A SURVEY ON SECURITY CHALLENGES OF VIRTUALIZATION TECHNOLOGY IN CLOUD COMPUTING

Nadiah M. Almutairy[1] and Khalil H. A. Al-Shqeerat[2]

[1] Computer Science Department, College of Sciences and Arts in Rass, Saudi Arabia
[2] Computer Science Department, Qassim University, Saudi Arabia

ABSTRACT

Virtualization has become a widely and attractive employed technology in cloud computing environments. Sharing of a single physical machine between multiple isolated virtual machines leading to a more optimized hardware usage, as well as make the migration and management of a virtual system more efficiently than its physical counterpart. Virtualization is a fundamental technology in a cloud environment. However, the presence of an additional abstraction layer among software and hardware causes new security issues. Security issues related to virtualization technology have become a significant concern for organizations due to arising some new security challenges.

This paper aims to identify the main challenges and risks of virtualization in cloud computing environments. Furthermore, it focuses on some common virtual-related threats and attacks affect the security of cloud computing.

The survey was conducted to obtain the views of the cloud stakeholders on virtualization vulnerabilities, threats, and approaches that can be used to overcome them.

Finally, we propose recommendations for improving security, and mitigating risks encounter virtualization that necessary to adopt secure cloud computing.

KEYWORDS

Cloud Computing, Virtualization, Security, Challenge, Risk
.

1. INTRODUCTION

Virtualization technology plays a vital role in the creation of a cloud-computing environment. It enables more than one operating system called virtual machine (VM) that co-reside on the same physical server and utilizing the dynamic allocation of resources on the same machine without meddling each other.

Virtualization technology helps numerous instances of the same application to be run on one or multiple cloud resources [1]. Virtualization layer automatically provides the scalability, where multiple users able to run their application at the same time. It allows the user to run own applications on a single-VM and he cannot see the data of other users. However, there are different vulnerabilities in the virtualization environment, and thus there are numerous security threats at the virtualization layer.

DOI: 10.5121/ijcsit.2019.11308

Virtualization technology provides benefits to anyone who uses a computer, commercial companies, government organizations, and IT professionals.

It gives organizations and people an opportunity to utilize and improve the use of their hardware by increasing the number and types of tasks that a single machine can handle [2].

Two significant benefits that can be provided in a virtualization environment are resource sharing, and isolation. Resource sharing is one of the most critical advantages of virtualization since users can allocate physical resources to a VMs based on their requirements. More than one VMs can run on the same host, and each VM can share the resources of the host. VMs share access to central processing units, disk controllers, physical network cards, and so forth.

Another benefit that can be given by the virtual environment is isolation; VM isolates own data from other VMs. The failure in one VM will not affect the performance or the executing of other VMs running on the same host. When the VM fails, there is no impact on users' ability to access other VMs, or the ability of other VMs on the same host to access resources they need. Moreover, isolation implies that programs running on one VM cannot see others that run on another VM.

It can be concluded that the different VMs can share resources of the physical machine with no interference between them. These properties enable different operating systems and applications to be securely and simultaneously running at the same time on a single physical machine.
Security is a hot issue in virtualization because of its characteristic, infrastructure, monitoring, and security policies. Various vulnerabilities, risks, and threats at the virtualization layer affect the integrity, confidentiality, and availability of cloud services and resources.

This study aims to identify and understand the main challenges and security issues of virtualization in cloud computing environments. Furthermore, it presents baseline recommendations for improving security and mitigating risks encounter virtualization to adopt secure cloud computing.

The rest of the paper is organized as follows. Virtualization security challenges and risks are investigated in the next section. Section III describes major attacks might threaten virtualization systems. The survey results and analysis are discussed in Section IV. Finally, section V presents helpful recommendations and guidelines to avoid or alleviate any potential virtualization threats.

2. SECURITY CHALLENGES AND RISKS

This section investigates set of common vulnerabilities and risks of virtualization in cloud computing environments.

1. User awareness: 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 [3].

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. 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.

2. Insecure APIs: A cloud-computing provider provides infrastructure, software, and platform services to the users and enables them to access the services through their interfaces. They designed their interfaces via the published application programming interfaces. According to [4], APIs pose a variety of security issues such as improper authorizations, weak credentials, and clear-text during transmission may affect the availability and the security of the cloud services.

3. Lack of security policies: The organization defines security policies to determine how to protect its assets from any potential threats and how to deal with these situations when they occur. The security policies of the cloud service provider may be inadequate or incompatible with the security requirements of an organization. Lack of security policies may pose some vulnerabilities that lead to the insecure environment of VMs.

From another side, VMs can be moved between physical environments as required. When a VM is migrated or moved from the source host to another host, the destination host might not have enough security to protect the VM [5]. Mobile VMs need baseline histories and security policies to move with them.

4. Weak authentication and session management: Authentication is the mechanism 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 both end users and components of the system. Improperly designed or implemented application functions related to authentication and session management may affect access and control policy [6]. Moreover, it enables attackers to compromise keys, session tokens, or passwords and to exploit flaws of other implementation to assume other identities of users.

5. Incorrect VM isolation: The hypervisor is responsible for ensuring isolation between different VMs. The isolation between VMs prevents the VM from gets access to others' virtual disks, applications, or memory on the same host [7]. Furthermore, isolation of VM limits the scope of the attack. It makes access resources, and sensitive data on the physical machine complicated.

A violation in isolation occurs when the attacker uses a compromised VM for communicating with other VMs on the same host [8]. Therefore, a shared environment requires an accurate configuration for maintaining strong isolation.

6. Insecure VM migration/mobility: Live migration technique is one of many advantages of the virtualization, which enables the application to be transparently transmission from one host machine to another without halting the VM [9]. After migration, the application continues in execution without any loss of progress. The user is unaware his VM is migrated. The VM is migrated by moving the VM's application with entire system state, including memory, the state of CPU, and sometimes disk to the destination host. However, during migration, the attacker may passively steal and snoop or actively modify confidential information. Therefore, the transmission channel has to be protected and secured against different passive and active attacks.

7. Lack of reliability and availability of service: Issues that related to the reliability of virtualization can affect the performance of cloud computing. The combination of many VMs may lead to performance problems. There are some factors lead to performance problems such as limited CPU or I/O bottlenecks. These problems happen more in a virtual environment than the traditional environment because in the virtual environment the physical server connected to numerous VMs that compete in accessing the critical resources. With many services being built on cloud infrastructures, the failure may occur and leads to the lack of availability of internet-based applications and services. In a terrible climate with much lightning, the electricity may be interrupted, which leads to a lack of availability of cloud services [10].

8. VM image sharing: VM image is a pre-packaged software template contains the configurations files that are utilized to create VMs. Therefore, the integrity of these images is fundamental for the general security of services provided by the cloud provider [11]. The users of cloud computing can create their own VM image from scratch or can use the existing images available in the shared repository. The VM images provide an easy way for deploying and restoring virtual systems efficiently and quickly across numerous of physical servers [12]. Sharing VM images is a commonly used practice in a cloud environment as a quick method to create VM. Although of these benefits or advantages, VM image sharing introduces some risks that in turn affect the security of the cloud. The malicious user can exploit the common repository to upload a VM image that contains malware. Thus, the VM that instantiated by using the uploaded malicious VM image will infect the cloud system. Furthermore, the infected VM can cause privacy breach when it is employed to monitor the data and activities of other users.

9. VM diversity: Many IT enterprises overcome the problem of security by enforcing homogeneity. In a virtual environment, VMs can facilitate more efficient usage models that get the benefit from executing older or unpatched versions of the software. Therefore, it is easy to own a wide range of different operating systems to run older or unpatched versions of software. Unfortunately, VM diversity may become a cesspool of infected machines when they are not secured. VM diversity may cause significant issues as one have to maintain patches, provide other protection for a diversity OSs, and cope with the risk posed by having numerous of unpatched or older machines on the network [13].

10. VM transience: In a physical computing environment, users own one or more machines that are online most of the time, so it is in a stable state. In contrast, in a virtualized environment, the machines can come and go from the network sporadically. This concept is called VM transience [14]. Therefore, 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.

Although VM transience limits the opportunity that an attacker can exploit to penetrate the system, it makes security audits and maintenance more challenging because machines must be connected online when they are scanned or patched. A fluctuating environment is more prone to a persisting infection because infected VMs can infect other vulnerable machines, and can go offline before detection.

3. VIRTUALIZATION THREATS AND ATTACKS

The virtualization threats and attacks that involved in this study are described in this section.

1. Cross-VM Attack: The cross-VM attack occurs when a malicious virtual machine avoids the hypervisor-level isolation in order to attack co-located VMs. According to [15] cross-VM attacks range from controlling other VMs by taking advantage of guest or hypervisor vulnerabilities to gain secret data by side-channel attacks. Numerous VMs are placed on a single server for maximizing the resource usage; this co-resident placement may cause cross VM side channel attack. The basic scenario of a cross-VM side channel attack is through co-location attack and poor implementation of the isolation methods; a malicious VM conducts side-channel attacks. Thus, sensitive information can be extracted to continue the attack using another method to get control of the whole system [16].

2. VM Rollback: The hypervisor can pause a VM during running, capture a snapshot of the current disk, memory, CPU states, and resume a snapshot in the future without VM awareness. This characteristic has been used for VM maintenance and fault tolerance, but it allows the attacker to start VM rollback attack [17]. The attacker can use old snapshots of VM, run it without the user's awareness, then remove the history of the VM execution, and again execute the different or the same snapshot. Since the history of the VM execution is lost, the attacker can avoid some security mechanisms or undo updates of some security mechanisms [18].

3. Data Loss and Data Leakage: Generally, Data leakage occurs when sensitive information gets into the wrong hands when it is being audited, stored, processed, or transferred. Whereas, the data loss occurs when stored data is lost due to loss of encryption key, or any accidental deletion [19].

4. Foot printing Attack: 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 out malicious activities on the system [20].

5. VM Sprawl: VM sprawl attack occurs when the number of VMs on the same host is continuously increasing without proper control, and some of them are in the idle state [21]. Since VMs retain the resources of the system such as network channels, memory, and these system resources are effectively missing and cannot be allocated to other VMs. VM sprawl causes a problem for cloud providers because a large number of VMs need a huge memory requirement [22].

6. VM Escape: VM escapes a threat intended to exploit a hypervisor. It is a situation where a malicious VM or user escapes from the control of hypervisor [23]. In VM escape, a malware software running in a VM can completely bypass the isolation between the VMs and the host. Thus, the attacker can get access to the hypervisor, which leads to the breakdown of the whole system. When the attack is successful, the attacker can get privileges to access the storage hardware, computing power, the shared resources, and other VMs.

7. VM Hopping: VM hopping is the process of jumping from one VM to another one by exploiting vulnerabilities in either the hypervisor or virtual infrastructure. Because the hypervisor performs high privileges, exploiting the hypervisor would have significant consequences [24]. When the attackers are maliciously getting access to different VMs belonging to other users, they can monitor the target VM's resource, changing its configurations, removed stored data, and affecting that VM's integrity, availability, and confidentiality.

8. Hyperjacking: Hyperjacking attack inserts VM-based rootkits to control the entire virtualized environment. It injects a fake hypervisor underneath the original one and modifies it [25]. VM-based rootkit established a covert channel for malicious injection code to the hypervisor and hiding it from the security mechanism [26]. Because the hypervisor runs at the most privileged on a system, it would be very hard or even impossible for any operating system (OS) running on the hypervisor to detect it.

4. SURVEY RESULTS AND ANALYSIS

In this study, the survey is conducted to gather opinions of faculty members, graduate students and IT staff on vulnerabilities and threats of virtualization in cloud computing, and to select effective security approaches used to alleviate the virtualization security risks. The number of participants in this survey is 127 participants. The survey is prepared based on the following research questions:

1. What are the essential virtualization vulnerabilities and risks in cloud-computing environments?

2. What are the virtualization threats and attacks may exploit the vulnerabilities of cloud computing?

3. What are security techniques that alleviate the security issues of virtualization technology? When reviewing responses to the questionnaire, we noticed that only 14% of the participants did not understand security vulnerabilities and risks of their cloud systems. Nearly 40% of respondents are not aware of threats and attacks that may threaten virtual systems and about 30% of them do not know security solutions used to avoid these threats. It indicates that cloud users need to be more aware of the security issues related to the virtual infrastructure.

4.1. Common Vulnerabilities of Virtualization

The responses to the first question are shown in Figure 1.

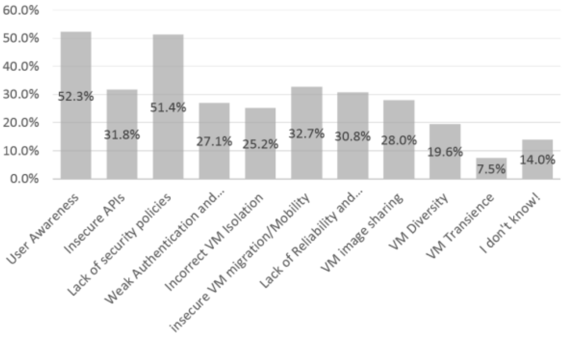

Figure 1. Virtualization vulnerabilities and risks

It is understood that the user awareness (with 52.3% votes from respondents) and lack of security policies (with 51.4% votes from respondents) are the common vulnerabilities that prone the cloud environment to be attacked. User awareness and the lack of security policies obtained close voting ratios from the respondents. It indicates that user awareness is the result of the lack of policies between service providers and users. It is crucial to ensure that policies must be clear between the user and the companies that provide services.

It is also observed some of the vulnerabilities available for selection in the questionnaire have the close voting ratios such as the insecure APIs (with 31.8% of respondents), lack of reliability and availability of service (with 30.8% of respondents), and insecure VM migration/mobility (with 32.7% of respondents). Insecure APIs, lack of reliability and availability of service, and insecure VM migration/mobility can cause leakage or loss of sensitive data, which cloud users are concerned.

27.1 % of those were included in the questioner selected weak authentication and session management, and 28% selected VM image sharing. We notice from these close voting ratios that respondents are afraid from sharing of VM image when authentication mechanisms are weak because the attacker can exploit the poor authentication mechanisms to upload a malicious VM to the image repository.

It is also concluded that 19.6% of the sample believe that VM diversity constitutes a vulnerability to cloud computing although it makes management tasks more difficult, such as software patching. The respondents did not notice that the ease and speed of creating VMs meant that there are new operating systems that may cause security risks. It is allowed to a wide range of different operating systems to run older or unpatched versions of software, and this heterogeneity may cause many vulnerabilities and risks.

The lowest rating was for VM Transience (7.5 votes from respondents). They are unaware of the security problems (like worm attack) resulting from that the virtualized environment is never in a stable state.

4.2. Threats or Attacks on Virtualization

Figure 2 represents the opinions of participants on major attacks might threaten virtualization systems in cloud computing environments.

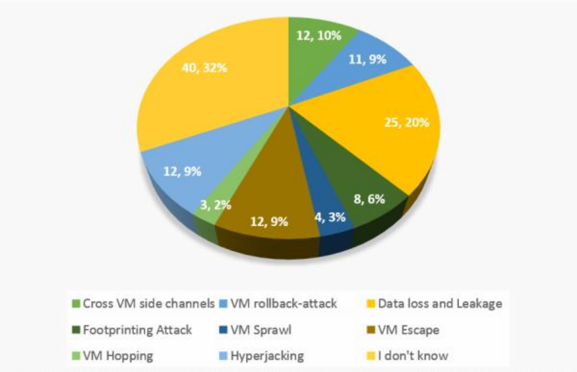

Figure 2. Virtualization threats and attacks

Sensitive data is always a concern for users. Therefore, 25.2% of the respondents agreed the data loss and leakage are a significant threat that can affect the virtual environment.

We noticed that the respondents have concerned with any threats or attacks against hypervisor or that exploit poor isolation. Therefore, hyperjacking, VM escape, cross VM side channels, and VM rollback are occupying the same rank.

Although footprinting helps the attackers to recognize that the victim system is operating in a virtualized environment to conduct malicious activities, only 8.6% of respondents selected footprinting. A little of respondents selected VM sprawl and VM Hopping with 4.3% and 3.2% respectively.

4.3. Security Approaches and Techniques:

The responses to this question are represented graphically in Figure 3. We noticed that 31.8% of respondents have a background about scientific secure framework to alleviate the virtualization security risks.

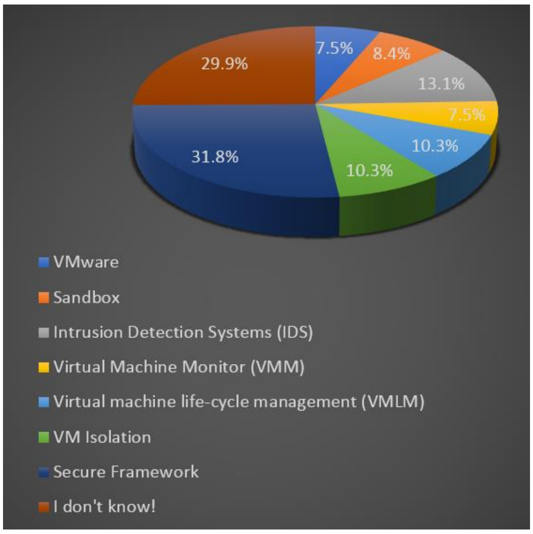

Figure 3. Virtualization approaches and techniques

13.1% of participants in the questionnaire have selected trust Intrusion Detection Systems (IDS) to protect cloud systems from intruders.

The virtual isolation and management are an essential benefit of virtualization technology that we have to focus on any solutions may enhance it. However, we find only 10.3% of the sample selected VM isolation and VM life-cycle management (VMLM) software as a practical solution. Only 8.4% of respondents think that a sandbox–based solution helps to defend against different attacks.

The findings show the solution based on Virtual Machine Monitor (VMM), and VMware solutions are occupying the same rank.

5. RECOMMENDATIONS

At the end of this study, we present a few baseline recommendations for stakeholders of cloud computing to enhance the security of virtualization.

A. User Awareness: User awareness is an essential part of any system to counter any attempt to tamper with the system. All involved parties such as service providers and organizations have to focus on the education and training of their staffs and apply assurance processes to evaluate the human resources. Small and medium-sized companies, corporations and government agencies can have a contribution in increasing user awareness by urging their professional staff to attend training courses of relevant institutes to build skills.

End users should know their rights and the threats that may breach their privacy in virtual environments by attending relevant courses and instructional activities.

B. Secure Host OS: The protection of the operating system (OS) on the host machine is critical because the virtualization layer exists above OS. A compromised OS provides a suitable environment to attack the virtualization layer. The providers of services need to update the version of OS, remove /disable unnecessary software and services, and install host intrusion detection system and anti-virus.

C. Secure the Hypervisor: The hypervisor is an additional software layer resides between VMs and the underlying hardware with or without a host OS. Some hypervisors automatically check updates and install them when found. Centralized patch management solutions can be used for administering updates. Disconnect unused devices from the host can help in securing the hypervisor. It is better to harden the configuration of the hypervisor to minimize areas of vulnerability.

We think the user accounts including privileged accounts on the hypervisor have to be integrated with the organization directory infrastructure. This choice ensures that authentication is done through a robust authentication protocol. Limiting the number of user (including privileged) accounts wants to access to the hypervisor helps in securing the hypervisor.

D. Protect the VM: There is a need to use a virtual firewall to prevent VM to VM attack and apply a robust authentication mechanism to block unauthorized access to VM. If a virtual machine is compromised, we have to suppose that all VMs within the same server has also been compromised. In such a case, restore each guest OS to a good image or snapshot that was taken before the compromise. Therefore, it is a good idea to create a backup of virtual drive that used by the guest OS. We have to isolate and protect the memory of guest VMs from other VMs that share the same physical system and even from an untrusted hypervisor.

E. Manage Snapshots and Images: When images are managed in a good way, organizations will get operational and security benefits. It is important to think about the security of VM image and snapshot. Images can be less risky than snapshots because snapshots have the contents of RAM, and this may contain sensitive data that was not even stored on the hard drive as clear text. The library of VM image have to reside outside of the host, and the library ought to have strict access control because images have to be protected against unauthorized modification, and every image of the library should have a digital signature. For detecting unauthorized modification, implement an integrity checksum mechanism to VM images /snapshots. It is best to encrypt the snapshots of VMs and store the checksum information separately from the VM image/snapshot. To detect a malware, such as a rootkit, scan the image files. The administrators have to implement strict processes and controls around the creation, access, and deployment of VM images. We have to use proper sanitization process when the stored snapshots needed to be deleted.

F. Prevent Data Loss and Data Leakage: To protect and secure sensitive data in the VMs, we have to encrypt the stored data in VM to minimize the risks that result from accessing the storage. Utilizing an encrypted secure transmission channel like SSL/TLS can helps in protecting the sensitive data. The users need to follow proper practices in managing and destroying data. The administrator has to apply identity checks when a guest OS wants to access the storage volumes. We have to Keep backups of necessary data regularly and put policies to guarantee that the backup systems are cleaned while erasing and wiping the VM images such as zero-filling for avoiding any extra data.

G. Prevent VM Sprawl: Because of the dynamic characteristic of virtual environments, a VM sprawl can occur. In such case, VMs are created to be used for a period, but it is not noticeable that they exist in a systems inventory. For example, some of these virtual machines may be created for short-term purposes such as testing, but remain active after they have served their initial purpose. These VMs can be missed during patching.

The hypervisor has to analyze the need for the new VMs and ensures that unnecessary VMs migrate to other servers with more availability and high-energy efficiency. We can use discovery and systems management tools to examine, patch, and implement security configuration changes to VMs.

6. CONCLUSIONS

Virtualization is a technique that has been broadly applied for the participation of the capabilities of physical computers by dividing the resources among operating systems. It helps numerous instances of the same application to be run on one or multiple cloud resources.

In this study, we have investigated the common challenges and risks of virtualization technology, in addition to main threats and attacks might compromise virtualized system in cloud computing environments.

The survey is conducted and distributed among faculty members and graduate students in some universities in Saudi Arabia, in addition to IT staff and experts

At the end of the study, a comprehensive list of recommendations has been suggested to avoid security risks in virtualized systems efficiently.

REFERENCES

[1] B. Loganayagi and S. Sujatha, “Creating virtual platform for cloud computing,” in Proc. 2010 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1-4.

[2] L. Garber, “The Challenges of Securing the Virtualized Environment,” Computer, vol. 45, no. 1, pp. 17-20, 2012.

[3] Cloud Security Alliance, “Top threats to cloud computing V1.0,” CSA, 2010. [Online]. Available: https://cloudsecurityalliance.org/ topthreats/csathreats.v1.0.pdf. [Accessed: Nov.-2017].

[4] Cloud Security Alliance,“The Notorious Nine. Cloud Computing Top Threats in 2013,” CSA, 2013. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats.%5Cnhttp://www. cloudsecurityalliance.org. [Accessed: Oct.-2017].

[5] G.Xiaopeng, W.Sumei, and C.Xianqin,“VNSS: A network security sandbox for virtual computing environment,” In Proc. 2010 IEEE Youth Conference on Information, Computing and Telecommunications, 2010, pp. 395–398.

[6] N. Afshan,“Analysis and Assessment of the Vulnerabilities in Cloud Computing,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 2, 2017, pp. 2015–2018.

[7] S. Bulusu and K, Sudia, “A Study on Cloud Computing Security Challenges,” Master thesis, School of Computing at Blekinge Institute of Technology, 2012.

[8] H. Wu, Y. Ding, C. Winer, and L. Yao,“Network Security for Virtual Machine in Cloud Computing,” in Proc. 5th International Conference on Computer Sciences and Convergence Information Technology, 2009, pp. 18–21.

[9] M. R. Anala, J. Shetty, and G. Shobha,“A frameIEEwork for secure live migration of virtual machines,” in Proc. Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2013, 2013, pp. 243–248.

[10] A. Parashar and A. Borde, “Cloud Computing: Security Issues and its Detection Methods,” Int. J. of Engg. Sci. & Mgmt., vol. 5, no. 2, 2015, pp. 136–140.

[11] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning,“Managing security of virtual machine images in a cloud environment,” in Proc. ACM workshop on Cloud computing security - CCSW ’09, 2009, p. 91.

[12] Cloud Security Alliance, “Best Practices for Mitigating Risks in Virtualized Environments,” Downloads.cloudsecurityalliance.org, 2015. [Online]. Available: https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risk s _Virtual_Environments_April2015_4-1-15_GLM5.pdf. [Accessed: 11- Jan- 2017].

[13] T. Garfinkel and M. Rosenblum,“When Virtual is Harder Than Real: Security Challenges in Virtual Machine Based Computing Environments,” in Proc. 10th Conf. Hot Top. Oper. Syst., 2005, pp. 20–25.

[14] I. Studnia, E. Alata, Y. Deswarte, M. Kaâniche, and V. Nicomette, “Survey of Security Problems in Cloud Computing Virtual Machines,” in Proc. Computer and Electronics Security Applications Rendez-vous (C&ESAR), 2012, pp. 61–74.

[15] Y. Azar, S. Kamara, I. Menache, M. Raykova, and B. Shepherd, “Co-Location-Resistant Clouds,” in Proc. 6th edition of the ACM Workshop on Cloud Computing Security, 2014, pp. 9-20.

[16] V. Varadarajan, "Isolation in Public Clouds: Threats, Challenges and Defenses", PhD thesis, University of Wisconsin–Madison, 2015.

[17] I. Khalil, A. Khreishah, and M. Azeem,“Cloud Computing Security: A Survey,” Computers, vol. 3, no. 1, 2014, pp. 1–35.

[18] Y. Xia, Y. Liu, H. Chen, and B. Zang, “Defending against VM rollback attack,” in Proc. IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012), 2012, pp. 1-5.

[19] R.D. Londhe and S.S. Sherekar, “Imperial Analysis of Threats and Vulnerabilities in Cloud Computing,” International Journal of Advanced Research in Computer Science, vol. 5, no. 4 2014, pp. 12-17.

[20] T. Brooks, C. Caicedo, and J. Park, “Security challenges and countermeasures for trusted virtualized computing environments,” In Proc. World Congress on Internet Security (WorldCIS-2012), 2012, pp. 117 – 122.

[21] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, “Virtualization security for cloud computing service,” in Proc. Int. Conf. Cloud Serv. Comput., 2011, pp. 174–179.

[22] R. Schwarzkopf, (2015) “Virtual Machine Lifecycle Management in Grid and Cloud computing,” University of Marburg. [Online]. Available: http://archiv.ub.uni-marburg.de/diss/z2015/0407/pdf/ drs.pdf. [Accessed: Aug.-2017].

[23] V.K. Veeramachaneni, “Security Issues and Countermeasures in Cloud Computing Environment,” Int. J. Eng. Sci. Innov. Technol., vol. 4, no. 5, 2015, pp. 82–93.

[24] K. Owens, “Securing Virtual Compute Infrastructure in the Cloud,” SAVVIS, 2009.[Online]. Available: http://viewer.media.bitpipe.com/1018468865_999/1296679360_880/Securing-Virtual-Compute-Infrastructure-in-the-Cloud.pdf. [Accessed: Jun-2017].

[25] S. Z. I. Tariqul and D. Manivannan, “A Classification and Characterization of Security Threats in Cloud Computing,” Int. J. Next-Generation Comput., vol. 7, no. 1, pp. 1–17, 2016.

[26] C. N. Modi and K. Acha,“Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review,” J. Supercomput., vol. 73, no. 3, 2017, pp. 1192-1234.