IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-9, Sept 2019 E-ISSN: 2347-2693

A Research on Cloud Computing Challenges in Virtualization and Cloud Environment

Vaibhav Sardana[1], Nidhi Saxena[2*]

[1,2]Gautam Buddha University, Greater Noida, Yamuna Expressway, Uttar Pradesh, India

Corresponding Author:nidhi4407@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i9.226229 | Available online at: www.ijcseonline.org

Accepted: 10/Sept/2019, Published: 30/Sept/2019

Abstract- Virtualization allows for multiple virtual machines or users to be logically segregated and access simultaneously the same physical machine from remote locations. It enables the cloud characteristics of resource pooling and multi-tenancy. Moreover it introduces the rapid elasticity feature and optimal management of resources. Virtualization supports the cloud in implementing its service and deployment models. Virtual machines can be created, copied and migrated which leads to security challenges. This paper elaborates on virtualization vulnerabilities and presents solutions existing in literature to the security threats.

Key words- Virtualization, Virtual machine, Challenges, Solutions.

I. INTRODUCTION

Virtualization gives several benefits than traditional systems [1]. Virtualization allows for running multiple operating systems simultaneously [1]. Moreover, virtualization offers improved, optimized and low cost services to clients through supporting the cloud in providing its services [2].Virtualization allows for many instances of virtual machines in a single physical machine [1]; these instances are called VMs. A VM has its own operating system and applications [3].A VM is initiated for each user that virtually provides a complete operating machine to the user [17].A VM monitor (VMM) or hypervisor is the module managing the VMs and permits different operating systems to run simultaneously on the same physical machine [17]. Security concerns may change according to the type of hypervisor used [1].Hosted hypervisor is deployed on the operating system [1, 4].This virtualized infrastructure is exposed to more threats than bare metal hypervisor [1]; VMs are hosted in the physical machine and they can communicate with each other [1]. This communications allows for attacks by intruders [5]. However, the communication among VMs is out of the scope of the study.

The remainder of the paper is organized as follows. Section two is the related work. Section three is the security vulnerabilities. Section four is the current solutions and section five is the conclusion.

II. RELATED WORK

Hassan Tabaki et al. [6] illustrated the unique issues of security and privacy challenges with cloud where Minqi Zhou et al. [7] examined cloud security and privacy issues in terms of the special relationship between the service providers and the users. However, they did not reveal the need and importance of virtualization security.

Kresimir Popovic et al. [8] provided in their work a generic overview of the security issues, the requirements and the challenges that many cloud service providers' face. Kui Ren et al. [9] investigated various security challenges for the public cloud without considering the threats in service models. However, none of the existing research considers the threat levels in different service models from the perspective of virtualization technologies. Hsin-Yi Tsai et al. [10] have examined various threats and security issues with virtualization including service models but they have not specified the impact of virtualization on cloud security with Database as a Service.

R.D. Pietro [11] proposed a new methodology, Transparent Cloud Protection System (TCPS) for the improvement of security issues in cloud services. Pietro claimed that TCPS can monitor cloud components integrity and ensure transparency and virtualization. TCPS improves the security and transparency and suggests a mechanism to detect intrusion. However, the work has not been proven or implemented in a real cloud environment. Maneesha [12] in his work discussed the types of clouds and their security challenges and explained how to prevent different security problems including DOS attacks and attack on VMs. Y.Chen et al. [13] presented their views regarding the cloud. Those views are related to multi-users concern regarding trust and the need for mutual inspection for business accounts and users isolations.

In 2009, T. Ristenpart et al. [14] showed that a cloud platform multiplexing many customers' VMs on a shared physical infrastructure can introduce new threats, such as cross-VM side-channel attacks. Their work emphasized the importance of virtualization technologies in cloud computing security. Yet, the authors stated only threats resulting from virtualization technologies. Grobauer et al. [15] defined some indicators of cloud specific threats but they did not discuss the implications of virtualization technology on different service models. Morsy et al. [16] considered cloud security issues in different service models, but they discussed only virtualization-related issues for the Iaas model.

III. SECURITY VULNERABILITIES

Virtualization exposes the cloud user and infrastructure to security vulnerabilities [18].The security issues related to virtualization are discussed below.

VM image sharing. A VM image is used to instantiate VMs [2]. A user can create his/her own image or use an image from the shared image repository [19].Sharing VM images in the image repository can evolve as a serious threat if it is used in a malicious manner [20]; A malicious user can investigate the code of the image to look for attack points or he can upload image that contains malware [20].The VM instantiated using the infected image will become source of introducing malware in the cloud [2].The infected VM can be used in the monitoring of the activities and data of other users resulting in a privacy breach [2]. Moreover if the image is not cleaned it can expose confidential information of the user [19].

VM isolation. VMs running on the same hardware need to be isolated from each other [2].Although logical isolation is present, the access to the same resources can lead to data breach and cross-VM attacks [2]. VMs isolation is not only needed on storage devices but also on memory and computational hardware [21, 22].

VM escape. A VM escape is a situation in which a malicious user or VM escapes from the control of the VMM [23].This situation can provide an attacker access to other VMs and can bring the VMM down [20]. In addition access to the computing and storage hardware can be provided [2].The IaaS service model is affected and that in turn can affect other service models [24].

VM migration. The VM migration is relocating a VM to another physical machine without shutting down the VM [25].The VM migration is carried out for different reasons such as load balancing, fault tolerance and maintenance [19,26] . During the migration process, the contents of the VM are exposed to the network that might lead to data security concerns [2]. Besides data, the code of the VM becomes vulnerable to attackers during migration [25, 20]. In addition, the migration module can be compromised by an attacker to relocate the VM to a compromised server or under the control of a compromised VMM [2].The VM migration is crucial and needs to be performed in a secured manner [19].

VM rollback. Virtualization allows the rollback of a VM to some previous state [2].However, rollback raises security concerns [27].For example, the rollback can enable the security credentials that were previously disabled [19].Moreover, the rollback can render the VM to a vulnerability that was previously patched [28].In addition, the rollback can revert the VM to previous security policies and configuration errors [19].

Hypervisor issues. A compromised VMM can put the VMs managed by the victim VMM under attacker's control [29].The metadata of the VMs may also be exposed to an attacker if the attacker takes control of a VMM [25, 29].A VMM provides large attack vector due to more entry points and interconnection complexities [29].In addition, there are many reported bugs in the VMM that let the attacker to take control of the VMM or bypass security restrictions [2, 29].

VM sprawl. VM sprawl is a situation where a number of VMs is increasing and most of the already instantiated VMs are in an idle state [30]. The VM sprawl results in the resources of the host machine to be wasted on a large scale [23].

IV. SOLUTIONS IN LITERATURE

The VM images require high security and integrity as they specify the initial state of the VM [2]. In addition, the VM images are used by various and unrelated users [2]. Therefore, the security of the images is the basis for the security of the whole cloud [2].Wie et al. [31] proposed Mirage, an image management system for the cloud. In Mirage the publishing and retrieval of VM images is controlled by an access control framework. The access control is provided at check in and check out of the repository. Publishing, retrieval and modifications of a VM image require proper permissions. Filters are applied to the images at publishing and retrieval to detect and remove unwanted information. The filters remove the leftover private information, malware and pirated software in the image. A tracking system is used to keep track of an image both in terms of actions and derivation. In addition, maintenance of the repository is also provided by Mirage. Maintenance services run periodically malware detection tools for the images in the repository and discover vulnerabilities and patches.

A VM needs to be protected against attacks not only in repository but also during execution time [2].The decoupling

of the security and management of the VM to protect the runtime environment of the VM is utilized in CloudVisor

[32]. A CloudVisor is a security module that works beneath the VMM using nested virtualization. A CloudVisor provides privacy and integrity to the VM resources during execution. The control transitions between the VMM and the VMs are intercepted by the CloudVisor to perform security operations such as hide the general purpose registers of the VM from VMM and exposing only the necessary one. The CloudVisor monitors the address translation to enforce memory isolation. Moreover it encrypts and decrypts every disk I/O by a VM. The disk data is ensured by using Merkel tree and MD5 hash algorithm. The integrity of the CloudVisor is ensured by a Trusted Platform Module (TPM).

In the cloud environment, VMs are migrated between different physical locations and cloud facilities for various reasons such as load balancing, physical machine failure, energy savings and hardware/software upgrading [2].One of the techniques presented in the literature to handle VM migration is by Aslam et al. [33].This technique allows VM migration only if the destination platform is secured to the user defined level. A Trust Assurance Level (TAL) is used that specifies the trust level of the destination platform. The TAL is computed using the credentials of the hardware Trusted Platform Module (TPM) and the credential of the Trust Token proposed by the authors. The Trust Token specifies the trust level of the applications. The user specifies the TAL (least, low, high, average, and normal) at the VM launch process. A VM migration is only allowed if the TAL of the destination platform is in the range of the specified user requirements. The process can also be used to measure the TAL of the hosted platform at the time of the VM launch. Moreover, the authors assume Platform Trust Assurance Authority as a third party for trust certification. The proposed technique lets the user audit the TAL of the destination platform after the VM migration to assure his requirements are met.

The hypervisor or VMM is the software that manages and controls the virtualization in the cloud [2].A compromised hypervisor can destroy the whole system [2]. Zhang et al. [34] presented a framework HyperCheck to ensure a secure execution of the hypervisor. The HyperCheck uses the CPU system management mode of x86 architecture for viewing the CPU and memory state of the machine. In addition it uses an SMM module that resides in the BIOS and is inaccessible by other CPU modes. The SMM module reads and verifies the content of the CR3 and IDTR registers as they play a central role of root kit detection. Moreover the PCI network card is used to read the physical memory and its driver is handled in the SMM module to avoid attacks. The memory contents and the results of the CPU registers verification are sent to a monitor machine that acts as a trusted third party. The memory contents are analyzed by an analysis module on the monitor machine based on linearity, firmness and quality. The complete snapshot is compared with the initial snapshot of the hypervisor. In case of malicious activities, human operators are notified. The transmission of the contents of memory to the monitor machine is performed through a secure connection. The encryption key for transmission is managed by the monitor machine. The HyperCheck was implemented for both open and closed source BIOS. The framework showed detection and defense against root kit, code and data integrity, DoS, and network security attacks.

The authors in [35] proposed a scheme to defend against the VM rollback attack by secure logging and auditing of VM operations (suspend, resume, and migrate). For each operation the hash value of the VM snapshot is calculated over its registers, memory contents and image disk. The hash value for each state is used for later activation of the snapshot. A similar mechanism of logging and auditing VM operations is also used in [36].Ref. [37] provides a mechanism HyperShot that ensures the integrity of the VM snapshots and the hypervisor. This is accomplished by a Trusted Platform Module (TPM) based attestation, digital signature, and trusted initialization of hypervisor.

To protect the private information leakage due to rollback, the authors in [38] proposed SPARC. The SPARC is a secure check pointing mechanism that allows the users to exclude the applications that process private information from being check pointed. Consequently the life time of the confidential information is reduced. The authors in [39] proposed also a strategy named Privacy-Preserving Checkpointing (PPC) for excluding of confidential information from check points. The PPC tracks the private information by information flow analysis and at time of a snapshot, removes the confidential information.

V. CONCLUSION

The goal of this research is to highlight security issues related to cloud computing virtualization and present some current solutions. Moreover, the paper contributes to the understanding of the vulnerabilities of virtualized cloud computing. However, there are security issues that still need to be resolved or require conducting more research. For example VM escape, VM isolation, VM secured migration and VM sprawl [1, 2]. Moreover an undefeatable security mechanism in the virtualized environment is yet to exist [1] .As virtualization technology is in its early days, many security threats still need to be countered.

REFERENCES

[1]. M. Gupta, D. Srivastava, D. Chauhan, Security Challenges of Virtualization in Cloud Computing, in: ICTCS'16 proceedings of the Second International Conference on Information &

Communication Technology for Competitive strategies, March 04-05, Udaipur, India 2016, dl.acm.org/citation.cfm?id=2905315. http://dx.doi.org/10.1145/2905055.2905315

[2]. M. Ali, S. Khan, A. Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences 305 (2015) 357-383.

[3]. Menasce, Daniel A. "Virtualization: Concepts, applications, and performance modeling." In Int. CMG Conference, 2005, pp. 407-414.

[4]. M. Garcia-Valls, T. Cucinotta, C. Lu, Challenges in real-time virtualization and predictable cloud computing, Journal of Systems Architecture 60 (2014) 726-740.

[5]. Gabriel Cephas Obasuyi, Arif Sari "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", Int. J. Communications, Network and System sciences, 8, 2015, 260-273.

[6]. Hassan Takabi and James B.D. Joshi, University of Pittsburgh, Gail-Joon and Ahn Arizona State University, "Security and Privacy Challenges in Cloud Computing Environments", IEEE security and privacy, www.computer.org/security, 2010, pp.24-31.

[7]. Mingi Zhou et al., "Security and Privacy in Cloud Computing: A Survey, " Proc. 6th Int'l Conf. Semantics, Knowledge and Grids, IEEE Press, 2010, pp. 105-112.

[8]. Kresimir Popovic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges, " Proc. 33rd Int'l Convention on Information and Comm. Technology, Electronics and Microelectronics (MIPRO 10), IEEE Press, 2010, pp. 344-349.

[9]. Kui Ren, Cong Wang, and Qian Wang, Ilnois Institute of Technology, "Security Challenges for the Public Cloud", IEEE Press, 2012, pp. 69-73.

[10]. Hsin-Yi Tsai, Melanie Siebenhaar and Andre Miede, Yu-Lun Huang, Ralf Steinmetz, "Threat as a Service?Virtualization's impact on Cloud Security", IEEE, IT Pro, 2012, pp: 32-37.

[11]. Flavio Lombardi & Roberto Di Pietro, "Transparent Security for Cloud", SAC'10 March 22-26, 2010, Sierre, Switzerland.

[12]. Maneesha Sharma, Himani Bhansal and Amit Kumar Sharma, "Cloud Computing Different Approach & Security Challenge", In International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, 2012, pp. 421-424.

[13]. Yanpei Chen, Vern Paxson and Randy H. Katz, "What's New About Cloud Computing Security?", Technical Report No. UCB/EECS-2010-5.

[14]. T. Ristenpart et al.., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199-212.

[15]. B. Grobauer, T. Walloscheck, and E. Stocher. "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 9, no. 2, 2011, pp. 50-57.

[16]. M. A. Morsy, J. Grundy, and I. Muller, "An Analysis of the Cloud Computing Security Problem," Proc. 17th Asia Pacific Software Eng. Conf. 2010 Cloud Workshop (APSEC 10), IEEE Press, 2010.

[17]. Y. Neng-Hai, Z. Hao, J. Xu, W. Zhang, C. Zhang, Review of cloud computing security, Acta Electron, Sinica 41 (2) (2013) 371-381.

[18]. K. Ren, C. Wang, Q.Wang, Security challenges for the public cloud, IEEE Internet Comput. 16 (1) (2012) 69-73.

[19]. K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 1-13.

[20]. W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp 1-10.

[21]. N. Gonzalez, C. Miers, F. Redgolo, M. Simplcio, T. Carvalho, M. Nslund, M. Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (1) (2012) 1-18.

[22]. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1-11.

[23]. M.H. Song, Analysis of risks for virtualization technology, in: Applied Mechanics and Materials, vol. 539, 2014, pp. 374-377.

[24]. S.H. Na, E.N. Huh, A broker-based cooperative security-SLA evaluation methodology for personal cloud computing, Sec. Commun. Netw. (2014), http://dx.doi.org/10.1002/sec.1086.

[25]. F. Zhang, H. Chen, Security preserving live migration of virtual machines in the cloud, J. Netw. Syst. Manage. 21 (4) (2013) 562-587.

[26]. A. Corradi, M. Fanelli, L. Foschini, VM consolidation: a real case based on openstack cloud, Future Gener. Comput. Syst. 32 (2014) 118-127.

[27]. R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, B. Freisleben, Increasing virtual machine security in cloud environments, J. Cloud Comput. 1 (1) (2012) 1-12.

[28]. H. Wu, Y. Ding, C. Winer, L. Yao, Network security for virtual machine in cloud computing, in: 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, pp. 18-21.

[29]. J. Szefer, E. Keller, R.B. Lee, J. Rexford, Eliminating the hypervisor attack surface for a more secure cloud, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 401-412.

[30]. K.S. Rao, P.S. Thilagam, Heuristics based server consolidation with residual resource defragmentation in cloud data centers, Futur Gener. Comput. Syst. (2014), http://dx.doi.org/10.1016/j.future.2014.09.009.

[31]. J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managing security of virtual machine images in a cloud environment, in: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 2009, pp. 91-96.

[32]. F. Zhang, J. Chen, H. Chen, B. Zang, Cloudvisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, in: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, 2011, pp. 203-216.

[33]. M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869-876.

[34]. F. Zhang, J. Wang, K. Sun, A. Stavrou, HyperCheck: a hardware-assisted integrity monitor, IEEE Trans. Denpendable Sec. Comput. (2013), http://dx.doi.org/10.1109/TDSC.2013.53.

[35]. Y. Xia, Y. Liu, H. Chen, B. Zang, Defending against VM rollback attack, in: IEEE/IFIP 42nd International Conference on Dependable Systems and Networks Workshops, 2012, pp. 1-5.

[36]. Y. Xia, Y. Liu, H. Chen, Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks, in: IEEE 19th International Symposium on High Performance Computer Architecture, 2013, pp. 246-257.

[37]. Srivastava, H. Raj, J. Gi_n, P. England, Trusted VM snapshots in untrusted cloud infrastructures, in: Research in Attacks, Intrusion and Defenses, Springer, Berlin, Heidelberg, 2012, pp. 1-21.

[38]. M. I. Gofman, R.Luo, P. Yang, K. Gopalan, Sparc: a security and privacy aware virtual machine check pointing mechanism, in: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, 2011, pp. 115-124.

[39]. Y. Hu, T. Li, P. Yang, K. Gopalan, An application-level approach for privacy-preserving virtual machine checkpointing, in: IEEE Sixth International Conference on Cloud Computing, 2013, pp. 59-66.

