Indian Journal of Science and Technology, *Vol 10(18), DOI: 10.17485/ijst/2017/v10i18/109044, May 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Cloud Security: A Multi Agent Approach Based Intrusion Detection System

Omar Achbarou, My Ahmed El Kiram and Salim Elbouanani

Department of Computer Science, Cadi Ayyad University, Marrakech, Morocco; Omar.achbarou@gmail.com, Kiram@uca.ma, elbouanani.salim@gmail.com

Abstract

The security is the biggest problem of cloud computing, it needs some Intrusion Detection Systems (IDSs) for detecting and preventing attacks in this environment. Multi Agents Systems (MAS) are distributed systems ideally designed and implanted as a set of agents interacting to solve issues that may exceed the capabilities of each individual agent. This approach provides an intelligent self-administered and fault-tolerant intrusion detection system with continuous execution time and minimal human intervention due to the use of Multi agent security systems has been monitored and automatically controlled in the cloud.

Keywords: Attack, Cloud Computing, Intrusion Detection System, Multi Agents Systems, Mobile Agent, Security

1. Introduction

Cloud computing is internet based where shared resources; software and information are provided to computers and other devices on-demand.

The National Institute of Standards and Technology (NIST) cited five main characteristics of cloud[1]: on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service. It also determinate three service models (infrastructure, platform, and software), and four deployment models (public, private, community and hybrid) that together categorize ways to deliver cloud services.

Figure 1 shows cloud deployment models together with their internal infrastructure (Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)), and the essential characteristics of this environment[2].

1.1 SaaS

To use provider software running on a cloud infrastructure and accessed from various client devices via a client interface.

1.2 PaaS

To provide a platform allowing customers to run, develop, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

1.3 IaaS

The most basic cloud-service model is that of providers offering computing infrastructure, machines and other resources.

Despite the enormous technical and business benefits of cloud, concern for security and privacy has been one of the main obstacles that impede its widespread.

In this work, we classify security problems and attacks of cloud computing environments such as Flooding Attack, Denial of Service (DoS) attacks, Side Channel Attacks, phishing, malware Cloud Injection Attacks. Intrusion Detection Systems (IDSs) are traditional solutions in the network and in the cloud to resist these attacks. IDS can detect suspicious activity by monitoring changes in network traffic, log files, system configuration, and end-user actions. When IDS is detected a suspicious

*Author for correspondence

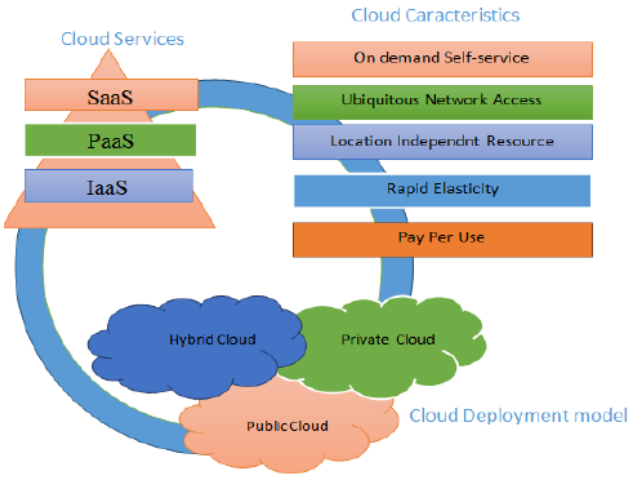

Figure 1. Cloud deployment models, characteristics, and infrastructures.

event, it sends an alert message to a monitoring console to initiate some actions to block these attacks.

IDSs are not easily adaptable to dynamic cloud environments or to the increasing complexity of user behavior. Which is why we need is a security management solution that is flexible to adapt to change and the complex evolution of cloud environments. In the perspective of a conception capable of managing the security system, particularly the detection of intrusions in existing cloud environments, we propose an IDS based on Multi agent approach to detect and prevent attacks and malicious in cloud computing.

In proposed "Multi agent approach based intrusion detection system" has designed different seven agents on for both mode (Host, Network) and actions are runs independently. These agents communicate with each other to check and prevent all malicious and attacks using message passing, technically termed as Agent Communication Language (ACL).

2. Attacks Related to the Cloud Security Categories

In what follows, we present a list of attacks on cloud. We briefly explain each attack and accompanied by a brief discussion. Table 1 presents a summary of attack names and attack category[3].

2.1 DoS Attacks

A DoS attack can render the services assigned to cloud users unavailable. Sometimes, when you try to access a service, we see that due to the server overloading with requests for access to this service, we cannot access the service and observe an error. This occurs when the number of requests that can be processed by a server exceeds its capacity[4].

Also, the attacker doesn't have to flood all cloud infrastructure, just simply can flood a single machine in order to realize a full loss of availability on the planned service[5].

Table 1. Known attacks on clouds

Attack name	Category
Flooding attack	Cloud Infrastructure
Attacks on Virtual Machine (VM) or hypervisor	Cloud Infrastructure
DoS	Network, cloud Infrastructure
Cloud Malware Injection Attack	Cloud Infrastructure, Access
Port Scanning	Network
Man-In-The-Middle Attack	Network, Access Control, data
Cross VM side channels	cloud Infrastructure
Phishing	cloud Infrastructure, Network, Access

2.2 Port Scanning

Port scanning is a technique used to search for open ports on a cloud environment. This technique is used by attackers to try to find flaws in computer systems. In the scenario of Cloud, the attacker can attack the services available through the scanning of ports[6].

2.3 Malware Injection Attacks

When data is transferred between the cloud provider and the user, the attacker can introduce malicious code between the two actors.

Cloud malware injection is the attack that can inject an application, malicious service, or even virtual machine into the cloud system according to service models such as IaaS, SaaS or PaaS[7].

Then, the attacker has to deceive the Cloud environment in order that, it use the new service implementation instance like one of the valid instances for the particular service attacked by the attacker. When this succeeds, the Cloud automatically redirects valid user requests to the malicious service implementation, and the attacker starts to execute his own code[8].

2.4 Attacks on Virtual Machine (VM) or Hypervisor

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. New vulnerabilities, such as zero-day vulnerability found in Virtual Machines (VM) that attracts an attacker access to the hypervisor or other VMs installed. The zero-day vulnerability has been exploited in the application virtualization Hyper VM which resulted in the destruction of many websites based on the virtual server[8].

2.5 Side Channel Attacks

In a cloud, the attacker runs a virtual machine instance on the same physical server in the victim's virtual machine and uses a shared physical component (for example, the processor cache) to retrieve the value of a virtual machine, A cryptographic key by observing the activity of the processor cache[9].

2.6 Phishing Attacks

In cloud computing, phishing attacks can be classified into two types of threats: the first, like an abusive behavior in which an attacker hosts a phishing attack site on cloud by using one of the cloud services (Paas, Iaas or SaaS) and second hijack accounts and services in the cloud through traditional social engineering techniques[10].

2.7 Man-In-The-Middle Cryptographic Attacks

In this case, an attacker placed between two parties in a cloud environment. Anytime attackers can be placed in the communication path, there is the possibility that they can change and intercept communications[11].

3. Intrusion Detection System

As detailed in previous section, there are different types of attacks in cloud environment. IDS are effective solution to detect and resist these attacks. IDSs are software or hardware systems that realize intrusion detection, log detected information, alert or perform predefined procedures[12,13]. They can be either hardware or software that includes whole observed computing entities[14].

An IDS system contains the following components:

- Sensors for generating security alerts
- Component to control the sensors and monitor events.
- Central component that saves events logged by the sensors in a database and uses a system of rules to generate alerts from security events received

Currently there are two types of IDS in cloud environment: Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS).

3.1 Host-Based IDSs

H-IDS is a system that monitors a cloud computing for the purpose of detecting an intrusion or attack and responds by logging activity and notifying the cloud user. A HIDS can be considered as an agent system that monitors and analyzes the environment to detect malware and attacks[15].

3.2 Network Based IDSs

NIDS monitor, analysis the specified and pre-identified network traffic. These systems play a big role to detect network attacks in cloud environment[16]. A NIDS is a system that attempts to will monitor network packets and deny or accept them based on the predefined rules.

4. Multi Agent System Concepts

Multi agent system has a group of intelligent agents interacting with the environment and with them. An agent is a computer system located in an environment that acts autonomously and flexibly to achieve the objectives for which it was designed (Figure 2).

Agents can be described with different characteristics[17]:

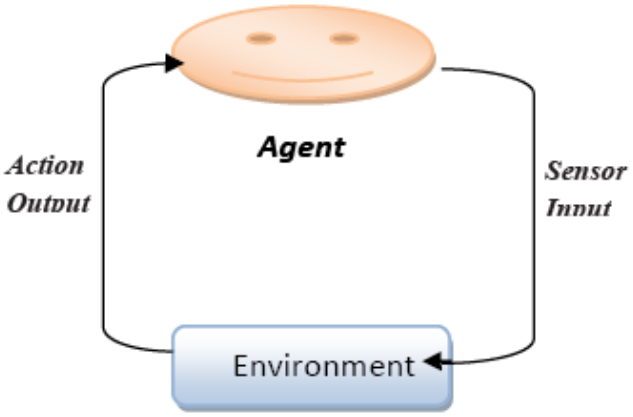

Figure 2. An agent in its environment.

4.1 Flexibility

The agent is able to carry out actions in an autonomous and reflexive way In order to achieve the objectives set for it. Flexibility in this case means reactivity and pro-activity.

4.2 Autonomous

The agent is able to act without any intervention, that is to say, the agent decides himself which action to undertake among those that are possible.

4.3 Social

The agent must be able to interact with other agents when the situation so requires to complete his tasks or to help these agents perform their tasks.

Multi-agent organizes message passing or shared memory techniques using ACL and transmits messages and protocol using QML "Knowledge Query and Manipulation Language" (Figure 3.)

Recently, many researchers have proposed multi-agent models combined with mobile computing environments using knowledge base that contains context information including social data and user's location information[18].

5. Multi agent Approach Based Intrusion Detection System

IDSs are not easily adaptable to dynamic cloud environments or to the increasing complexity of user behavior. Which is why we need is a security management solution that is flexible to adapt to change and the complex evolution of cloud environments. In the perspective of a conception capable of managing the security system, particularly the

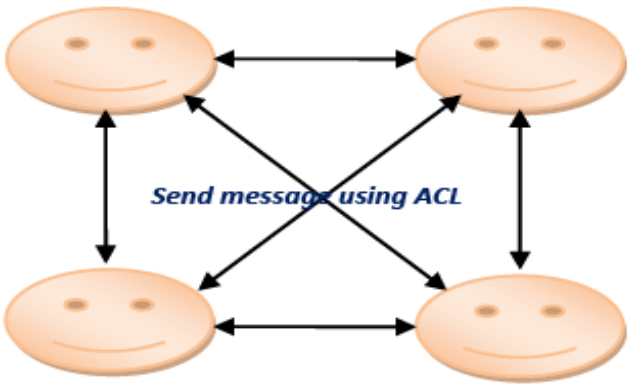

Figure 3. Distributed architecture of MAS.

detection of intrusions in existing cloud environments, we propose an IDS based on Multi Agent approach to detect and block all attacks in cloud computing.

The general architecture of our system is illustrated in Figure 4 and is structured around three main interacting layers and seven agents interact in our approach.

The rule of Interface Agent is to sniffing the flows of network traffic. For sniffing various types of traffic like TCP, UDP, IP, ICMP, ARP in this proposed system have developed for specific agents to sniff specific types of flows). For sniffing they have communicate with Monitor Agent.

Monitor Agent: can analyze packets received and sent to the Analyzer agent. Monitor agent is a dispatcher between mediation layer and control layer.

Monitor Agent: collects information, and finally sends or carries back the result to Analyzer Agent. Consequently, Analyzer Agent will analyze the coming information, and sends the result to the Rule Agent, the latter compare and match with intrusion patterns in IDS Rule Set, Also update the IDS database to alert more attacks, if any deviation found it generates signal and send signal to Supervisor Agent.

Supervisor Agent: It has two different types of agent the first is intrusion detection agent and second is intrusion prevention agent.

Intrusion Detection Agent is an intelligent IDS that can detect two signals, one of which is known Intrusion and another Intrusion unknown. These signals signal the system by an intrusion detection agent. This Agent generates a report of information classified at category as we have already quoted for the cloud user. And send other comprehensive expert advisory report for the cloud provider.

Intrusion Prevention Agent: This Agent performs some preventive services like blocking of suspicious IP address to reach to the target host. And Drop All packets received from that attacker IP.

5.1 Discussion

IDSs are not easily adaptable to dynamic cloud environments or to the increasing complexity of user behavior. That is why we propose an Intrusion Detection system based on Multi agent system to detect and prevent all attacks in cloud environment. For ensure a high level of trust in cloud computing, we propose a new approach based on cooperative of IDS and Multi agent system.

This approach provides an intelligent self-administered and fault-tolerant intrusion detection system with

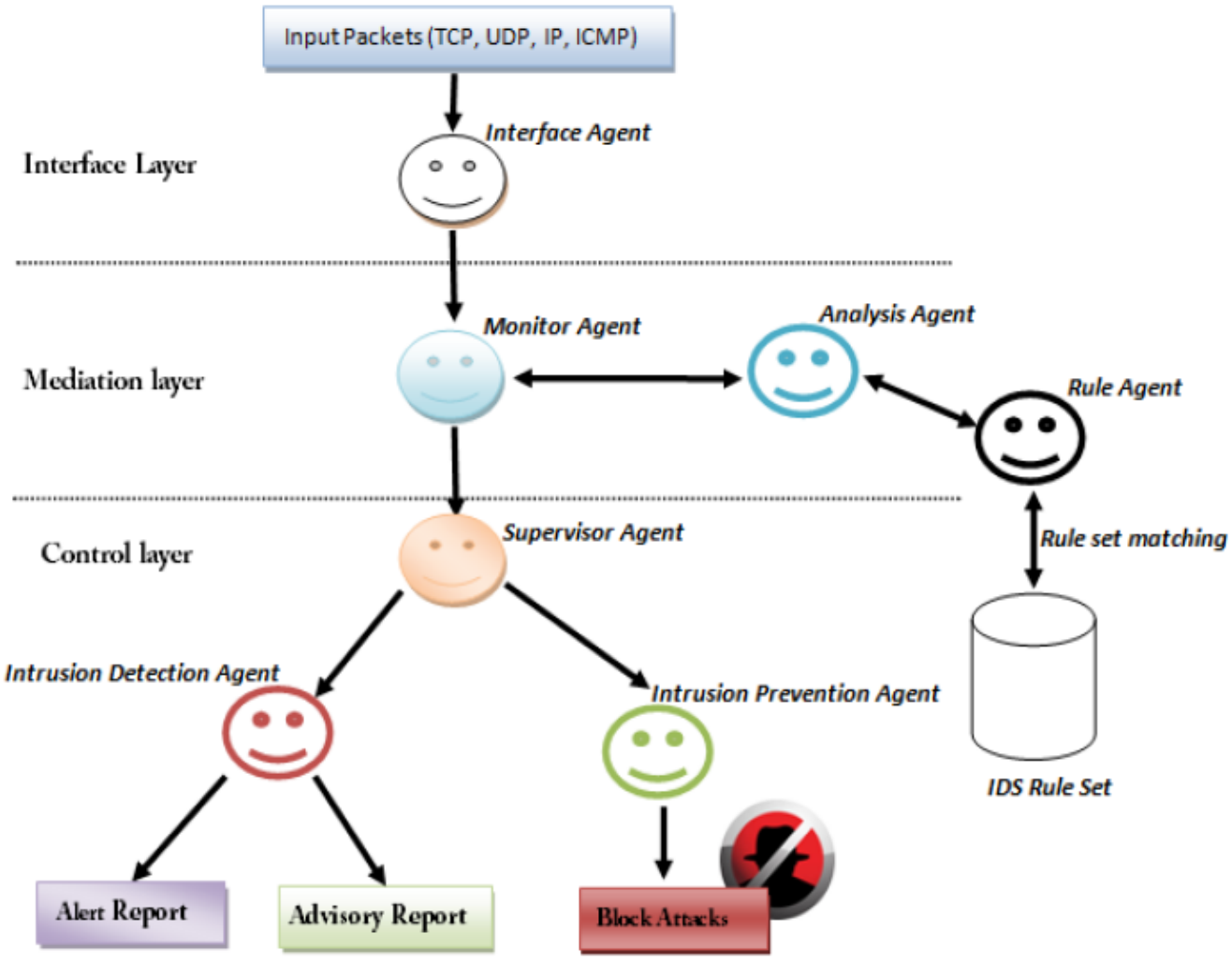

Figure 4. Architecture of our proposed approach.

continuous execution time and minimal human intervention due to the use of Multi agent security systems has been monitored and automatically controlled in the cloud environment.

The advantage of the proposed architecture is that it uses mobile agents as a communication entity. The aim here is to reduce the traffic on the network and to reduce the amount of information exchanged.

6. Conclusions and Future Work

Cloud Computing is at the keen interest and numerous works has been published in this field.

There is a major need of bringing security, transparency and reliability in cloud environment for client satisfaction. Then, one of the security issues is how to reduce the impact of any type of intrusion in this environment. Thus this paper has proposed an intelligent approach, which is based on the collaboration of IDS systems, and Multi agent Systems. It has designed different seven agents on for both mode (Host, Network) and working and operations are runs independently and communicate with each other to check and identify all malicious in cloud computing.

This approach provides an intelligent self-administered and fault-tolerant intrusion detection system with continuous execution time and minimal human intervention through the use of multi-agent security systems has been monitored and automatically controlled in the cloud environment.

Further research can be undertaken to improve the work presented. The future directives are:

1. We will continue to deepen the concepts and the notions of this approach and to proceed after to its implementation in order to validate it.
2. We will concentrate on the techniques of implementation of this approach, like Java Agent Development framework (JADE) which allows the development of systems Multi-agents in cloud environment.

7. References

1. National Institute of standards and technology. Final version of NIST cloud computing definition published [Internet]. 2011 [updated 2016 Sep 21; cited 2011 Oct 25]. Available from: Crossref
2. Bellifemine F, Caire G, Greenwood D. Developing multi-agent systems with JADE. Wiley Online Library; 2007 Feb 20. p. 1–286. Crossref
3. Khalil I, Khreishah A, Azeem M. Cloud computing security: a survey. Multidisciplinary Digital Publishing Institute, Computers. 2014 Feb 3; 3(1):1–35. Crossref
4. Peng T, Leckie C, Ramamohanarao K. Information sharing for distributed intrusion detection systems. Journal of Network and Computer Applications, Elsevier, ScienceDirect. 2007 Aug; 30(3):877–99. Crossref
5. Marinova-Boncheva V. A short survey of intrusion detection systems. Problems of Engineering Cybernetics and Robotics. 2007; 58:23–30.
6. Vieira K, Schulter A, Westphall C, Westphall CM. Intrusion detection for grid and cloud computing. Institute of Electrical and Electronics Engineers (IEEE) IT Professional. 2010 Jul–Aug; 12(4):38–43. Crossref
7. Kantamneni A, Brown LE, Parker G, Weaver WW. Survey of multi-agent systems for microgrid control. Engineering Applications of Artificial Intelligence, Elsevier, ScienceDirect. 2015 Oct; 45:192–203. Crossref
8. Yoon H, Lee M, Gatton TM. A multi-agent based user context Bayesian neural network analysis system. Artificial Intelligence Review. 2010 Oct; 34(3):261–70. Crossref
9. Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications. 2013 Jan; 36(1):42–57. Crossref
10. Bhadauria R, Chaki R, Chaki N, Sanyal S. A survey on security issues in cloud computing. Computer Science, Cryptography and Security. 2011 Sep 25; 5(6):83–7. Crossref
11. Singh A, Shrivastava M. Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT). 2012 Apr; 4(1):321–3. Crossref
12. Sqalli MH, Al-Haidari F, Salah K. EDoS-shield - a two-steps mitigation technique against EDoS attacks in cloud computing. In the Proceedings of the 4th Institute of Electrical and Electronics Engineers (IEEE) International Conference on Utility and Cloud Computing ; 2011 Dec 5–8. p. 49–56.
13. Balasubramanian R, Aramuthan M. Security problems and possible security approaches in cloud computing. International Journal of Scientific and Engineering Research. 2012 Jun; 3(6):1–4.
14. Lee J-H, Park M-W, Eom J-H, Chung T-M. Multi-level Intrusion Detection System and log management in Cloud Computing. Institute of Electrical and Electronics Engineers (IEEE) 13th International Conference on Advanced Communication Technology (ICACT), Seoul, South Korea; 2011 Feb 13–16. p. 552–5.
15. Gruschka N, Jensen M. Attack surfaces: a taxonomy for attacks on cloud services. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 3rd International Conference on Cloud Computing, Miami, USA; 2010 Jul 5–10. p. 276–9. Crossref
16. Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. Institute of Electrical and Electronics Engineers (IEEE) International Conference on Cloud Computing; 2009 Sep 21–25. p. 109–16. Crossref
17. Gunasekhar T, Rao KT, Saikiran P, Lakshmi PV.A survey on solutions to distributed denial of service attacks. International Journal of Computer Science and Information Technology (IJCSIT). 2014; 5(2):2373–6.
18. Navaz ASS, Sangeetha V, Prabhadevi C. Entropy based anomaly detection system to prevent DDoS attacks in cloud. International Journal of Computer Applications. 2013 Aug; 62(15):42–7.