Safeguard Hypervisor attacks in cloud computing

Shreyal Gajare
Computer Engineering,
Maharashtra Institute of Technology, Pune

Prof.Shilpa Sonawani
Maharashtra Institute of Technology,
Pune

Abstract: In last few decades, the computation world in cloud computing is in boom. Cloud computing is a new delivery model for enabling convenient ,on-demand network access of the computing resources. As cloud computing reduces cost and complexity of applications, and is also flexible and scalable it has become one of the exciting technologies. Thus organizations are working hard to maintain security and resilience in cloud technology. Virtualization is one of most crucial element that makes cloud computing. A key Part of virtualization is the hypervisor which manages the physical platform and can access all of its resources. As hypervisor is the manager of virtualization it is more vulnerable for attacks. Thus in this paper a technique combining virtual machines and hypervisor intrusion detection system is proposed for detecting and preventing hypervisor attacks in cloud environment. VMHIDS adopts various features inspecting tasks which occur frequently and prevent suspicious events.

Keywords: Hypervisor; Hypervisor Attack; Hypervisor-based Intrusion Detection System; Virtualization

I. Introduction

Cloud computing is model that accounts two essential concepts: ‘abstraction’ and ‘virtualization’ to increase the capacity and capability of IT by providing on demand. Security is the major concern for this system, because the services of cloud computing is based on the sharing. Virtualization is one of most important element that makes cloud computing. Virtualization is a term that refers to the abstraction of computer resources. The main component of virtualized system is hypervisor and is responsible to enforce isolation between virtual machines and resource management of the hardware. Hypervisor is the software which permits multiple guest virtual machines to run concurrently on the same server. Hypervisor is the single point of failure. So, the hypervisor also needs to be carefully monitored for signs of compromise.

However, the current approaches like, Intrusion Detection System –Hypervisor-based (HICDS) on protecting the hypervisor attack are not adequately. This indirectly leads to the Cloud Service Provider (CSP) to face the security issues due to the vulnerability of the hypervisors. The weakness of the HIDS is the lack of effective functionalities that can fulfill the requirements of both of the cloud providers and users. The HIDS approach requires the administrator to manipulate manually if the attack is detected. This is because the Hypervisor-based IDS do not run in real time environment.

The major purpose this article serves is to detect necessary approaches for defending hypervisor attacks in cloud computing.

II. Background

A. Cloud Computing

Cloud computing is a general term for the delivery of hosted services over the internet. Cloud computing allows users and enterprises with various computing capabilities to store and process data either in a privately-owned cloud, or on a third-party server located in a data center - thus making data-accessing mechanisms more efficient and reliable. It can be visualized into frontend and backend as shown in Figure 1.According to [1], the frontend is whereby the authorized users can utilize the services offered by the cloud computing, namely the application, servers, networks and storage.

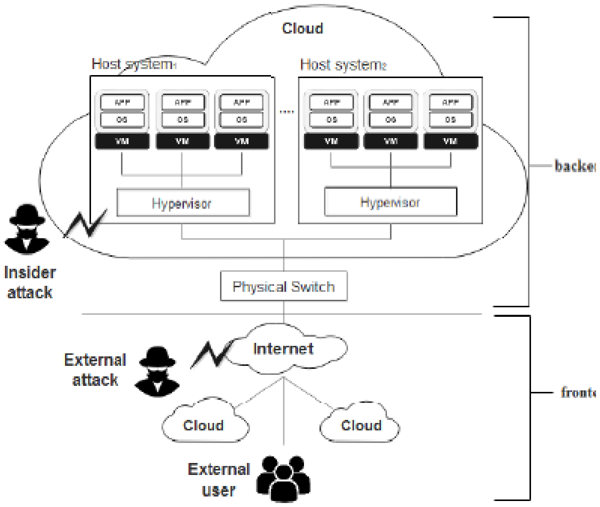

Figure 1. Overview of Cloud Computing

There are various systems used in cloud computing specifically in virtualized environment. These host systems comprise of virtualization technology that supports various VMs utilize similar resources while performing execution on hypervisors.

B. Hypervisor / Virtual Machine Monitor(VMM)

Hypervisor also known as Virtual Machine Monitor is responsible for managing VMs in cloud computing. It monitors for resources shared among the virtual machines. Further it also isolates any unauthorized virtual machines to access in cloud environment [2]. The main functions of the hypervisors are creating, terminating, moving the VMs and allocation the resources. There are two types of hypervisors Native (Type 1) and Hosted (Type 2) as shown in figure 2.

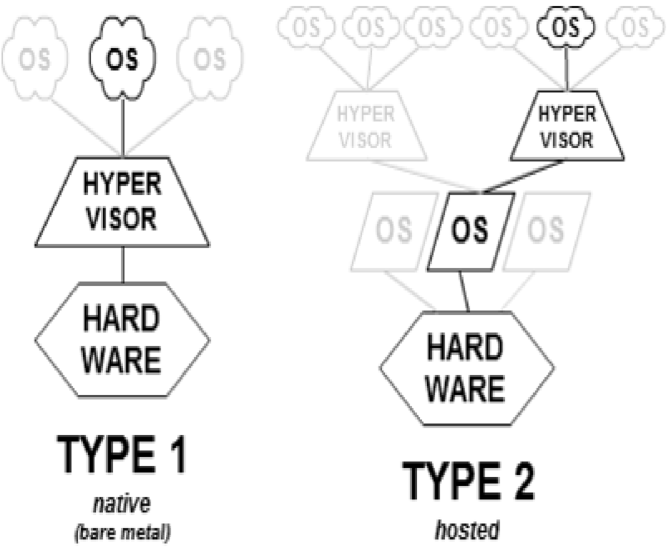

Figure 2. Type1 and Type 2 Hypervisors

- Class I Hypervisor (Native)

In Type I Hypervisor, the execution is carried out solely on the host system's hardware as the operating system [2]. Moreover, the resources are scheduled and allocated to the VMs by communicating directly with the host system. For instance, XEN and VMWare ESX.

- Class II Hypervisor (Hosted)

In type II Hypervisor, the execution is similar to other processes in the operating system of the host system [2]. In addition, the host system is also able to manipulate the virtual machines with the built in guest operating system. For instance, KVM, VMWare GSX and User Mode Linux.

C. Attacks related to Cloud Infrastructure

The attacks that are correlated to the security of the CSP are categorized into access control, cloud infrastructure, data, network and security standard [3]. The cloud infrastructure is defined as the intrusion to the internal infrastructure of the cloud computing at the virtualized environment. Moreover, the figure 3 summarizes the infrastructure of cloud computing. There are three main layer of cloud computing infrastructure, such as namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

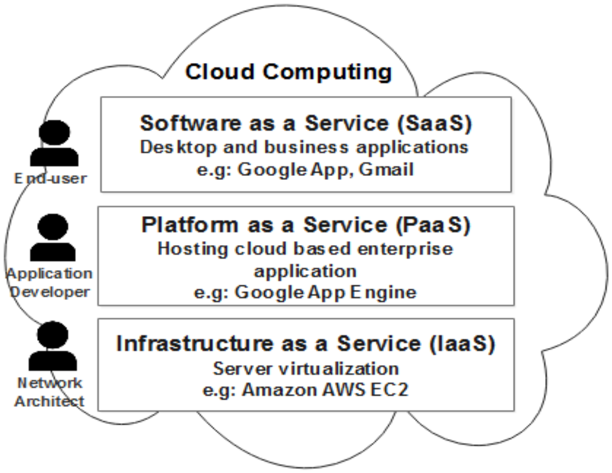
Cloud Computing
Software as a Service (SaaS)
Desktop and business applications
e.g: Google App, Gmail
End-user
Platform as a Service (PaaS)
Hosting cloud based enterprise application
e.g: Google App Engine
Application Developer
Infrastructure as a Service (IaaS)
Server virtualization
e.g: Amazon AWS EC2
Network Architect

Figure 3. Internal Cloud Computing Infrastructure

1) Attacks in IaaS layer

Infrastructure as a Service is the additional layer between hardware and Operating System in the cloud computing. It is built to support and strengthen the virtualization technology which is used by the hypervisor. Moreover, virtualization technology allows the administrative operations by permitting the creation of Application Programming Interface (API). As the number of hypervisors increase the number of attacks are also increased. This is because the exploitation of the channels and APIs to the cybercriminals also increased [4]. The VM Escape also may affect the IaaS layer.

2) Attacks in PaaS layer

Platform as a Service layer is a platform and obligates to protect both the programming framework and runtime engines from the cybercriminals. Hence, the encryption method is adopted in the PaaS layer to secure the users from any interference from the cybercriminals. Nevertheless, the multi-tenancy support has led to vulnerability. This is due to the fact that multi-tenancy enables numerous users from different platforms to use cloud computing at the same time. Therefore, the cybercriminals may disrupt the execution of the PaaS [4].

3) Attacks in SaaS layer

The SaaS layer provides services that extract data from multiple sources in the cloud computing. The example of the software is web application. [5] This has given the opportunity for the cybercriminals to create abnormal behavior of the cloud computing by inserting malicious script into the webpage. One of the prominent attacks in the SaaS layer is SQL injection. In the year of 2012, LinkedIn was being attacked by the hacker through the SQL injection attack. The information such as passwords had been possessed by the hacker and then published it into the password cracking forum. The victims have been increased up to 6.5 million. Therefore, the LinkedIn has confronted a $5 million lawsuit due to this issue [5].

D. Virtualization Attacks

One of the top cloud computing threats involves one of its core enabling technologies: virtualization. In virtual environments, the attacker can take control of virtual machines installed by compromising the lower layer hypervisor. It is noticeable that the Cloud Service Provider (CSP) is easily obtainable and this has beneficial for both cybercriminals and malevolent users. Hence, the presence of vulnerabilities in the CSP has leveraged the malevolent attacks. Without the virtualization, the multiple users to communicate and share the similar physical resources are merely impossible. Through the virtualization, the cloud users able to use various applications freely by conducting several useful functions such as migrate, roll back and more in the VMs [6].

In general, the virtualization attacks can be categorized in conventional/traditional attacks and virtualization precise attacks [7].

- Insider Virtualization Specific Attacks

The virtualization specific attacks can further divided into insider attacks and external attacks. The insider attack is defined as the malevolent users that equipped and misused their knowledge about the cloud system [8]. This has indirectly influence the confidentiality, integrity and availability of the CSP. Moreover, the malevolent users have trigged the severe threat to the CSP. Besides there are others insider attacks, namely the Communication between Virtual Machines and VM Escape.

- External Virtualization Specific Attacks

The external virtualization specific attacks is defined as any attacks that launched by both malicious cloud computing users and other external users who have possessed the unauthorized accessibility from the CSP [9]. It is observable that the methods of three notable external attacks such as Breakout attack, External Modification of Virtual Machines and Hypervisor attack.

E. Hypervisor Attacks

The Hypervisor Attack categorized as external attack is defined as the exploitation on the hypervisor’s vulnerabilities which allow the cybercriminal to possess the accessibility and authorization over the hypervisors [10]. Initially, the cybercriminals has launched the attack on particular virtual machine. Then, the malevolent virtual machine will conduct the trade-off with the hypervisor. Subsequently, the cybercriminals take the opportunity to proliferate the attacks on all the VMs that running under the compromised hypervisor. In the end, all virtual machines will be affected gradually under the compromised hypervisor. The famous of the hypervisor attacks are BluePill, DKSM and SubVirt.

III. Previous Work

A. Virtual Firewall

A virtual firewall (VF) is a network firewall service or appliance running entirely within a virtualized environment and which provides the usual packet filtering and monitoring provided via a physical network firewall.

In general, the destination IP, protocols and sources of the network packets are inspected by the virtual firewall whether pass or terminate their access. As a result, the transferred packets are either accepted or rejected after they are filtering and matching with their pre-determined procedures and policies. The virtual firewalls have the ability to implement the security policies which portable with virtual machines [11]. Additionally, in order to get the lower provision costs, the requirement of the specific hardware deployment is removed by the virtual firewall.

B. Intrusion Detection Types

There are countless Intrusion Detection Systems (IDS) that are available in the market. As the firewall do not guarantee to detect the malevolent attacks and protect for the security of the cloud computing. A research has proven that the IDS that are invented with the mixture of the series of machine learning methodologies is better efficiency compared to the single learning methodology. IDSs are software or hardware systems that realize intrusion detection, log detected information, alert or perform predefined procedures. An IDS is composed of several components [12]:

- Sensors which generate security events.
- Console to monitor events and alerts and control the sensors.
- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

Various types of IDS are Intrusion Detection and Preventing System (IDPS), Intrusion Detection System (Network based) (NIDS), Intrusion Detection System (Host Based) (HIDS), and Intrusion Detection System (Hypervisor Based).

- Intrusion Detection and Preventing System

For the early stage of various attacks discovery and to counteract from successful, IDPS is introduced as the essential tool to defend the attacks and other weaknesses. In addition, [13] have researched that the IDPS has offered an additional layer to against their failure behavior. Further it has explained, how the IDPS defends the

VM against VM-to-VM and breakout attack. In addition, Intrusion Detection and Prevention System (IDPS) are a hardware and software mechanisms that used to supervise network traffic and systems activities to recognize and protect against malicious activities.

- Network Based Intrusion Detection System (NIDS)

The Cloud Service Provider plays vital role in managing and organizing the NIDS. In common, the NIDS is installed on the network boundary that allows multiple virtual machines to be monitoring simultaneously [14].

- Host Based Intrusion Detection System

A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority. A HIDS can be thought of as an agent that monitors and analyzes whether anything or anyone, whether internal or external, has circumvented the system’s security policy.

- Hypervisor Based Intrusion Detection System

It is the main method that use to defend attack on hypervisor in cloud computing. The intangible layer between the hypervisor and guest of kernel is implemented by Hypervisor-based IDS. Kernel is being protected as this layer providing security. Hypervisor-based IDS observes the system metrics through cloud requests from the hypervisor and detect any possible misuse trends [15]. The communication between virtual machines, hypervisor and virtual machine, and virtual networking are being tracked and observed by Hypervisor-based IDS. This detection technique is operating inside the hypervisor and it could be effective in cloud.

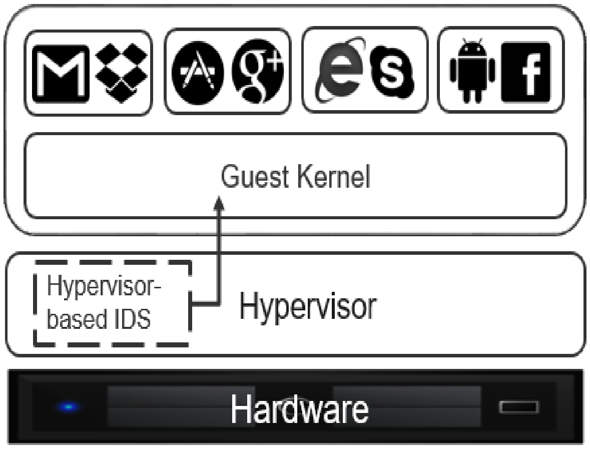

Figure 4. Hypervisor based IDS Architecture

IV. Proposed Solution

There are various available methods or systems are available in the market that specifically protect the cloud computing but most of them are used to protect cloud computing instead of the hypervisors. In order to develop an efficient tool that specifically defends the hypervisor attacks, in this paper the strength and weakness of above approaches are determined. From the existing tools for defending cloud computing like virtual firewall, Intrusion Detection and Prevention System, IDS (network based), IDS (host based), IDS (Hypervisor based) an effective solution is proposed to overcome the weakness. Thus Virtual Machines Hypervisor Intrusion Detection System (VMHIDS) is proposed.

Unlike Hypervisor-based IDS system, it is placed on the hypervisor and its' virtual machines to provide a more accurate detection of unsuspicious attacks. This approach protects both of the hypervisor and virtual machines from either insider or external attack on cloud environment. The continuous monitoring with VMHIDS from hypervisor or VMs enables to analyze real time events for automatic detect and block the malicious events. VMHIDS monitors and keep tracks on each file and process that communicate within the hypervisor in cloud computing. Besides, since VMHIDS is placed on both VMs and hypervisor, new attacks or suspicious attack on hypervisor can be detected easily for faster prevention. The system architecture of the VMHIDS is shown as the figure 5

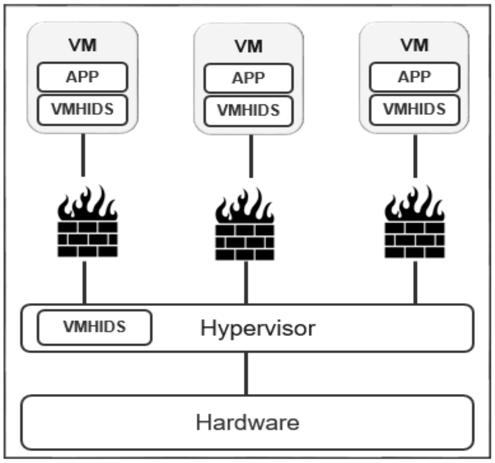

Figure 5. VM and Hypervisor IDS Architecture

It is understood that hypervisor attack is launched via internet. To be specific, it attacks on the packet delivered to the hypervisor. In that the case, the VMHIDS has adopted the anomaly-based detection concept to identify the malicious packets in real time by tracking and analyzing the network traffic. The internal implementation of the VMHIDS is constructed with eight interconnected components.

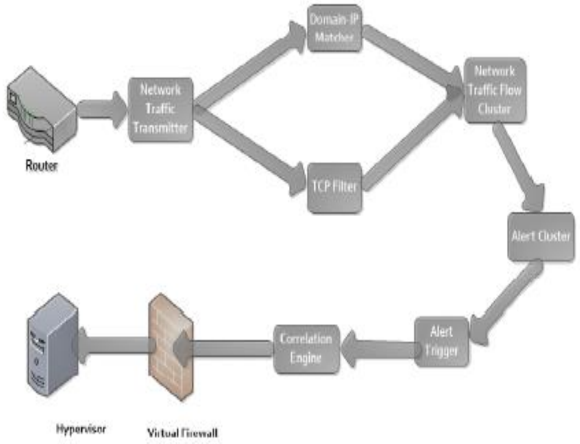

Figure 6. Internal Representation of VMHIDS

V. Conclusion

Thus, Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS) is proposed for protecting from the hypervisor attacks. It is followed that the hypervisor attack is categorized in the cloud infrastructure and external attack. In order to further extend the hypervisor attack, this paper also provides an overview of the attacks that related with cloud infrastructure. Consequently, there are five exiting approaches such as virtual firewall, Intrusion Detection and Prevention Systems (IDPS), Network based IDS, Hosted-based IDS and Hypervisor-based IDS are used to compare along with their strength and weakness. Hence, Virtual Machines Hypervisor Intrusion Detection System is proposed to conquer the weakness found in the existing systems.

VI. Future Scope

In the future, research should aim to provide new architectures, policies and techniques to maintain security on higher level for hypervisors. This kind of structured security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computing concept for industrial as well as future research farms. This paper also gives a strong theoretical concepts for security in order to build a more generalized architecture to prevent different kinds of attacks.

References:

[1] A. Riddle, and S. Chung, “A Survey on the Security of Hypervisors in Cloud Computing”, *2015 IEEE 35th International*

Conference on Distributed Computing Systems Workshops, 2015.

[2] Ajay Kumara M. A and Jaidhar C. D, “Hypervisor and Virtual Machine Dependent Intrusion Detection and Prevention System for Virtualized Cloud Environment”, *2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN)*, 2015

[3] O. Achbarou, M. Kiram and S. Bouanani, “Securing Cloud Computing From Different Attacks Using Intrusion Detection System”, *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 3, p. 61, 2016.

[4] G. Nenvani and H. Gupta, "A survey on attack detection on cloud using supervised learning techniques", *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016.

[5] P. Chouhan, F. Yao and S. Sezer, "Software as a service:Understanding security issues”, *2015 Science and Information Conference (SAI)*, 2015.

[6] Y. Han, J. Chan, T. Alpcan and C. Leckie, “Using Virtual Machine Allocation Policies to Defend against Co-resident Attacks in Cloud Computing” *IEEE Transactions on Dependable and Secure Computing*, pp. 1-14, 2015.

[7] L. Kwiat, C. Kamhoua, K. Kwiat, J. Tang and A. Martin, “Security-Aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach”, *2015 IEEE 8th International Conference on Cloud Computing*, 2015.

[8] I. Agrafiotis, J. Nurse, O. Buckley, P. Legg, S. Creese and M. Goldsmith, “Identifying attack patterns for insider threat detection”, *Computer Fraud & Security*, vol. 2, no. 7 pp. 9-17, 2015.

[9] J. Yeh, H. Hsiao and A. Pang, “Migrant Attack: A Multi-resource DoS Attack on Cloud Virtual Machine Migration Schemes”, *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, 2016

[10] J. Shi, Y. Yang and C. Tang, “Hardware assisted hypervisor introspection”, *SpringerPlus*, vol. 5, no. 1, 2016

[11] C. Modi and K. Acha, “Virtualization Layer Security Challenges and Intrusion Detection/ Prevention Systems In Cloud Computing: A Comprehensive Review”, *the Journal of Supercomputing*, 2016

[12] V. Marinova-Boncheva, “A short survey of intrusion detection systems,” Problems of Engineering Cybernetics and Robotics, vol. 58, pp. 23–30, 2007.

[13] J. Jabez and B. Muthukumar, “Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach”, *Procedia Computer Science*, vol. 48, pp. 338-346, 2015.

[14] W. Lin, S. Ke and C. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors", *Knowledge-Based Systems*, vol. 78, pp. 13-21, 2015

[15] S. Iqbal, M. Mat Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. Khan and K. Raymond Choo, “On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service”, *Journal of Network and Computer Applications*, vol. 74, pp. 98 –120, 2016.