A review paper on hypervisor and virtual machine security

Zunaid Aalam¹, Vinod Kumar¹, Surendra Gour²
¹Department of Computer Science and Engineering, SGT University, Gurgaon
²Department of Computer Science and Engineering, Jamia Hamdard.

Email: zunaid.aalam6194@gmail.com

Abstract- A hypervisor is a computer programme or software that facilitates to create and run multiple virtual machines. It is also known as Virtual Machine Manager (VMM). Due to their popularity, it exploits the attack surface, because the Hypervisor code contains much vulnerability. Since the Hypervisor is a core element of any cloud computing service, it is always on the top priority of the attackers. There are many Software (open source) and Hardware-based Solutions are available in the market to monitor and control the hypervisor activities. This paper summarizes various types of attacks, vulnerabilities, security issues and challenges related to hypervisor and virtual machines.

Keywords: Virtualization, Hypervisor, Virtual Machine, Vulnerability, VMBR, DoS.

1. Introduction
Virtualization allows multiple machines to run on a single Hardware. This VMM has the capabilities to share the resources of the physical machine. Resources of this physical machine are managed by the software Known as Hypervisor [1]. Hypervisor works as an isolating layer which manages the physical hardware and the Virtual machines. This code increase attack surface, because Hypervisor has full access to Virtual machines data in CPU registers, Memory and I/O [2]. Due to that Hypervisor is a lucrative target for the attackers. When a Hypervisor is a compromise, intruders can gain the full access of all the VMs hosted on particular Physical Machine. There are two types of Hypervisor available in Market [3].

(i) Type 1 Hypervisor
Type 1 Hypervisor direct installed and run on the Physical layer (Hardware). These are also known as Native Hypervisor or bare metal Hypervisor [4]. There is no requirement of any Host Operating system. Type 1 Hypervisor has direct access and control over Hardware resources. Cloud service provider generally used this type of Hypervisor [5]. Some of the Type 1 Hypervisor is Proxmox, VMware ESXI, and Citrix Xenserver, Ovirt, Hyper-V [6]. In this Figure, there are showing the structure of Type 1 Hypervisor.
(ii) **Type-2 Hypervisor**
Type-2 hypervisor installs on Host operating system of a physical Machine. These hypervisors are also known as Hosted Hypervisor. It supports VMs by coordinating calls for CPU, memory, disk, network and other resources through the Physical host’s operating system. Example of Type-2 Hypervisor is VMware Workstation and Oracle VM VirtualBox [7]. In this Figure, there are showing the structure of Type 2 Hypervisor.

**Figure 1.** Structure of type 1 Hypervisor.

**Figure 2.** Structure of type 2 Hypervisor.
(iii) Hypervisor Security

Each Virtual Machine installed in the virtual environment has its security zone which is not accessed by the other Virtual Machines security zones. A hypervisor is an abstraction layer that breakup host machine from the guest machines [8]. A hypervisor is the centralized controlling agent of all the virtual machines and has its security zone. All the security zones in the virtual environment lay with in the same physical environment and same security zone [9].

To explore the security issues related to Hypervisor security, first, we have to know about the various privilege mode for CPU. There is three privilege level in any processor[10]. These are shown in the Figure-3.

![Figure 3. Privilege level in any processor.](image)

Ring 0 is innermost and most privilege level in the protection Rings. This level is also known as Kernal level. Any Software and application at this level have full command on the host Hardware. Ring 1 and ring 2 have comparatively less privilege than ring 0. These two rings are related to Operating System services. Outermost is ring 3, all the applications programme run on this layer [11-14]. The hypervisor runs on the Kernal mode, which is the most privilege level and Guest operating system runs on the less privilege mode then the Hypervisor. Hypervisor Architecture along with its privilege level is shown in Figure 4. User application runs on ring 3, having no privilege to control the hardware resources. The hypervisor manages the hardware resources which is access by the guest operating system[15-18].

As Hypervisor run on the upper layer of Physical hardware. Physical resources are accessible only through the Hypervisor that's why security of the cloud environment depends on Hypervisor. It also acts as a firewall, which prevents the unauthorized sharing of physical resources. Hypervisor isolates the guest operating system[18,19], host operating system and physical hardware. If an attacker bypasses the security at the guest operating system, Hypervisor monitors it. It works as a manager between the guest OS and Physical hardware. Guest machine(VMs) operating system has come through the Hypervisor to access the physical machine components[20].

A hypervisor is like a code of thousands of line. To prevent security and minimize the vulnerability of the Hypervisor. Hypervisor code should be as least as possible. There are generally three results of an attack in a virtualized environment[21].
In First case the guest machine is compromised. In second case Multiple Virtual Machines are compromised and in the third case, the Host Machine or Hypervisor compromised[22]. First and Second case can be restored to previous well-known configuration state, but in the third case, attackers have full control of the physical hardware. According to a survey based on VMs security, it is found that around 60-65% Virtual machines which are in production are less secure than the Physical Machines because of ignoring the traditional security measures[23].

The attacker used the compromised guest to communicate with other guest installed on the same physical hardware. When Hypervisor has compromised then attacker it can access all the resources of guest machine and host also, He can perform the various attacks linked Denial of Service (DOS) attack and Botnet attacks[24].

2. Features of Hypervisors/VMs (Security)
Virtualization gaining popularity day by day because of their features like restoring the VMs to pre-attack states, isolation of users, imitate computing environment, support remote computation. These are some benefits concerning security[25-27].

2.1 Abstraction of physical resources
Hypervisor abstract the Physical layer and strictly bounded resources are allocated to the Guest Machine. Through abstracting the Hardware details Hypervisor restrict the access of physical hardware. The Guest machine running inside the Hypervisor don’t know about the host operating system and Hardware[28]. When an attacker doesn’t know about the details of the operating system and Hardware of the Hypervisor the surface of attack level is reduced and compromising of Machine is difficult[29]. The Hypervisor aims to allocate the resources to the resources to each Virtual Machines. Each Virtual Machine encapsulates itself and prevents other VMs from accessing their resources. An attacker can not compromise the physical machine and only one virtual machine at a time [30].

2.2 Pre-attack State Restore
The virtual disk of each Virtual Machine stored at the Host machine as a file. Virtual Machine takes a backup (Snapshot) of the virtual disk on a regular time interval or any changes made in
configuration[31]. Incase of Machine Compromization or any other type of infection, We can restore the VMs from backup disk files. It provides the integrity of the data and disinfection of Machine[32].

2.3 Isolation of Physical resources
Hypervisor makes partitions of the physical resources and makes isolated entities. A hypervisor allows each VMs to run independently. Attack and compromisation of one VM can not affect the other. Isolation and Abstraction characteristics of the Hypervisor an additional security feature. In case any VM compromised, Hypervisor remove this VM and restore it to pre-attack state[33].

3. Vulnerabilities and Attacks
Virtual machines and Physical Machines both are vulnerable to the theft and various type of attacks like Denial of service attack(DoS)[34]. VM Infrastructure is vulnerable to the DOS attack, which withholds resources from all VMs installed on Physical Machine. We can Fix it in many cases by applying QOS for the resource consumption per VMs[35]. There are some Vulnerabilities and attacks at Hypervisor Level.

3.1 Modification in Hypervisor
In this type of attack, attackers try to modify the Hypervisor(OS). One form of this type of attack is Virtual Machine Machine based Rootkits (VMBR). VMBR is malware, it is difficult to detect and remove through malware detectors[36]. It is capable to breach the guest OS security and dig out the way to compromise the hypervisor or directly attack a hypervisor to gain the full control of the system. Blue Pill and Subvirt are examples of these type of Malware[37]. There are many methods to prevent from Hypervisor modification. A host can use a trusted relationship with a hypervisor or the guest verify the integrity of the hypervisor at the time of booting[38].

3.2 Guest to guest attack
It is also known as VM communication. In this type of attack, One Infected VM try to infect the other machines on the same environment. A malicious Guest can probably access another guest through shared resources like Memory, Network connections[39]. For example, if a VM opts the memory allocation lies of the other VM then it can perform the read-write operation to that location and distributed the other operations[40]. For the prevention of these type of attack system or cloud, an administrator has to define the rules and policies for communication between VMs and only authorized VMs to take part in communication within the VM Infrastructure[41]. Example of these type of attacks is SQL injection attack and spoofing attacks.

3.3 Data Stealing / Mobility
Theft of the Virtual Machine can happen without physical access of the machine. The data of each VM are store in a virtual disk in the form of an image. Most of the hypervisor provides the facility to copy this disk image and run on other physical Machine[42]. This is a good feature of hypervisor but it has some drawback also. Attackers can copy the VM over the network and access data in their environment and have enough time to dig out all the security arrangements like passwords type of encryption used[43].

3.4 Hypervisor Intrusion
Abstraction, Isolation and resource allocation between the guest and host is managed by the Hypervisor. The main target of the attackers to get full control of the hypervisor and execute the malicious code with root access[44]. The function of hypervisor is to convert instructions received from the guest to the instruction for the Host Operating System. If the Guest is compromised, then the instructions sent by the guest to hypervisor may be aberrant[45-48].
4. Conclusion and Future Work
Virtualization technology probably has new vulnerabilities. For Security professional, it is a big challenge to make all VMs secure in the computing environment. In this paper, we describe the features of the hypervisor and discussed the attacks and vulnerabilities in Virtualization environment[48-52]. The hypervisor should rigorously control the communication between the VMs, limit the resources and monitoring the consumption of the resources by VM on regular basis for preventing the Daniel of Services(DoS) attacks. It is mandatory to secure the host and each VMs (guest) to secure the whole virtual environment[52-54]. We have to Compliance all the advisory released by the CERT-In related to cloud security and Vulnerability[55]. As a future work of my paper, we will install the VMs on the different type of open source-based hypervisor like proxmox[56-57],ovirt, Citrix and perform the Vulnerability Assessment and penetration testing to exploit the vulnerabilities of the system[58] using the various freeware tools. Some of the tools are Burp Suite, Network Miner packet analyzer, TCPDump, Nmap and hydra etc[59-60].

References
[1] John patrick and Rameez Asif,” Securing Cloud Hypervisors: A Survey of the threatens, Vulnerabilities and Countermeasures”, 11 June 2018.DOI-10.1155/2018/1681908.
[2] Nguyen TH, Di Francesco M, Yla-Jaaski A (2017) Virtual machine consolidation with multiple usage prediction for energy-efficient cloud data centers. IEEE Trans Serv Comput.
[3] Basu D,Wang X, Hong Y, Chen H and Bressan S (2019) Learn-as-you-go with megh: Efficient live migration of virtual machines, IEEE Trans Parallel Distrib Syst 30(8):1786–1801.
[4] Nasim R, Zola E, Kasselr AJ (2018) Robust optimization for energy-efficient virtual machine consolidation in modern datacenters. Cluster Comput 21(3):1681–1709.
[5] Shidik GF, Azhari A, Mustofa K (2016) Improvement of energy efficiency at cloud data center based on fuzzy Markov normal algorithm VM selection in dynamic VM consolidation. Int Rev Comput Soft (IRECOS) 11(6):511–520.
[6] Abdullah M, Lu K, Wieder P, Yahyapour R (2017) A heuristic-based approach for dynamic vms consolidation in cloud data centers. Arab J Sci Eng 42(8):3535–3549.
[7] Zhang, T., Lee, R.B., Cloudmonatt: An architecture for security health monitoring and attestation of virtual machines in cloud computing. In: Proceedings of the 42nd Annual International Symposium on Computer Architecture. 2015:362–374.
[8] Pang S, Xu K, Wang S, Wang M Wang S (2020) Energy-saving virtual machine placement method for user experience in cloud environment. Math Prob Eng 1–9.
[9] Singh N, Dhir V (2019) Hypercube based genetic algorithm for efficient vm migration for energy reduction in cloud computing. Stat Opt Inf Comput 7(2):468–485.
[10] Kansal NJ, Chana I (2016) Energy-aware virtual machine migration for cloud computing—a firely optimization approach. J Grid Comput 14(2):327–345.
[11] Wu Q, Ishikawa F, Zhu Q, Xia Y (2016) Energy and migration cost-aware dynamic virtual machine consolidation in heterogeneous cloud datacenters. IEEE Trans Serv Comput 1–13.
[12] Rybina K, Schill A (2016) Estimating energy consumption during live migration of virtual machines. In: IEEE international black sea conference on communications and networking (BlackSeaCom), pp 1–5.
[13] Kumar N, Zeadally S, Chilamkurti N and Vinel A (2015) Performance analysis of Bayesian coalition game-based energy-aware virtual machine migration in vehicular mobile cloud, IEEE Network 29(2):62–69.
[14] Dave Shackleford(2013).”Fundamentals of Virtualization Security.In:Judy Flynn. Virtualization security :Protecting Virtualized Environments,Canada:Jhon Wiley,PP2-13.
[15] Li X, Garraghan P, Jiang X, Wu Z, Xu J (2017) Holistic virtual machine scheduling in cloud datacenters towards minimizing total energy. IEEE Trans Parall Distrib Syst 29(6):317–1331.
[16] Ismaeel S, Karim R, Miri A (2018) Proactive dynamic virtual-machine consolidation for energy conservation in cloud data centres. J Cloud Comput 7(1):1–28.
[17] Kim J, Ruggiero M, Atienza D, Lederberger M (2013) Correlation-aware virtual machine allocation for energy-efficient datacenters. Des Automat Test Eur Conf Exhib (DATE), 1345–1350.
[18] T. Gardinkel.M.Rosenblum,”When Virtual is Harder than Real: Security Challenges in virtual Machine Based Computing Environments,”USENIX Association,2005.http://www.stanford.edu/talg/papers/HOTOS05/virtual-harder-hotos05.pdf
[19] N.Arya,M.Gidwani and S.K. Gupta,” Hypervisor security – A makor concern”,International Journal of Infomanation and Computation Technology,vol.3, no.6,pp533-538,2013.
[20] M.Ali,S.U.Kan and A.V. Vasilakos,”Security in cloud computing :opportunities and challenges”,Information Science,vol.305,pp.357-383,2015.
[21] S.Jin,J.Seol,J.Huh and S.maeng,"Hardware-assisted secure resource accounting under a vulnerable Hypervisor", . ACM
SIGPLAN Notice vol.50.no 7, pp.201-213,2015.

[22] Farzad Sabahi, “Secure Virtualization for Cloud Environment Using Hypervisor-based technology”, Singapore, http://www.ijmlc.org/papers/87-A888.pdf

[23] L. Turnbull and J. Shropshire, “Breakpoints: An analysis of potential hypervisor attack vectors”, in Proceeding of the IEEE SoutheastCon 2013.

[24] Chen L, Shen H (2014) Consolidating complementary VMs with spatial/temporal-awareness in cloud datacenters, IEEE Conf Comput Commun 1033–1041.

[25] Esfandiarpoor S, Pahlavan A, Goudarzi M (2015) Structure-aware online virtual machine consolidation for datacenter energy improvement in cloud computing, Comput Electr Eng 42:74–89 (2015).

[26] Ahvar E, Ahvar S, Mann ZA, Crespi N, Garcia-Alfaro J, Glitho R (2016) CACEV: a cost and carbon emission-efficient virtual machine placement method for green distributed clouds. In: IEEE International Conference on Services Computing (SCC), pp 275–282.

[27] A. Singh and K. Chatterjee, “Cloud Security issues and challenges: A survey,” Journal of Network and Computer Applications Vol.79, pp.88-115,2017.

[28] A. Ukil,D.Jana,and A.De.Sarkar, “ A Security Framework in Cloud Computing , ”International Journal of Network Security and its Application ,vol.5,no.5,pp.11-24,2013.

[29] A.Cleeff,W.pieters and R.Wieringa, “ Security implications of Virtualization: A literature study”. In proceedings of the 12 th IEEE International Conference on Computational Science and engineering (cse09),vol.3,pp.201,2015.

[30] S.K. Majhi and S.K. dhal, “A study on security vulnerability on cloud platforms”, in proceeding of the 1st International conference on Information security and Privacy 2015.

[31] S.Singh,y.Jeong and J.H. Park , “ A survey on cloud computing security:Issues,threats and solutions,” Journal of Network and Computer Applications Vol.75,pp.200-222,2016.

[32] L. Turnbull and J. Shropshire, “Breakpoints: An analysis of potential hypervisor attack vectors,” in Proceedings of the IEEE SoutheastCon 2013: Moving America into the Future, 2013.

[33] Lin W, Xu S, Li J, Xu L, Peng Z (2017) Design and theoretical analysis of virtual machine placement algorithm based on peak workload characteristics. Soft Comput 21(5):1301–1314.

[34] Ruan X, Chen H (2015) Performance-to-power ratio aware virtual machine (VM) allocation in energy-efficient clouds. In: IEEE international conference on cluster computing, pp 264–273.

[35] S. Manavi and S. Mohammadalian, “Secure model for virtualization layer in cloud infrastructure,” International Journal of Cybersecurity and Digital Forensics, vol. 1, no. 1, pp. 32–40, 2012.

[36] L. Almutair and H. Zaghoul, in Proceedings of The Third International Conference on Digital Information Processing and Communications (ICDIPC ‘13), pp. 676–686, UAE, 2013.

[37] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[38] Kamesh and N. Sakhti Priya, “Security enhancement of authenticated RFID generation,” International Journal of Applied Engineering Research, vol. 9, no. 22, pp. 5968–5974, 2014.

[39] O. Harfoushi, B. Alfawwaz, N. a. Ghatasheh et al., “Data security issues and challenges in cloud computing: A conceptual analysis and review,” Communications and Network, vol. 6, no. 1, pp. 15–21, 2014.

[40] N. Arya, M. Gidwani, and S. K. Gupta, “Hypervisor security- A major concern,” International Journal of Information and Computation Technology, vol. 3, no. 6, pp. 533–538, 2013.

[41] Farahnakian F, Pahikkala T, Liljeberg P, Plosila J, Tenhunen H (2014) Multi-agent based architecture for dynamic VM consolidation in cloud data centers. In: IEEE 40th euromicro conference on software engineering and advanced applications, pp111–118.

[42] Liu Y, Sun X, Wei W, Jing W (2018) Enhancing energy-efficient and qos dynamic virtual machine consolidation method in cloud environment. IEEE Access 6:31224–31235.

[43] Arroba P, Moya JM, Ayala JL, Buuya R (2017) Dynamic Voltage and Frequency Scaling-aware dynamic consolidation of virtual machines for energy efficient cloud data centers. Concurrency Comput: Pract Experience 29(10):1–13.

[44] A. Cleeff, W. Pieters, and R. Wieringa, “Security implications of virtualization: A literature study,” in Proceedings of the 12th IEEE International Conference on Computational Science and Engineering (CSE ’10), vol. 3, pp. 353–358, 2009.

[45] S. Jin, J. Scol, J. Huh, and S. Maeng, “Hardware-assisted secure resource accounting under a vulnerable hypervisor,” ACM SIGPLAN Notices, vol. 50, no. 7, pp. 201–213, 2015.

[46] S. N. Brohi, M. A. Bamiah, M. N. Brohi, and R. Kamran, “Identifying and analyzing security threats to virtualized cloud computing infrastructures,” in Proceedings of the 2012 International Conference on Cloud Computing Technologies, Applications, and Management, ICCCTAM 2012, pp. 151–155, are, December 2012.

[47] A. Ukil, D. Jana, and A. De. Sarkar, “A Security Framework in Cloud Computing,” International Journal of Network Security and Its Applications, vol. 5, no. 5, pp. 11–24, 2013.

[48] L. Adhianto, S. Banerjee, M. Fagan et al., “HPCTOOLKIT: Tools for performance analysis of optimized parallel programs,” Concurrency and Computation: Practice and Experience, vol. 22, no. 6, pp. 685–701, 2010.

[49] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” Journal of Network and Computer Applications, vol. 79, pp. 88–115, 2017.

[50] S. K. Majhi and S. K. Dhal, “A Study on Security Vulnerability on Cloud Platforms,” in Proceedings of the 1st
International Conference on Information Security and Privacy 2015, pp. 55–60, ind, December 2015.

[51] I. M. Khalil, A. Khreishah, and M. Azeem, “Cloud computing security: A survey,” Computers, vol. 3, pp. 1–35, 2014.

[52] A. A. Malik, H. Anwar, and M. A. Shibli, “Federated identity management (FIM): Challenges and opportunities,” in Proceedings of the Conference on Information Assurance and Cyber Security, (CIACS ’15), vol. 1, pp. 75–82, 2016.

[53] S.-K. Kim, S.-Y. Ma, and J. Moon, “A novel secure architecture of the virtualized server system,” The Journal of Supercomputing, vol. 72, no. 1, pp. 24–37, 2016.

[54] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.

[55] N. Sabharwal and R. Shankar, Apache Cloudstack Cloud Computing, Packet Publishing Ltd., 2013.

[56] X. Wang, Z. Du, Y. Chen, and M. Yang, “A green-aware virtual machine migration strategy for sustainable data-center powered by renewable energy,” Simulation Modelling Practice and Theory, vol. 58, pp. 13-14, 2015.

[57] Dai X, Wang JM, Bensaou B (2015) Energy-efficient virtual machines scheduling in multi-tenant data centers. IEEE Trans Cloud Comput 4(2):210–221.

[58] Masoumzadeh SS, Hlavacs H (2013) Integrating VM selection criteria in distributed dynamic VM consolidation using fuzzy Q-Learning. In: Proceedings of the 9th international conference on network and service management (CNSM), pp 332–338.

[59] Pahlevan XQ, Zapater M, Atienza D (2017) Integrating heuristic and machine-learning methods for efficient virtual machine allocation in data centers. IEEE Trans Comput-aided Des Integr Circ Syst 37(8):1667–1680.

[60] Haghshenas K, Mohammadi S (2020) Prediction-based underutilized and destination host selection approaches for energy-efficient dynamic VM consolidation in data centers. J Supercomput 1–18