Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems

Omar Achbarou, My Ahmed El kiram, and Salim El Bouanani

Dept. of Computer Science, Cadi Ayyad Univesity (UCAM), Morocco

***Abstract* — Cloud computing is a new way of integrating a set of old technologies to implement a new paradigm that creates an avenue for users to have access to shared and configurable resources through internet on-demand. This system has many common characteristics with distributed systems, hence, the cloud computing also uses the features of networking. Thus the security is the biggest issue of this system, because the services of cloud computing is based on the sharing. Thus, a cloud computing environment requires some intrusion detection systems (IDSs) for protecting each machine against attacks. The aim of this work is to present a classification of attacks threatening the availability, confidentiality and integrity of cloud resources and services. Furthermore, we provide literature review of attacks related to the identified categories. Additionally, this paper also introduces related intrusion detection models to identify and prevent these types of attacks.**

***Keywords* — Cloud Computing, Cloud Security, Threats, Attacks on Cloud, Intrusion Detection System (IDS)**

I. Introduction

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

The National Institute of Standards and Technology (NIST) defined five characteristics of cloud computing [1]: on-demand self-service, rapid elasticity or expansion, broad network access, resource pooling, and measured service. It also defined three “service models” (software, platform and infrastructure), and four “deployment models” (private, community, public 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.

Despite the enormous technical and business benefits of cloud computing, 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. To prevent these attackers, Intrusion Detection Systems (IDSs) are effective solutions to resist them. IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks.

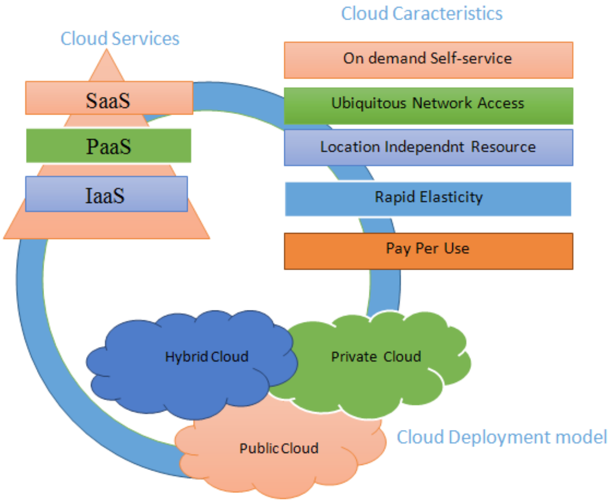

Fig. 1. Cloud deployment models, Characteristics, and infrastructures

The remainder of this paper is structured as follows. The next section presents the main categories of cloud computing security. In Section 3, we present description of the well known attacks affecting cloud computing. Intrusion detection Systems and our types are detailed in section 4. The section 5 presents our proposed model to detect, classify and resist these types of attacks. And the last section summarizes the main contribution of this work and details our perspectives.

II. Categories of Cloud Security

As part of this work, we started an investigation into the security issues and attacks on cloud computing. Cloud computing also suffers from various traditional attacks such as Flooding Attack, Side Channel Attack, port scanning, denial of service (DoS), Distributed Denial of Service (DDoS) etc. We classify these attacks and problems related to the security of cloud computing in five categories, which are summarized in Table 1 [2]:

TABLE I. CLOUD SECURITY CATEGORIES.

Category	Description
Security Standards	Describes the standards required to take precaution measures in cloud computing in order to prevent attacks.
Network	Included network attacks such as denial of service (DoS), DDoS, etc.
Access Control	Included identification, authentication and authorization attacks.
Cloud Infrastructure	Includes attacks each layer of the cloud as SaaS, PaaS and IaaS, it is particularly associated with the virtualization environment.
Data	Covers data related security issues including data migration, integrity, confidentiality, and data warehousing.

DOI: 10.9781/ijimai.2017.439

In addition to identifying cloud security issues and classifying them into several categories, we have identified dependencies among these categories and the security issues they encompass. If one of the categories is prone to certain attacks, other categories may also become prone to these attacks.

III. 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 of the consequences of the attacks in the cloud environment. Table 2 presents a summary of attack names and attack category [2] [7] [9].

A. *Denial of Service Attacks*

A DoS attack is an attempt to make the affected services unavailable to the authorized users In such an attack, the server providing the service is flooded with a large number of applications and therefore the service becomes unavailable for the authorized user. Sometimes when you try to access a website, we see that due to overload, the server with the website is inaccessible and we observe an error message. This occurs when the number of requests that can be processed by a server exceeds its capacity [4].

Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [5].

TABLE II. KNOWN ATTACKS ON CLOUDS.

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

B. *Port Scanning*

An attack that identifies open, closed and filtered ports on a system in cloud environment [3]. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. In the scenario of Cloud, the attacker can attack the services available through the scanning of ports (discovering open ports on which these services are provided) [10].

C. *Malware Injection Attacks*

In the cloud computing, a lot of data is transferred between the cloud provider and the consumer; it is necessary user authentication and authorization [5]. When data is transferred between the cloud provider and the user, the attacker can introduce malicious code between the two actors.

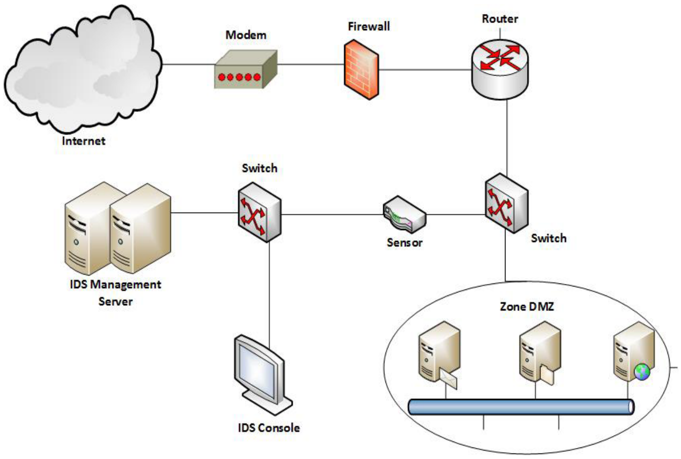

Fig. 2. Network-based Intrusion Detection System architecture

This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed [7].

D. *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 attract an attacker access to the hypervisor or other VMs installed. The zero-day vulnerability has been exploited in the application virtualization HyperVM which resulted in the destruction of many websites based on the virtual server [3].

E. *Side Channel Attacks*

These attacks exploit the physical properties of materials to gather information that may give a diagram or pattern of the system to attack. The fact that multiple virtual machines share the same hardware side channel attack makes it relatively easy to achieve. Without implementation of the safety device in the hardware, equipment sharing is dangerous [2].

In cloud computing environments, it is possible to map the infrastructure and identify where the virtual machine resides. It is then possible to instantiate new VMs until one is placed in co-residence with the target VM. After being instantiated, VM attacker can retrieve sensitive data from the legitimate VM attacked. This is a side channel attack-type [16].

F. *Phishing Attacks*

In cloud computing, phishing attacks can be classified into two categories of threats: first, as an abusive behavior in which an attacker hosts a phishing attack site on cloud by using one of the cloud services and second hijack accounts and services in the cloud through traditional social engineering techniques [8].

G. *Man-In-The-Middle Cryptographic Attacks*

This attack is performed when an attacker placed between two users in a cloud environment. Anytime attackers can be placed in the communication path, there is the possibility that they can intercept and change communications [9].

IV. Intrusion Detection System

As detailed in previous section, there are different types of attacks in cloud environment. Intrusion Detection Systems (IDS) are effective solutions to detect and resist these attacks. IDSs are software or hardware systems that realize intrusion detection, log detected information, alert or perform predefined procedures [11, 12].

An IDS is composed of several components [13]:

- 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.

Mainly there are two types of IDS in cloud computing systems: Host based IDS (HIDS) and Network based IDS (NIDS).

A. Host-based Intrusion Detection Systems

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 [14].

B. Network based Intrusion Detection Systems

Network-based IDS (NIDS) observe, monitor and analyses the specified and pre-identified network traffic. It can detect different situations based on specified points and generally located between the end point devices like routers, firewalls. A NIDS is an intrusion detection system that attempts to discover unauthorized access to a network by analyzing traffic on the network for signs of malicious activities and events. An example for NIDS architecture and sensor placement is shown in Figure 3 [15].

V. Proposed Work

A. Work

Our proposed model in Figure 3 is a resourceful Cloud IDS which can use a lot of technics to pick up IDS security performance over the Cloud computing. IDS use sensors to check for malicious customer data packets. Initially, the firewall blocks packets from invalid users, otherwise it shipments to the IDS component should analyze them based on predefined rules. The rules are defined based on well known attack strategies by the intruders, it can check the identity of the packets

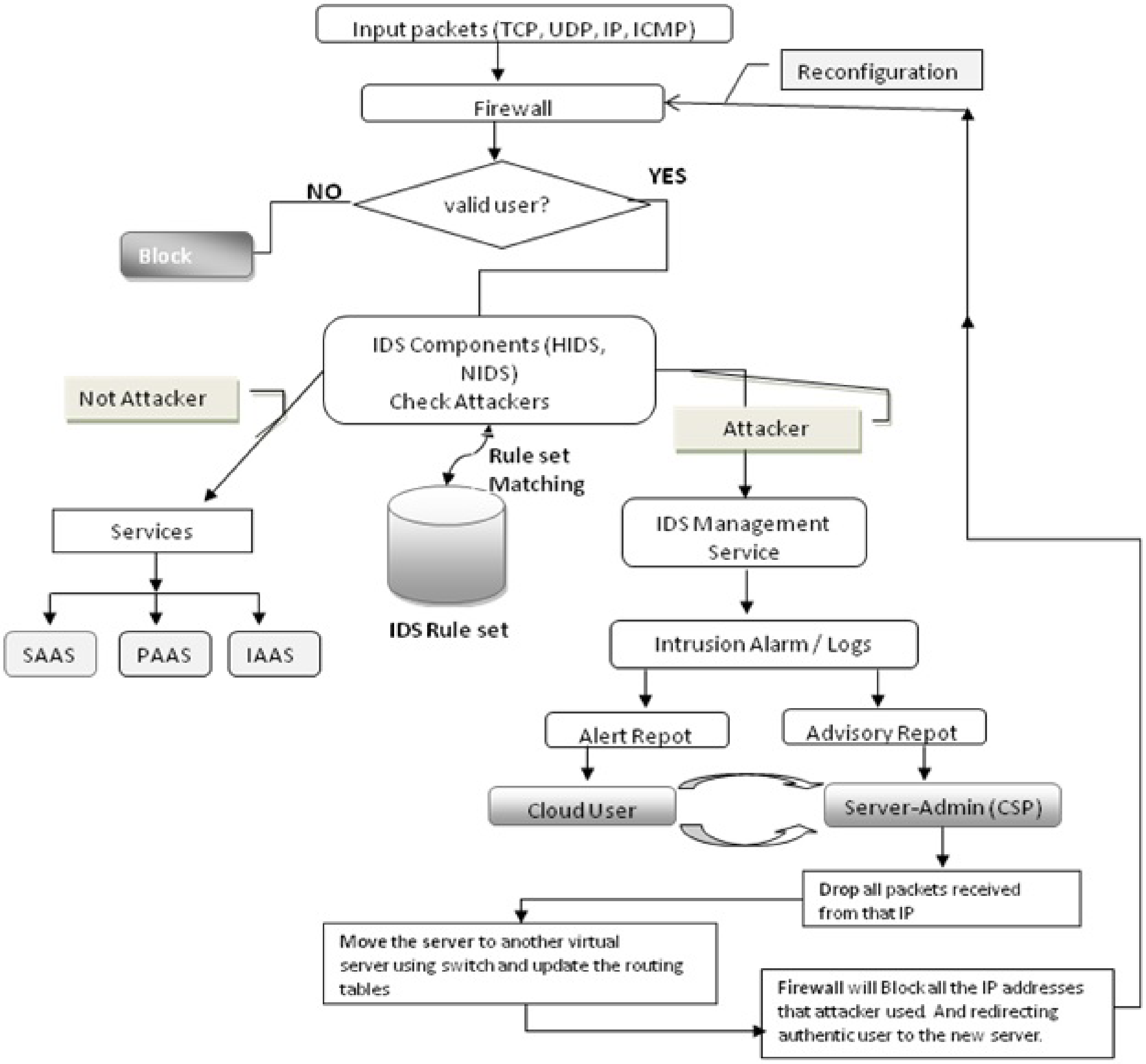
Input packets (TCP, UDP, IP, ICMP)
Reconfiguration
Firewall
NO
valid user?
YES
Block
IDS Components (HIDS, NIDS)
Check Attackers
Not Attacker
Attacker
Rule set
Matching
Services
IDS Rule set
IDS Management Service
SAAS
PAAS
IAAS
Intrusion Alarm / Logs
Alert Repot
Advisory Repot
Cloud User
Server-Admin (CSP)
Drop all packets received from that IP
Move the server to another virtual server using switch and update the routing tables
Firewall will Block all the IP addresses that attacker used. And redirecting authentic user to the new server.

Fig. 3. Proposed IDS Model

if it comes from a pirate, it redirects to the IDS management service that can provide instant reports on the cloud user with an advisory report for the cloud service provider. If it is not from a pirate sends them to the cloud services.

Alerts logs are easily communicated to the user of the Cloud with an expert opinion for the cloud service provider (CSP). The server-admin on examining the security risks involved performs emergency response to the attack by identifying the source IP addresses involved in the attack could automatically generate the access lists that would drop all the packets received from that IP. If the attack type is DDoS attack, the botnet formed by all the zombie machines are blocked. The server-admin then responds to the attack by transferring the targeted applications to virtual machines hosted in another datacenter. Router automation would immediately re-route operational network links to the new location. Hence, the firewall located at the new server will block all the IP addresses that attacker used and if any genuine user is trying to connect to the server, he will be redirected to the new server.

Our model is always dynamic because there are still several days to put launched by this model such as firewall reconfiguration to block new attacker. Also update the IDS database to alert more attacks. So our model is complete to detect such kind of attack.

To manage a large number of data flow packets in such an environment IDS Approach proposed in this paper. IDS able to process huge amount of data and may reduce packet loss. After effective treatment of IDS alerts watched proposed move to a monitoring service by third parties, who in turn informs the cloud directly to users about their system under attack. Figure 3 shows the proposed IDS model. The user cloud access its data on remote servers to the service provider site on the cloud network. Applications and user actions are monitored and recorded by IDS. Alerts logs are easily communicated to the user with a cloud expert advice from cloud service provider.

B. *Advantages of proposed model*

1. High volume of data in cloud environment could be handled by a single node IDS through a multi-threaded approach.
2. Classify the attack to generate well organized alert Report.
3. Being at a central point, proposed Cloud IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach.
4. The automatic updates of the routing table on the network to block attacks detected
5. Automatic firewall configuration to block all IP addresses used by the attacker.

VI. Conclusions

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

This research is primarily done to study the problems and attacks of cloud computing such as DOS Attack, Flooding Attack, and Phishing Attacks on Virtual Machine. Moreover, we classified these attacks into five security categories, namely: security standards, network, access, cloud infrastructure, and data. And we have detailed each one of these attacks. Also this work focuses on the effective solutions to detect this kind of attacks, including intrusion detection systems (IDSs). We propose the deployment of integrated and layered IDS on cloud that designed to cover various attacks.

This IDS integrates knowledge and behavior analysis to increases a cloud‘s security.

References

[1] Final Version of NIST Cloud Computing Definition Published. Available online : http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed on 03 April 2015).

[2] I. Khalil, A. Khreishah, and M. Azeem, “Cloud Computing Security: A Survey,” Computers, vol. 3, no. 1, pp. 1–35, Feb. 2014.

[3] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, 2013.

[4] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, “A Survey on Security Issues in Cloud Computing,” Int. J. Innov. Technol. Explor. Eng., vol. 5, no. 6, pp. 83–87, 2011.

[5] M. H. Sqalli, F. Al-Haidari, and K. Salah, “EDoS-shield - A two-steps mitigation technique against EDoS attacks in cloud computing,” Proc. - 2011 4th IEEE Int. Conf. Util. Cloud Comput. UCC 2011, pp. 49–56, 2011.

[6] R. Balasubramanian and Dr.M.Aramuthan, “Security Problems and Possible Security Approaches In Cloud Computing,” Int. J. Sci. Eng. Res., vol. 3, no. 6, pp. 1–4, 2012.

[7] N. Gruschka and M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” Proc. - 2010 IEEE 3rd Int. Conf. Cloud Comput. CLOUD 2010, pp. 276–279, 2010.

[8] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” in 2009 IEEE International Conference on Cloud Computing, 2009, pp. 109–116.

[9] A. Singh and M. Shrivastava, “Overview of Attacks on Cloud Computing,” Int. J. Eng. Innov. Technol., vol. 1, no. 4, pp. 321–323, 2012.

[10] Damien Riquet, Gilles Grimaud and Michaël Hauspie. “Study of the impact of the attacks and distributed multi-path on network security solutions”, MajecSTIC, 2012.

[11] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” Natl. Inst. Stand. Technol., vol. 800–94, no. July, p. 111, 2012.

[12] G. Tyler, “Information Assurance Tools Report Intrusion Detection Systems,” Information Assurance Technology Analysis Center (IATAC), September 2009.

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

[14] K. Vieira, A. Schulter, C. Westphall, and C. M. Westphall, “Intrusion detection for grid and cloud computing,” IT Prof., vol. 12, no. 4, pp. 38–43, 2010.

[15] J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung, “Multi-level Intrusion Detection System and log management in Cloud Computing,” 13th Int. Conf. Adv. Commun. Technol., no. Vmm, pp. 552–555, 2011.

[16] B. Sevak, “Security against Side Channel Attack in Cloud Computing,” Int. J. Eng. Adv. Technol., vol. 2, no. 2, pp. 183–186, 2012.

Omar Achbarou is a PhD student, he received his Master’s degree in Computer Science from the Cadi Ayyad University Marrakech Morocco. His research interests are computer science, cloud computing security, Internet of Things and big data.

My Ahmed El Kiram is a full professor of computer science at the Department of Computer Science, Faculty of Science Semlalia, Cadi Ayyad University, Morocco. His major field of study is IT security, cryptographic systems and cloud computing. He is the author of numerous publications related to his research interests.

Salim Elbouanani is a PhD student at the Computer Science Department of the Cadi Ayyad University in Marrakesh; Morocco. His is research interests are the security and privacy in the internet of things. He is also working actively in the design of new smart objects solving real problematics in the Marrakesh region.