Effective Way to Defend the Hypervisor Attacks in Cloud Computing

[1]Muhammad Shahid Dildar, [2]Nayeem Khan, [2]Johari Bin Abdullah, [2]Adnan Shahid Khan
[1]Faculty of Computer Science, King Khalid University (KKU), Community College, Khamis Mushayt, Saudi Arabia
[2]Faculty of Computer Science and I.T, University Malaysia Sarawak (UNIMAS), Kuching 94300, Sarawak, Malaysia
mdildar@kku.edu.sa, 15010049@siswa.unimas.my, ajorahi@unimas.my, skadnan@unimas.my

***Abstract*—Nowadays, the organizations are emphasizing on the security and resilient aspect of the cloud computing to protect the privacy and confidentiality of their data information. However, the hypervisor attack remains a hot issue by the cloud user even though enormous research have accomplished to inhibit the vulnerabilities in the virtualized cloud environment.Therefore, we have proposed the Virtual Machines and Hypervisor Intrusion Detection System, VMHIDS as our technique in detecting and preventing the hypervisor attacks in the virtualized cloud environment. The VMHIDS has adopted several features from the other techniques by inspecting the tasks frequently which then prevent suspicious event occur. Through the VMHIDS, the hypervisor attack is mitigated.**

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

I. INTRODUCTION

Nowadays, the popularity of the cloud computing trend is growing among the public, private and commercial domain. Cloud computing is distinct as to influence of information with a remote server, which hosted on the Internet in place of an electronic device or local server [1]. In the cloud computing, the similar resource is shared among numerous users that run their respective program in the virtualized system from the distinct virtual machines. This can be done by utilizing the hypervisor for virtualization, the core technology used in cloud computing architecture. Although, the cloud computing architecture also contains the computer utility and Service-Oriented Architecture (SOA).

Commonly, the cloud computing services facilitate the data, allocate the resources flexible, allow easy administration for the small size organization without professional IT technicians and minimize the hardware cost [1]. The characteristic of cloud computing such as service transparency and flexibility have triggered the interest most of the organization to adopt the cloud services over storing their data information externally. Nowadays, the organizations are emphasizing on the security aspect and resilient aspect to protect the privacy and confidentiality of their data information. Nevertheless, these characteristics also indirectly leveraged the malevolent attacks that are harmful to the security and privacy [2]. Although the enormous researches about the common manners of the various malware have done in order to prevent vulnerabilities in the cloud computing. And yet the hypervisor attack is still concern by the cloud users.

However, the current approaches for instance, Intrusion Detection System –Hypervisor-based (HICDS) on protecting the hypervisor attack do not adequately. This indirectly leads to the Cloud Service Provider (CSP) to face the security issues due to the vulnerability of the hypervisors. Once the hypervisor is compromised, the cybercriminals can easily and fully control over the entire cloud computing. It is important to note that the safety of the virtual machines are not assurance regardless how secure of the CSP when there is a vulnerability in its hypervisor.The weakness of the HIDS is the lack of effective functionalities that able to 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 core purpose of this article is to determine competent approaches for defending the hypervisor attacks in cloud computing. This paper is organized in this way. Part 2 illustrates the background for Cloud Service Providers, insider attack, external attack, Hypervisor Attack, and type of hypervisor. Part 3 presents prior work associated with the method of defending the hypervisor attack in cloud computing. Part 4 explains our proposed solution that is Virtual Machines and Hypervisor Intrusion Detection System (VMHIDS) and outline, its strength compared to the existing methods. Lastly, Part 5 concludes the article.

II. BACKGROUND

A) Cloud Computing

It can be visualized into frontend and backend as shown in Figure 1.According to [3], the frontend is whereby the authorized users can utilize the services offered by the cloud computing, namely the application, servers, networks and storage. Meanwhile, the hardware and software resources convey the cloud service in real time via the internet as shown in the backend of the cloud computing. There are numerous host systems used in the cloud

978-1-5090-5814-3/17/$31.00 ©2017 IEEE