest machine. Experiments results show that the proposed system can deal with virtual machines from different OS versions and has an acceptable execution time.Authors[80] leveraged the nested virtualization to propose an in-the-box way for monitoring the hypervisor - In-Hypervisor Memory

Introspection (IHMI). In the proposed architecture, Hypervisor Address Space and the Monitor Address Space are separated from each other, and Virtualization Exception (VE) handler operates between them. In order to protect and isolate the monitor from the untrusted hypervisor, a protected address space is used. The hypervisor and the monitor are isolated from one another through Extended Page Table (EPT). The memory content of the hypervisor is protected by setting it non-writable to the hypervisor, and any attempt to modify it will generate an EPT violation or VE, which means that the hypervisor's execution is suspended. The hypervisor and monitor memory isolation is achieved using a unidirectional mapping, which allows the monitor to have access to the hypervisor's memory while forbidding the reverse. By using VMFUNC instruction, the switch between the hypervisor and the monitor can be performed without involving the nested hypervisor, which leads to improved performance. For secure context switching between the hypervisor and the monitor, the VE handler is non-writable for the hypervisor. To disable the untrusted hypervisor's influence, the checker disables interrupts and uses a new stack, and checks the VE information area.

HyperSentry[81] is a framework allows stealthy and in-context integrity measurement of the running hypervisor or other highest privileged software. Taking advantage of the Intelligent Platform Management Interface (IPMI) an out-of-band communication channel is used to trigger the System Management Interrupt (SMI), which triggers the HyperSentry for integrity measurement. When an SMI occurs, the current CPU state is saved, and the context is switched to the System Management Mode (SMM). HyperSentry constitutes of two components: the SMI handler and the Measurement Agent. Trust on the SMI handler is obtained during the boot when its code is copied to the SMRAM, and then the SMRAM is locked to prevent from access or modification. When a request for integrity measurement is received, HyperSentry requires the access to the hypervisor's code, data and CPU state needed for measurement.

Unlike many works that try to protect the Virtual Machine Monitor (VMM) from malicious VMs attacks, an approach proposed to protect VMs from a compromised VMM. CloudVisor[82] is a transparent prototype system that resides below a commodity VMM leveraging the hardware-assisted (nested) virtualization.

It protects the privacy and integrity of VMs owned resources (such as CPU, memory and I/O device), by still letting the VMM allocate and manage resources for VMs. CloudVisor interposes interactions in-between the guest VMs and VMM through a clearly defined entry and exit points. Differently, from traditional virtualization systems that have a composite TCB including VMM and management tools that are more prone to attacks, CloudVisor excludes them from TCB. With CloudVisor all accesses that are not from VM itself only can view encrypted VM's data. CloudVisor architecture is organized in such a way that VMM is still responsible for resource management, VM construction and destruction, and scheduling, but it is monitored transparently by CloudVisor to ensure the protection and isolation. In the nested virtualization scheme, host mode runs CloudVisor, while in guest mode runs VMM and guest VMs. To secure control transition, CloudVisor keeps a VM control structure for each VM, by which it controls what kind of instruction or events lead to a VM exit. To protect memory, it uses a two-step address translation, using page table and EPT. Among others, CloudVisor provides memory isolation, tracking memory ownership, legal memory accesses, handling data exchange with I/O storage, disk I/O privacy and integrity.

Secure MMU[83] and HyperWall[84] also separate the memory resources management from the security protection, but with no need of a nested hypervisor. Secure MMU is a hardware-based mechanism aims to isolate and protect the guest VMs memory from other VMs that share the same physical system and even from an untrusted hypervisor. Secure MMU makes a separation so that the hypervisor still performs resource management but with limitations. A hardware controller is used to update the page mapping and set a pointer to the nested page table. TCB of the proposed approach contains only the hardware system, excluding the hypervisor.

Hardware-assisted secure virtual machine[85] (H-SVM) is an extension of Secure MMU. It is hardware-based virtual machine isolation and protection that intends to minimize the architectural changes that support virtualization. Direct updates of page tables by hypervisor are blocked by H-SVM to ensure memory isolation. All changes that a hypervisor needs to make in nested tables are made by requesting to H-SVM. H-SVM protects the integrity and confidentiality of guest VMs, excluding the availability.

HyperWall is a hardware-based architecture developed to support hypervisor-secure virtualization. Even though the hypervisor is not trusted, HyperWall still allows it to

manage the platform resources freely. According to customer requirements/specifications, the guest VM's are protected by Confidentiality and Integrity Protection (CIP) tables from hypervisor or DMA access. Furthermore, this architecture allows the server to verify the provided hardware protections to the cloud customer and cleans the VM's memory and state in case of termination.

CIP tables protect VM memory, which includes mapping of access rights for the hypervisor and DMA to the memory pages. Even if a page is not protected, thus, it allows access to the hypervisor and DMA; it is assigned to a VM so that the compromised hypervisor cannot assign it to another VM. Whenever a new VM is created, terminated or there is a change in the memory assigned to a VM, the CIP tables are updated. CIP tables are stored in a portion of DRAM not accessible to any software. Physical memory used by VM during runtime, physical to machine memory mapping tables and the protection specified by users (pre-CIP data) also are protected. Encryption keys are used for customer verification, to protect the processor state of a VM when it is terminated, and for external communication. The HyperWall prevents VM rollback attack by disabling some functionalities of the hypervisor such as suspend/resume function.

As compared to HyperWall, a solution to protect from VM rollback attack has been proposed[75], while keeping the virtualization functions such as VM suspend/resume and VM migration. This goal is achieved by logging all VM rollback activities, and then the user can audit the log and examine suspicious rollbacks. This solution requires minimal user interaction, and it is based on the CloudVisor. A NoHype[86] architecture has been introduced for removing the virtualization layer. It prepares a more secure virtualization layer by minimizing its size or securing it with additional hardware. In the NoHype architecture, each processor core is allocated to run just one VM. It means guest VMs cannot share processor cores, which eliminate the need for the hypervisor. The number of VMs is limited to the number of processor cores, while the memory is partitioned between the VMs. Thus, each guest OS can access a dedicated physical memory on a host. Every guest OS can access its assigned physical device directly at a given time.

Unlike HyperWall, H-SVM, NoHype, HyperCoffer[76] can protect against physical attacks. Hardware and Software frameworks aim to provide integrity and privacy for VMs by trusting only the processor chip. External memory or devices are considered untrusted by the HyperCoffer, so it requires memory encryption and integrity checking. Due to low overhead, HyperCoffer uses address-independent seed encryption[87] (AISE) for encrypting memory, and Bonsai Merkle Tree (BMT) for checking integrity, in addition to VM-Table for multiplexing. VM-Table contains the VMID, which is the unique index of a VM. It is stored in a portion of the physical memory of CPU that is accessible only to the processor. Logging and auditing are used by HyperCoffer to secure against VM rollback attack. Since every time the processor installs or resumes a VM, the hash of a vector containing some necessary information for AISE and BMT is added to a chain in a nonvolatile register, which can be audited from the user. In the meantime, the memory snapshot image is encrypted and protected by BTM, which is encrypted further by an encryption key assigned to a VM during runtime.

The proposed framework[14] called secure live virtual machine migration (SLVM). This framework aims to protect against network intrusions, viruses, attacks and preserves the integrity and the confidentiality of migration data. SLVM has two modules: Common Security modules that apply to both the host VM and the Guest VMs underlying this host and Individual/Per VM security module that is specified separately the security requirements for each virtual machine running over the host.

To protect the virtual machine migration process from data tampering by a Man-in-the-Middle (MitM) and time-of-check-to-time-of-use (TOCTTOU) problem, a two-level security framework[88] has been proposed. After selecting a VM for migration to reduce power consumption in a cloud environment, a destination host needs to be selected for that VM. The second task is more complicated because it can create a situation that the destination host cannot fulfill the VMs requested resources. To secure the system from TOCTTOU, Authors have proposed to use a token system. Before the request for available resources in the network is made, the node first asks for the token. If the token is not already in use, then it can broadcast its request.

The components of CoM framework[38] are virtual machine migration agent (VMMA), security context migration agent (SCMA), and live migration controller (LMC). Five steps are used to perform the migration. First, The VMMA allocates resources at the hypervisor where VM is going to migrate. In step 2, The VMMA copies VM's pages in an incremental way whereas SC set of migrated VM is transferred by the SCMA.

In the third step, VM stop working on the source hypervisor. Then the VMMA copies remanding memory pages and the CPU state to destination hypervisor. The destination SEs will receive the changed SC set at the source. Finally, the migrated VM continues in execution on the destination host. Trusted cloud computing platform[89] (TCCP) provides a closed box execution environment. It ensures a confidential execution for guest VMs. TCCP guaranties that the privileged administrator of the cloud provider cannot investigate or tamper with the customer's VM. Furthermore, it provides an attestation feature to the user, so that the users before launching their VM they can know if the IaaS service is secure or not. To achieve this, the TCCP should enforce a security perimeter and restrict the VM execution inside it. If the admin remotely logs to a VM, he cannot have access to VMs memory.

The TCCP extends the concepts of the trusted platform to a whole IaaS backend service. The TCCP trusted computing base is composed of two parts: a trusted VMM (TVMM), and a trusted coordinator (TC). Each node in the cluster runs a TVMM to host customer's VMs. The TC manages the set of trusted nodes that are placed inside the security perimeter and run the TVMM.VNSS[90] is a framework that aims to ensure distinct security level requirement for VMs as well as full lifecycle protection for VMs. The framework is composed of security sandbox controller (SSC), security policies create an agent (SPCA), virtual machine creates agent (VMCA), virtual machine migration agent (VMMA), security context migration agent (SCMA) and security policies migration agent (SPMA). SSC maintains the schedule of all these agents. During VM creation, the SCC calls the VMCA which will create an instance of the virtual machine, and then the SPMA that will generate security policies for the VM. Initially, SSC triggers VMMA, SCMA, and SPMA upon VM migration. VMMA is responsible for moving the VM instance, while SCMA synchronizes the security context of VM, and then SPMA resumes security policies of VM on the destination host.

sHype[91] is a secure hypervisor architecture which controls information flow between different operating systems that share the same hardware platform. It provides mechanisms that control resource sharing since resource sharing is inevitable in distributed services. The mandatory security controls implemented by the hypervisor are the isolation of VMs and resource sharing among them. sHype implements a secure reference monitor interface to enforce constraints on the information flow between VMs. In the sHype access control architecture, the reference monitor is implemented by enforcement hooks, which get access decisions from the access control module (ACM). ACM defines and applies access rules based on the formal security policy.

Another work to provide strong isolation between numerous of VMs is a Second level VMM[92] (SeVMM). SeVMM aims to control the sharing resources and provides isolation between VMs. Moreover, it manages and controls the virtual resources such as virtual processor by intercepting the entire security-related calls among guest and host operating system. SeVMM supports a different of security policies such as the CW, BLP, TE, to guarantee the integrity of the inter-domain data flow and the system. Flask framework is used to configure security strategy in SeVMM. It is composed of three modules to achieve objectives. The first module is the Security Policy Management module, which manages the whole security policies and protects the modification and update of security policy in the third module. When the resource is initialized, the security attribute is allocated according to the security policy in this module. The second module is a Safety Hook module responsible for controlling access to the shared virtual resources by gaining some information about VMs such as types of operations and attributes of virtual resources and then transfer this information into the third module.

The third one is a Security Policy Enforcement module, which takes a decision based on the security policy and information given by hook.Researchers[54] proposed a scheme for securing the inter-VM communication traffic by limiting the access to the critical resources. The controlling and analyzing inter-VM traffic are done via an addition frame tag through an agent to the payload of the packet. It aims to recognize sending the application in a communication within the same tenant. Virtual Firewall architecture (V-firewall)[8] aims to protect and inspect the inter-communication of VMs to protect against potential attacks in the internal and external networks. In addition to protection against flooding and spoofing attacks. In this architecture, V-firewall is installed on the hypervisor whereas Agent is on guest OS. The gent is used to monitor outbound and inbound traffic to VM and send logs to V-firewall to decide grant or deny traffic according to security policies.

Hypervisor-based virtualization technology[3] aims to secure the cloud environment. It adds some reliability/

security monitoring units: VM security monitor (VSEM), VM reliability monitor (VREM) which are in the VM level. Two monitoring units also are added in the hypervisor level, hypervisor security monitor (HSEM) and hypervisor reliability monitor (HREM). There are VSEM and VREM units within each running VM. VSEM monitors the VM behavior and sends a report to HSEM. VREM monitors some parameters that are related to the reliability such as the workload. It sends useful information to the HREM and gives a resource to VM according to its state. HREM detects the attacks overflow depending on the requests and then notifies HSEM about it. A Virtual Machine Introspection[93] (VMI) Based Architecture takes advantage of virtual machine monitor (VMM) technology for establishing intrusion detection systems. It allows good visibility of the monitored host's state, while still maintaining strong isolation between the monitored host and the IDS because it resides "outside" of the host it monitors.

Virtual Machine Monitor provides isolation of IDS from the monitored host in the VMI IDS architecture. VMM provides a communication interface between itself and VMI IDS, which allows the later one to send inspection, monitor, and administrative commands. VMwall[94] is presented for inspecting the Internet traffic. VMwall is a tamper-resistant application-oriented firewall that takes advantage of application-level firewalls and isolation provided by the virtual machine. Isolation of application-level firewall is achieved by placing it in a trusted VM, which depends on the hypervisor to restrict the attack between trusted VM and malicious VM. VMwall uses VM introspection to detect another VMs process connected to a suspected network. It depends on the requirement to find the head of linked data structures, correct order in addition to the length of data structure fields, so the attacker cannot alter them.

VMwall provides a tamper-resistant, independent and lightweight verification architecture using VM isolation and VMI. The design VMwall has two major components: a kernel module and a user agent. The kernel component intercepts all incoming or outgoing guest VMs network packets and applies per-packet policy provided from the user agent to decide whether to allow or drop every packet. On interception process, if a firewall rule for the packet exists on its rule table, it acts depending on that rule to allow or drop the packet. Otherwise, it calls the user agent to create a rule for it. Until the user agent provides the rule, the kernel module queues the incoming packets. Then, the rest of the packets from that connection are handled depending on that rule. The user agent obtains the policy by introspecting the processes executing on the guest VM and assessing the legitimacy of such processes. First, it attempts to identify the sending/receiving VM depending on the packet's source/destination IP, and then finds the process bounded to the source/destination port.

If the user agent does not find a process (in its whitelist) bounded to the port, it will block the connection. Otherwise, it will allow the connection. To overcome the theft-of-service attack against cloud services, an external API[66] has been proposed for calculating the power consumptions of VM at different times while the user is using the VM. This API will detect and prevent theft-of-service attack depending on the statistics of power consumptions of a VM. The API is stored on an external cloud so that the API's integrity can be maintained in case the cloud that hosts VMs is compromised during the attack. The API computes the power consumption of VM's processes by adding the measured power consumption at different intervals of time. Later, API can compare the calculated VM's power consumption from this API with the calculated power consumption from the internal cloud. In case that there is a difference, the API can notify the administrator about this, or the user can be charged depending on the external calculated power consumption.

6.1 Comparison of Mitigation Techniques

The reviewed mitigation techniques and solutions, in the previous section, are compared in this study based on the following five criteria:

1. Data Confidentiality: any solutions encrypt the data in transit, disk, or memory satisfy the data encryption criterion.
2. Data Integrity: any solutions protect VM data from being altered satisfy the integrity criterion. In addition, any solutions compute the hash of data in transit satisfy this criterion. Solutions that maintain the integrity of the hypervisor code satisfy this criterion.
3. Securing the Hypervisor: any solutions protect the code of hypervisor or detect the malicious activity in hypervisor satisfy the securing hypervisor criterion.
4. Securing the VM: any solutions present mechanisms to secure VM satisfy securing VM criterion.
5. Control access: solutions that imposed policies to access the resources.

Table 3 summarizes the comparison between the reviewed solutions mitigation techniques and the specified security criteria.

Table 3. Comparison of the mitigation techniques

Solutions	Security Criteria				
	Data Confidentiality	Data Integrity	Securing the hypervisor	Securing the VM	Control access
HyperSafe		√	√		
VEDefender			√	√	
IHMI		√	√		
HyperSentry			√		√
NoHype			√		√
CloudVisor	√	√		√	
Secure MMU	√	√		√	
H-SVM	√	√		√	
HyperWall	√	√		√	
HyperCoffer	√	√		√	
SLVM	√	√		√	
A two-level framework				√	
CoM framework				√	
TCCP	√	√		√	
VNSS				√	
sHype					√
SeVMM					√
Securing inter-VM traffic				√	
V-firewall				√	
VMI				√	
VMwall				√	

7. Conclusion

The rapid expanding of cloud computing and virtualization technology make cloud infrastructure more complicated and have brought a series of security challenges. This research has identified critical security issues of virtualization technology in cloud computing environments. The collective security vulnerabilities and risks have been classified into several categories according to their effect on virtual environments. Furthermore, security threats and virtual-based attacks have been presented according to virtualization uses of the vulnerabilities and security risks. In this study, we have reviewed some solutions and alleviation techniques suggested in the literature review for improving the security of cloud virtualization systems. Finally, these reviewed mitigation techniques are compared according to five specified security criteria; data confidentiality, data integrity, securing the hypervisor, securing the VM, and access control.

8. References

1. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011; 34(1):1–11. https://doi.org/10.1016/j.jnca.2010.07.006.
2. Al-Shqeerat K, Al-Shrouf F, Hassan M, Fajraoui H. Cloud computing security challenges in higher educational institutions- A survey. International Journal of Computer Applications. 2017; 161(6):22–9. https://doi.org/10.5120/ijca2017913217.
3. Sabahi F. Secure virtualization for cloud environment using hypervisor-based technology. International Journal of Machine Learning and Computing. 2012; 2(1):39–45. https://doi.org/10.7763/IJMLC.2012.V2.87.

4. A taxonomy and survey of cloud computing systems. Available from: https://ieeexplore.ieee.org/document/5331755.
5. Chatzikyriakidis I. Trends and risks in Virtualization. Kingston University London. 2011. p. 1–97.
6. Virtual machine security guidelines; 2017. Available from: https://www.cisecurity.org/wpcontent/uploads/2017/04/CIS_VM_Benchmark_v1.0.pdf.
7. Demystifying the cloud: Important opportunities, crucial choices. Global Netoptex Incorporated; 2009. p. 4–14.
8. Haeberlen T, Dupré L. Cloud computing: benefits, risks and recommendations for information security. European Network and Information Security Agency; 2016. p. 1–50.
9. Bulusu S, Sudia K. A study on cloud computing security challenges. Blekinge Institute of Technology. 2012. p. 1–137.
10. Infrastructure as a Service Security: Challenges and Solutions. Available from:
11. A survey on the security of virtual machines. Available from: http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec/
12. Birje M. Security issues and countermeasures in cloud computing. International Journal of Applied Engineering Research. 2015; 10(86):71–5.
13. Wu H, Ding Y, Winer C, Yao L. Network security for virtual machine in cloud computing. 5th International Conference on Computer Sciences and Convergence Information Technology; 2010. p. 1–4.
14. Anala M, Shetty J, Shobha G. A framework for secure live migration of virtual machines. International Conference on Advances in Computing, Communications and Informatics; 2013. p. 243–8. https://doi.org/10.1109/ICACCI.2013.6637178.
15. Schwarzkopf R. Virtual machine lifecycle management in grid and cloud computing. University of Marburg; 2015. p. 1–349.
16. Garfinkel T, Rosenblum M. When virtual is harder than real: Security challenges in virtual machine based computing environments. Proceedings of the 10th Conference on Hot Topics in Operating Systems; 2005. p. 20–5.
17. Guidelines on security and privacy in public cloud computing. Available from: https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing
18. Winkler V. Security concerns, risk issues, and legal aspects. Securing the Cloud. 2011. p. 55–81. https://doi.org/10.1016/B978-1-59749-592-9.00003-8.
19. Studnia I. Survey of security problems in cloud computing virtual machines. Computer and Electronics Security Applications Rendez-vous (C&ESAR); 2012. p. 61–74.
20. Hashizume K, Rosado D, Fernández-medina E, Fernandez E. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 2013; 4(5):1–13. https://doi.org/10.1186/1869-0238-4-5.
21. Security threats to evolving data centers; 2015. Available from: http://www.trendmicro.es/media/wp/security-threats-to-evolving-data-centers-en.pdf.
22. Nagar N, Suman U. Analyzing virtualization vulnerabilities and design a secure cloud environment to prevent from XSS attack. International Journal of Cloud Applications and Computing (IJCAC). 2016; 6(1):1–14. https://doi.org/10.4018/IJCAC.2016010101.
23. Vaughan-Nichols S. Virtualization sparks security concerns. Computer. 2008; 41(8):13–5. https://doi.org/10.1109/MC.2008.276.
24. Cloud security alliance. Best Practices for Mitigating Risks in Virtualized Environments. 2015. p. 1–35.
25. Wei J, Zhang X, Ammons G, Bala V, Ning P. Managing security of virtual machine images in a cloud environment. Proceedings of the 2009 ACM workshop on Cloud Computing Security; 2009. p. 91–6. https://doi.org/10.1145/1655008.1655021.
26. Modi CN, AchaK. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. The Journal of Supercomputing. 2017; 73(3):1192–234. https://doi.org/10.1007/s11227-016-1805-9.
27. Reuben JS. A survey on virtual machine security. Seminar on Network Security. 2007. p. 1–5.
28. Ranjith P, Priya C, Shalini K. On covert channels between virtual machines. Journal in Computer Virology. 2012; 8(3):85–97. https://doi.org/10.1007/s11416-012-0168-x.
29. Cloud Computing: Security Risk, SLA and Trust. Jönköping University. Available from: http://hj.diva-portal.org/smash/record.jsf?pid=diva2%3A323596&dswid=-3340.
30. Batra S, Applications C, Group C. Preliminary analysis of cloud computing vulnerabilities. International Journal of Innovation Science and Research. 2013; 2(5):49–51.
31. Khorshed T, Ali A, Wasimi S. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems. 2012; 28(6):833–51. https://doi.org/10.1016/j.future.2012.01.006.
32. Singh S. Virtualization and information security: A virtualized DMZ design consideration using VMware ESXi 4.1. Unitec Institute of Technology; 2012. p. 1–130.
33. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing. 2013; 63(2):561–92. https://doi.org/10.1007/s11227-012-0831-5.
34. Bamiah M, Brohi S. Seven deadly threats and vulnerabilities in cloud computing. International Journal of Advanced Engineering Sciences and Technologies. 2011; 9(1):87–90.
35. Douglas H, Gehrmann C. Secure virtualization and multicore platforms. Swedish Institute of Computer Science; 2009. p. 1–71.

36. Security issues in cloud computing. Available from: https://ieeexplore.ieee.org/document/6513028.
37. Threats to virtual environments. Security Response. Available from: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/threats-to-virtual-environments-14-en.pdf.
38. Xianqin C, Han W, Sumei W, Xiang L. Seamless virtual machine live migration on network security enhanced hypervisor. IEEE International Conference on Broadband Network and Multimedia Technology; 2009. p. 847–53. https://doi.org/10.1109/ICBNMT.2009.5347800.
39. OWASP the ten most critical web application security risks. Available from: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.
40. Afshan N. Analysis and assessment of the vulnerabilities in cloud computing. International Journal of Advanced Research in Computer Science. 2017; 8(2):1–4.
41. Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Security and Privacy. 2011; 9(2):50–7. https://doi.org/10.1109/MSP.2010.115.
42. Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM. Security issues in cloud environments: A survey. International Journal of Information Security. 2014; 13(2):113–70. https://doi.org/10.1007/s10207-013-0208-7.
43. Gonzalez N. A quantitative analysis of current security concerns and solutions for cloud computing. 3rd International Conference on Cloud Computing Technology and Science; 2011. p. 231–8. https://doi.org/10.1109/CloudCom.2011.39.
44. Islam T, Manivannan D. A classification and characterization of security threats in cloud computing. International Journal Next-Generation Computing. 2016; 7(1):1–17.
45. Tang Y, Lee PPC, Lui JCS, Perlman R. FADE: Secure overlay cloud storage with file assured deletion. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; 2010. p. 1–18.
46. Sobey CH, Orto L, Sakaguchi G. Drive-independent data recovery: The current state-of-the-art. IEEE Transactions on Magnetics. 2006; 42(2):188–93. https://doi.org/10.1109/TMAG.2005.861757.
47. Security aspects of virtualization. Available from: WP2016%201-3%203%20Study%20on%20security%20aspects%20of%20virtualization%20(1).pdf.
48. Luo S, Lin Z, Chen X, Yang Z, Chen J. Virtualization security for cloud computing service. International Conference on Cloud and Service Computing; 2011. p. 174–9. https://doi.org/10.1109/CSC.2011.6138516..
49. The notorious nine cloud computing top threats in 2013. Cloud Security Alliance; 2013. p. 1–21.
50. Owens K. Securing virtual compute infrastructure in the cloud. Savvis; 2009. p. 1–13. PMCid:PMC4781541.
51. Kong J. Protecting the confidentiality of virtual machines against untrusted host. Intelligence Information Processing and Trusted Computing; 2010. p. 364–8. https://doi.org/10.1109/IPTC.2010.11.
52. Behl A. Emerging security challenges in cloud computing. World Congress on Information and Communication Technologies; 2011. p. 217–22.
53. Parashar A, Borde A. Management cloud computing : Security issues and its detection methods. International Journal of Engineering Sciences and Management. 2015; 5(2):136–40.
54. Toward inter-VM visibility in a Cloud environment using packet inspection. Available from: https://ieeexplore.ieee.org/document/6632122.
55. Althobaiti AFS. Analyzing security threats to virtual machines monitor in cloud computing environment. Journal of Information Security. 2017; 8(1):1–7. https://doi.org/10.4236/jis.2017.81001.
56. Ahuja SP, Komathukattil D. A survey of the state of cloud security. Network and Communication Technologies. 2012; 1(2):66–75. https://doi.org/10.5539/nct.v1n2p12.
57. Shahzad A, Litchfield A. Virtualization technology: Cross-VM cache side channel attacks make it vulnerable. Australasian Conference on Information Systems; 2015. p. 1–14. PMid:25616160.
58. Tsai H, Chiao N, Steinmetz R, Darmstadt TU. Threat as a service: Virtualization's impact on cloud security. IT Professional. 2012; 14(1):32–7. https://doi.org/10.1109/MITP.2011.117.
59. Kedia P. A survey on virtualization service providers, security issues, tools and future trends. International Journal of Computer Applications. 2013; 69(24):36–42. https://doi.org/10.5120/12123-8491.
60. Pearce M, Zeadally S, Hunt R. Virtualization: Issues, security threats, and solutions. ACM Computing Surveys. 2013; 45(2):1–17. https://doi.org/10.1145/2431211.2431216.
61. Wang Z. HyperSafe : A lightweight approach to provide lifetime hypervisor control-flow integrity. IEEE Symposium on Security and Privacy; 2010. p. 380–95. https://doi.org/10.1109/SP.2010.30.
62. Rakotondravony N. Classifying malware attacks in IaaS cloud environments. Journal of Cloud Computing: Advances, Systems and Applications. 2017; 6(26):1–12.
63. Wang X, Wang Z, Liu Y, Luo Y, Li X. Detecting memory leak using virtualization technology. Information. 2013; 16(3):1693–707.
64. Khalil I, Khreishah A, Azeem M. Cloud computing security: a survey. Computers. 2014; 3(1):1–35. https://doi.org/10.3390/computers3010001.
65. Zhou F, Goel M, Desnoyers P, Sundaram R. Scheduler vulnerabilities and Coordinated attacks in cloud computing. Proceedings of the 2011 IEEE 10th International Symposium on Network Computing and Applications. 2011. p. 123–30. https://doi.org/10.1109/NCA.2011.24.

66. An identification and prevention of theft-of-service attack on cloud computing. Available from: https://ieeexplore.ieee.org/document/7496632.
67. Sabahi F. Cloud computing Reliability, Availability and Serviceability (RAS): Issues and challenges. International Journal on Advances in ICT for Emerging Regions. 2011; 4(2):12–23.
68. Kalpana G, Kumar PV, Krishnaiah RV. A brief survey on security issues in cloud and its service models. International Journal of Advanced Research in Computer and Communication Engineering. 2015; 4(6):457–63.
69. Cloud computing security considerations. Available from: https://etherealmind.com/wpcontent/uploads/2011/04/Cloud_Computing_Security_Considerations-1.pdf.
70. Azar Y, Kamara S, Menache I, Raykova M, Shepherd B. Co-location-resistant clouds. Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security; 2014. p. 9–20. https://doi.org/10.1145/2664168.2664179.
71. Varadarajan V. Isolation in public clouds: Threats, challenges and defenses. University of Wisconsin-Madison; 2015. p. 1–227.
72. Cloud computing: Issues and challenges. Available from: https://ieeexplore.ieee.org/document/5474674.
73. Lombardi F, Pietro R, Soriente C. CReW: Cloud resilience for windows guests through monitored virtualization. IEEE Symposium on Reliable Distributed Systems; 2010. p. 338–42. https://doi.org/10.1109/SRDS.2010.48.
74. Brooks T, Caicedo C, Park J. Security challenges and countermeasures for trusted virtualized computing environments. World Congress on Internet Security; 2012. p. 117–22.
75. Xia Y, Liu Y, Chen H, Zang B. Defending against VM rollback attack. IEEE/IFIP International Conference on Dependable Systems and Networks Workshops; 2012. p. 1–5.
76. Xia Y, Liu Y, Chen H. Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks. International Symposium on High Performance Computer Architecture; 2013. p. 23–7.
77. Durairaj M, Manimaran A. A study on security issues in cloud based e-learning a study on security issues in cloud based e-learning. Indian Journal of Science and Technology. 2015; 8(8):757–65. https://doi.org/10.17485/ijst/2015/v8i8/69307.
78. Cheng G, Jin H, Zou D, Ohoussou AK, Zhao F. A prioritized Chinese wall model for managing the covert information flows in virtual machine systems. International Conference for Young Computer Scientists; 2008. p. 1481–7. https://doi.org/10.1109/ICYCS.2008.534.
79. Zhang S, Meng X, Wang L, Xu L, Han X. Secure virtualization environment based on advanced memory introspection. Security and Communication Networks. 2018. p. 1–16. https://doi.org/10.1155/2018/3780407.
80. Tang W, Mi Z. Secure and efficient in-hypervisor memory introspection using nested virtualization. IEEE Symposium on Service-Oriented System Engineering; 2018. p. 186–91. https://doi.org/10.1109/SOSE.2018.00031.
81. Azab AM, Skalsky NC. Hyper sentry : Enabling stealthy in-context measurement of hypervisor integrity. ACM Conference on Computer and Communications Security; 2010. p. 38–49.
82. Zhang F, Chen J, Chen H, Zang B, Cloud visor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. 23rd ACM Symposium on Operating Systems Principles; 2011. p. 203–16.
83. Jin S, Huh J. Secure MMU: Architectural support for memory isolation among virtual machines. International Conference on Dependable Systems and Networks Workshops; 2011. p. 217–22. https://doi.org/10.1109/DSNW.2011.5958816.
84. Szefer J, Lee RB. Architectural support for hypervisor-secure virtualization. International Conference on Architectural Support for Programming Languages and Operating Systems; 2012. p. 1–13. https://doi.org/10.1145/2150976.2151022.
85. Jin S, Ahn J, Cha S, Huh J. Architectural support for secure virtualization under a vulnerable hypervisor. Annual IEEE/ACM International Symposium on Microarchitecture; 2011. p. 1–12. https://doi.org/10.1145/2155620.2155652.
86. Keller E, Szefer J, Lee RB. NoHype : Virtualized cloud infrastructure without the virtualization. Annual International Symposium on Computer Architecture; 2010. p. 350–61. https://doi.org/10.1145/1815961.1816010.
87. Rogers B, Chhabra S, Solihin Y, Prvulovic M. Using address independent seed encryption and bonsai merkle trees to make secure processors OS-and performance-friendly. Annual IEEE/ACM International Symposium on Microarchitecture; 2007. p. 183–94. https://doi.org/10.1109/MICRO.2007.16.
88. Yashveer Y, Krishna CR. Two-level security framework for virtual machine migration in cloud computing. i-Manager's Journal on Information Technology. 2018; 7(1):34–44. https://doi.org/10.26634/jit.7.1.14095.
89. Santos N, Gummadi K, Rodrigues R. Towards trusted cloud computing. 2009 Conference on Hot Topics in Cloud Computing; 2009. p. 1–5. PMCid:PMC2831950.
90. Xiaopeng G, Sumei W, Xianqin C. VNSS: A network security sandbox for virtual computing environment. IEEE Youth Conference on Information, Computing and Telecommunications; 2010. p. 395–8. https://doi.org/10.1109/YCICT.2010.5713128.

91. Sailer R. sHype : Secure hypervisor approach to trusted virtualized systems. IBM Research Report; 2005. p. 1–13.
92. Chen WZ, Zhu HW, Huang W. SeVMM: VMM-based security control model. International Conference on Cyberworlds; 2008. p. 820–3.
93. Garfinkel T, Rosenblum M. A virtual machine introspection based architecture for intrusion detection. Network and Distributed Systems Security Symposium; 2003. p. 1–16. PMid:12522106.
94. Srivastava A, Giffin J. Tamper-resistant, application-aware blocking of malicious network connections. International Workshop on Recent Advances in Intrusion Detection; 2008. p. 39–58. https://doi.org/10.1007/978-3-540-87403-4_3.