Cloud Security Management Model based on mobile agents and web services interaction

Abir KHALDI1, Kamel KAROU1, Henda BEN GHEZALA1
1 RIADI Laboratory ENSI, University of Manouba, Manouba, Tunisia

Abstract - Security is one of the most important issue faced by the cloud adoption. Therefore, cloud actors such as customers, provider, business partners, and auditors are asking for major security controls and measures to be set in order to supervise and protect cloud assets and services. In fact, the security management is a very complex task specially in cloud environment because of its multi-layers services and multi-tenancy. In this paper, we propose a universal cloud security management model to cover all cloud services. This model is based on four phases: the perception, the detection, the reparation and the evaluation. The last phase offers a security assessment for each cloud service and also for cloud hypervisor to evaluate cloud service based on more than one security assessment indicator. The cloud security management model profits of the advantages of mobile agent and web service interaction.

Keywords: cloud security, SIEM, mobile agent, web service

1. Introduction

NIST [1] defines three cloud services models: Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Those cloud services may suffer from several vulnerabilities which are due to design, programming, or configuration errors. Such vulnerabilities can be exploited by malicious users to succeed their attacks [2][3][4].

In fact based on many studies [5][6][7][8][9], cloud adoption willingness was tightly related to security concerns. Therefore cloud services need to guarantee more security in order to sell better.

The idea of this work is to propose a universal cloud security management model for all cloud services model. This model collects and correlates cloud services event log to detect vulnerabilities and/or attacks in order to repair any anomaly detected. An evaluation step to assess cloud service security is an integrated part of this model. It gives more than one security assessment indicator to measure the cloud service security level. To ensure a dynamic model, we propose to introduce a smart autonomous mobile agent interacting with web service to correlate event log between different cloud assets and to automatically repair anomaly if detected.

The remainder of the paper is organized as follows. In Section 2, we give an overview of related work in cloud security management in the cloud. Section 3 presents the proposed cloud security management model. Furthermore, we define the different model components then we describe the four phases of the model. Finally, Section 5 concludes our paper and describes our future work.

2. Related Work

Many studies focus on the security management in the cloud environment, as a requirement for cloud business evolution.

In [10] an automated evaluation of cloud security mechanisms and their efficiency is proposed. The access control and the intrusion detection systems are the main objectives of this research. This approach concerns only the cloud infrastructure.

The Cloud Security Alliance (CSA) [11] professionals and researchers presented the concept of Security-as-a-Service (SECaaS) to cloud services. They developed a set of requirements, and discussed implementation considerations and concerns. However, the provided recommendations did not detailed a specific model covering all cloud services.

Niekerk et al [12] proposes a model to integrate traditional security solutions into a cloud infrastructure. In fact, their model presents a high level description and does not provide any details on the implementation and evaluation of the security in the cloud infrastructure, platform or software layer.

Hussain et al [13] introduced SECaaS using service oriented architecture (SOA) to allow cloud customers to have more control over hosted services. A user-centric approach was employed to allow users to choose security services and monitor the status of their applications and data in the cloud environment. However, their architecture is only focusing on the access control settings and some security settings in the chosen cloud service model (IaaS, PaaS, or SaaS).

In [14], the authors studied security controls recommended by standards such as ISO/IEC 27001 and NIST SP 800-35. They noticed that 30% of the controls can be automated. They introduced a security information and event management (SIEM) framework to automate these security controls in this work. But, they did not consider the application of their framework on the multi-layer/multi-tenancy architecture of a cloud computing environment.
3. Proposed Cloud Security Management Model (CSMM)

In this section we present the CSMM components and we describe the different CSMM phases as shown in figure 1.

3.1 CSMM components

The CSMM is composed of 4 principal components:

- Sensors: The CSMM exploit sensors outputs to recognize what can occur in different cloud services models (IaaS/PaaS/SaaS). We deploy two types of sensors:
  - Service Sensors: sensors deployed in different cloud service (SaaS, PaaS, IaaS) can be a log manager, an IDS/IPS, Web application Firewall (WAF), etc.
  - Hypervisor Sensors: The hypervisor is a critical component for cloud environment. Hypervisor sensor can be a log manager sensor to collect all VMs events and/or an NIDS/NIPS to detect and/or to prevent cloud attacks.

- Mobile agent (MA) [15]: it is a smart mobile code which can migrate with a base rules to detect and repair cloud anomalies (vulnerabilities, attacks).
- Web service (WS) [16]: it is the intermediate between sensors outputs databases and the mobile agent. Mobile agent and web service interaction [17] helps to secure cloud assets and ensure a rapid and interoperable communication.
- Cloud actors: it can be a cloud customer or a cloud provider involved in the cloud security management model.

3.2 CSMM phases

The CSMM is based on four phases:

- **Phase 1** is the Perception phase. It constitutes the first step of the cloud SIEM (Security Information and Event Management). This step named SIELD (A Security Information and event log and database) considers the events and logs database (ELD) as a repository for all events and logs sent by the different cloud sensors. It is updated in real time and has a mirrored ELD backup as a contingency in case of failure.

- **Phase 2** is the Detection. It is composed of:
  - A Security Information and event Correlation (SIEC) module: The correlation is a key step as it is used to detect events not previously noticed. It uses the information stored in the SIELD in order to provide meaningful results. The correlation results are evaluated to identify relationships and detect threats.
  - A Security Information and event knowledge base (SIEKB) module: The knowledge base (KB) is an online known threat centralized repository for cloud customer infrastructure, platforms and software services. It contains symptoms that match certain event(s) along with the recommended counter measures and/or responses.
  - A Security Information and event Analysis (SIEA) module: The security information and event analysis (SIEA) module allows cloud security analysts to perform advanced research on events. Some events need further explanation and investigation to provide additional details.

The cloud reports are XML documents which contains the results of the Cloud SIEM. We create a cloud report for each cloud service and an hypervisor cloud report. Based on the cloud reports, we can detect if there is any vulnerabilities and/or attacks that should be repaired. In a previous work [18], we design a framework to detect a distributed cloud attacks in hybrid cloud based on MA/WS interaction.

- **Phase 3** is the Reparation. In fact, we propose two solutions to repair an existing anomaly: if the anomaly and its repair mode is known by the mobile agent, it can be automatically repaired. If it is not, the cloud provider and/or the cloud customer should decide and act to resolve problem. When the anomaly is repaired, it should be mentioned in the cloud report. A load balancing technique is proposed in our
previous work [19] to improve cloud services availability in cloud environment.

**Phase 4** is the Evaluation. We exploit the cloud reports results to assess cloud security service. Therefore we will adopt the chen’s et al [17] threat evaluation model for cloud service. After evaluation, the security assessment can help cloud actors to decide to make more security controls in their cloud services.

4. **Summary and Future Work**

In this work, we propose a universal CSMM to enhance security in cloud environment. The use of mobile agent instead of client/server model decreases the cloud traffic and distributes the processing charge between virtual machines. It gives CSMM an autonomous and dynamic aspect by repairing anomaly automatically within the smart mobile agent. In the next work, we are going to develop the evaluation phase by proposing a quantitative approach to measure the cloud security situational awareness.

5. **References**


