Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 433 – 442

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb

Chaimae Saadi[a], Habiba Chaoui[b]

[a&b]*Systems Engineering Laboratory, Data Analysis and Security Team*
National School of Applied Sciences, Campus Universitaire, B.P 241, Kénitra 14000, Morocco

Abstract

The cloud computing security has become a basic necessity. It acquires knowledge about vulnerabilities, attacks, activities of attackers and tools to secure it. This work proposes new cloud infrastructure architecture, which combines IDS based on mobile agent sand using three types of honeypots in order to detect attacks, to study the behavior of attackers, increase the added value of Honeypot and IDS based mobile agents, solve systems limitations intrusion detection, improve knowledge bases IDS thus increase the detection rate in our cloud environment.

Peer-review under responsibility of the Organizing Committee of CMS 2016

*Keywords:*Cloud; IDS; Mobile gents; Clust-density; Hneyd; Honeycomb; Honeynet; Honeywall; Attacks.

1. Introduction

The Cloud is a way to reduce costs and simplify the management of resources. Positioning the cloud in an operational environment provides easy and quick access to computing resources anywhere, anytime, with any device, but ensuring the security of this environment still difficult to deploy [1]. IaaS providers offer their customers unlimited access computing, network and storage capacity - often coupled with a registration process where authentication to register and immediately begin using cloud services. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals were able to conduct their activities with relative impunity [2]. PaaS providers have traditionally suffered most from such attacks; however, recent data show that hackers have begun targeting IaaS providers as well. Future areas of concern include

Corresponding author. Tel.: +212 6 70 45 96 95 (a); 212 6 42 50 04 54 (b).
E-mail address: chaimaesaadi900@gmail.com (a), mejhed90@gmail.com (b).

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.189

password and key cracking, DDoS, launching dynamic attack points, hosting malicious data and botnet command and control [4].The SaaS providers expose a set of APIs and software interfaces that customers use to manage and interact with cloud services computing which allows for exactly the methods used by hackers to compromise systems with clouds, their motivations and attitudes to the compromised machine [4]. They are tree important forms of the cloud: The public cloud is the first to appear, its principle is to host Web applications on a shared• environment with an unlimited number of users (e.g. Amazon, Google, etc.)[2]. The private cloud is an environment deployed within a company. Implement a private cloud means the transformation of the internal infrastructure using technologies such as virtualization to deliver on-demand services in a simple and fast way [4]. The hybrid cloud allows the coexistence and communication between a private cloud and a public cloud in an organization sharing data and applications [1].

Based on several approaches proposed by several authors [1-14], this work presents the contribution of IAAS infrastructure as a service of private cloud OpenStack which combines the Intrusion Detection System (IDS) based on mobile agent with three basic types of honeypots: honeyd, honeycomb and Honeywall.

The purpose of this paper is to combine the different security challenges in a cloud environment by using: - IDS based on mobile agent that combines two types of intrusion detection "Behavioral and scenarios" in one IDS [2]; - Honeyd to attract all types of hackers to our work environment [3]; - The Honeywall which has several features at the same time to facilitate the detection of several types of intrusion in our system [4]; - The honeycomb in order to generate new signatures [5]. This paper is organized as follows: section 2 presents the related work concerning intrusion detection honeypots in cloud environment. Section 3 introduces some security tools used in this paper. Section 4 describes our proposal architecture and the experimental results. Conclusion is given in Section 5.

2. Related works

The improvement of security of cloud computing has become a necessity for many scientific researchers. Sebastian and all, in [6] requested a need to deploy IDS in the cloud by providing IDS extensible architecture that may be used in the cloud infrastructure. Aman Bakshi and all suggested a framework for the setting cloud DDoS attacks using IDS in a VM (virtual machine) [7]. This may be done by using intrusion detection sensors installed in a virtual machine to sniff network traffic and analyze packets on the Internet using Snort. Chi-Chun and all Developed a framework for cooperation to reduce network IDS cloud DDoS attacks [8]. All these approaches use the technique based on signatures, limited to detect only known attacks. With the onset of honeypots technology in cloud computing. Nithin and all used Cloud Security Honeypots - Honeypots in an exciting new technology that offers enormous potential for the security community [9]. The aim of [8-9] is to explain how honeypots are used for securing cloud computing systems, their advantages and disadvantages but, regrettably, no results approved. Hwan-Seok and all proposed a dynamic honeypot design technique using virtualization technology that increases resource utilization and ease of extension in [10]. The analyze technology of the IP address domain and performs periodically agent is stored DB in the IP list to create dynamic virtual machine. Collected IP address is assigned to the virtual machine, and it is possible to connect with the outside through the virtual machine and port forwarding. But this proposed technique did not show effective results which could be confirmed by the administrator of the intrusion detection system. Then the authors of [12] show the cloud security tactics, which is composed by multistage anomaly IDS, honeypot and ABAC. Outside Cloud, multi-step Anomaly IDS consists of 3 phases: the monitoring phase, the slight anomaly detection phase, and targeted abnormality detection stage. The proposed scheme is designed to support real-time and detects symptoms of attack and new attack patterns. If there is an attack, it is directed to external honeypot, or attack is redirected to Attribute-Based Access Control (ABAC) and enters inside the cloud. ABAC controls the various resources for large volumes of data in the cloud. The ABAC limited amounts of resources, and notify the IDS Multistage anomaly where the use of resource exceeds resource limits. The formal definition of the ABAC consist of four parts: the access control entities, the entities related attributes, political representation and evaluation of policies. Eman and all has presented a security architecture for cloud environment, they decided to work with Amazon AWS cloud and honey jar, they used the Venus Flytrap that is a little honeypot emulates interaction vulnerable services such as HTTPS, SSH, FTP, SIP ... They have implemented this architecture for 3 months in 3 regions: Singapore, Virginia Eastern United States and Sao Paulo to analyze types of attacks, the number of attacks and malware injected into each region. With analysing data it is shown that the types of attacks are captured: Connection attempts, classification ports of attacked, malicious infections, and URL infection. The authors of [12] combine a simple IDS with honey pot, this architecture is designed to stop attacks at the beginning of

the network by IDS, if it were to exceed the IDS, the attack will be blocked by the firewall under the rules considered by the administrator, eventually, it will be blocked by Honeypot. The disadvantage of this architecture is that the attacker can use the honeypot to attack the LAN. When Honeypot is placed behind a firewall, it may introduce new security risks for the internal network, especially if the internal network is not secured against the Honeypot through additional firewalls.

3. Tools and methods

In this section, we present the various security tools such as:

3.1. Intrusion detection based on mobile agents and Clust-density IDS-AM-Clust

To improve the ability of intrusion detection systems based on mobile agents [14] or Clust density [15], the intrusion detection system aims to merge the two latest technology [14] [15]: in a single IDS named "IDS-AM-Clust". This was the subject of a work already realized by our team [16].

The following figure (fig.1) shows the flow of network traffic process in our mobile agents using Clust-density:

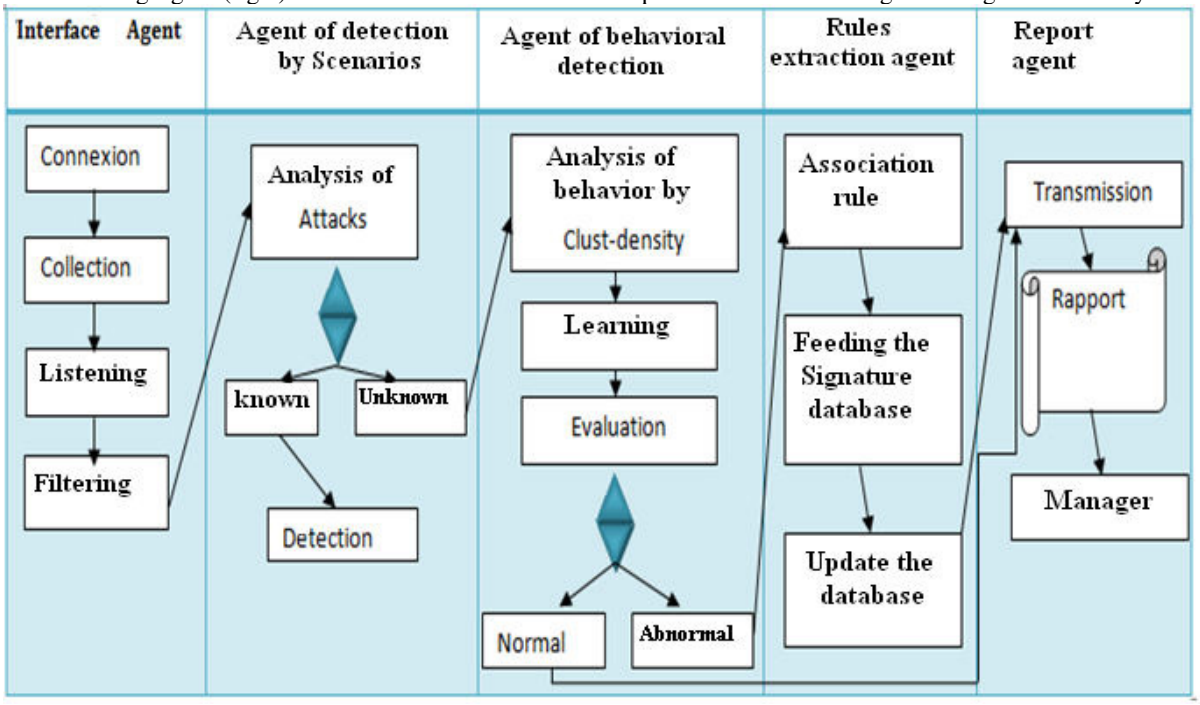

Figure 1 : Process for intrusion detection by IDS-AM-Clust [16]

The development of this system was using Sun Java Develop Kit 7 and 3.7 platform JADE (Java Agent Development) that simplifies the implementation of multi-agent systems [14]. In addition, Open source library used is the JPCAP 0.7.

3.2. Honeyd

Honeyd are the Honeypot Low interaction: easy to deploy, emulate real services, they do not interact with the hackers, it offers a limited detection because they only detect scan port and they are detectable by hackers [4].

3.3. Honeycomb

Honeycomb is a pattern detection engine that monitors any network traffic that Honeyd receives and creates NIDS signatures for any patterns that occur regularly [5]. It is assumed that any regular traffic that Honeyd receives is malicious in nature, as honeypots in general serve no other network purpose and should not be receiving valid traffic. The advantages to use Honeycomb include reducing overhead caused by using additional programs to perform the same task and it is integrated into Honeyd hence will not have any synchronization issues. Additionally the creation of NIDS signatures could be very useful for detecting very new automated mobile malware and integrating the signatures into Network Intrusion Detection Systems on wireless networks to track the spread and effect of such malware [17].

3.4. *Honeynet :*

The Honeynet are high-interaction honeypot. They have a big project to search for attacks from the hacker's community. The aim of the project is to look for tools, tactics and motivations of the hackers [6]

Component of honeynet

3.4.1. ***Data Capture****:* Data capture is the monitoring and recording of all threat activity in the Honeynet architecture, these captured data are then analyzed to learn the tools, tactics, and motivation of the attackers [18]. The challenge is to capture as much data as possible without detecting the threat. One of the challenges with the capture data is that the majority of the attacker's activities arrived on encrypted channels (like IPSec, SSH, SSL, etc.). The capture data mechanisms should consider encryption [20].

3.4.2. ***Data Control****:* We define risk, there was always the possibility of an attacker or malicious code uses a honeypot to attack or harm non-honeynet systems [21]. One of the best ways to approach the data control is to not rely on a single mechanism with which to implement it. Instead, the implementation of the control of data using layers, such as counting outbound connections, intrusion prevention gateways, or bandwidth restrictions. The technique used is limiting outgoing connections [22].

3.4.3. ***Data Analysis****:* This is the third condition. The goal of a honeypot is information, a honeypot is worthless if you do not have the ability to convert the data they collect to information, and we must have some ability to analyze data [23].

The key of the Honeynet architecture is the Honeywall. It is a gateway device between the honeypots around the world. All traffic to and from the honeypot has to go through the Honeywall [20]. This gateway is typically a bridge of layer 2 which means that device should be invisible to all interactions with honeypots [25].

3.5. Open Stack Cloud computing

OpenStack is a project initiated by Rackspace and NASA platforms designed to manage large scale and low cost, it is an open source operating system officially launched in March 2010. This is comparable to Amazon Web Services architecture [32]. OpenStack is a cloud operating system capable to control a large amount of computing, storage and network resources through a virtual data center, all managed by a dashboard allowing to administrators control over users and resources available through a web interface[33]. It is free software that enables private and public cloud construction. OpenStack is a community and a project in addition to software that is designed to help

organizations implement a system server and virtual storage [26]. OpenStack consists of a series of software and open source projects that are maintained by the community including: OpenStack Compute (named Nova), OpenStack Object Storage (Swift named) and OpenStack Image Service (Glance appointed) [27].

Table1: Comparison between Eucalyptus and Openstack

	Eucalyptus	OpenStack
Product by	Santa Barbara University	Rackspace, NASA, Dell, Citrix
Goal	Implement Cloud Computing commercial aspect	implement a cloud computing and managing more efficient the infrastructure
Area of use	Companies want to build their own Cloud Computing	Service providers, Companies, researchers…
Programing language	Java,C and Python	Python
Tolerance of failure	Separation of clusters controllers	Data replication

4. Proposed approach : Iaas security using IDS based on mobile agents and honeypots

4.1. Test environment

The objective of this test is to implement our honeypot-IDS architecture in a Cloud environment

4.1.1. Step of authentication

To ensure a high level of safety and to avoid attacks such as DOS, U2R, R2L and prob, we deployed secure authentication architecture. In general, user registers by providing personal information. Subsequently, the Cloud services provider provides an ID (identifier) user's own, used authentication technologies can be: Id/password, PKI (Public Key Infrastructure), SSO (Single Sign On)... etc. To authenticate user in the first place, the scanner scan information such as ID / password, time, Position, location,...etc [27]. In our proposed model, the RSA encryption algorithm is used to secure the communication between the user and the provider, using the public key and the private key. The main advantages of RSA's security are: firstly, RSA is based on the simple authentication using probabilistic algorithms. Secondly, it is so difficult to a malware to find the two factorizations. The RSA algorithm is based on simple mathematical results known since the 18th century. Finally, RSA does not need a channel for the exchange of a key [30].

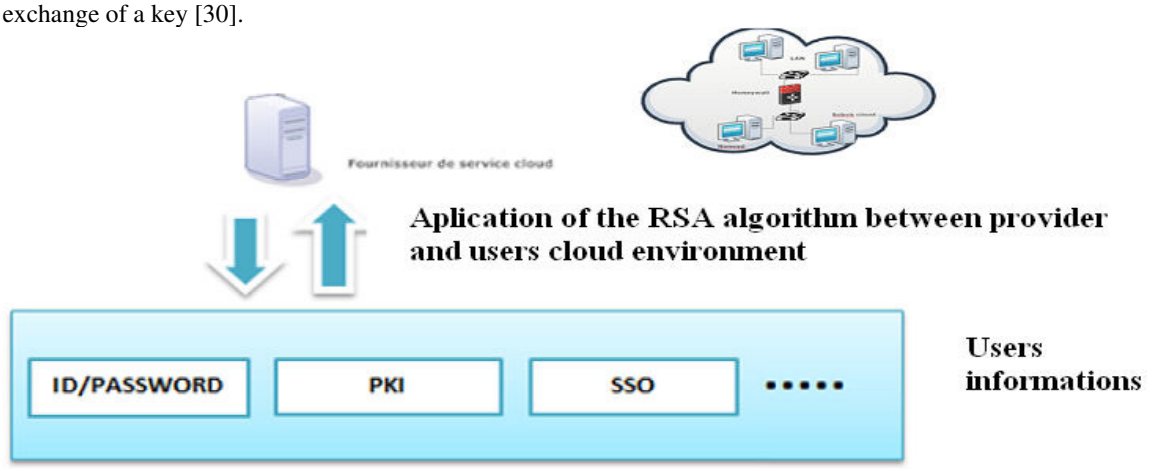

Figure 2 : Authentification in our cloud

The basic idea of our architecture is as follows: after the authentication stage, Firewall monitors incoming and outgoing traffic in our system by using the provider security policy. The model that follows will present the network traffic path:

4.1.2. Overview of the model

Architecture with which we worked is basically a Cloud OpenStack precisely the IAAS layer precisely the environment that has a computational capacity and storage, as well as network connectivity to manage a workload requested by applications.

Before accessing the Datacenter, it is important to go through the authentication phase. This phase allows users to authenticate using one of several methods such as "Id/password, PKI (Public Key Infrastructure), SSO (Single Sign. On)" The cloud provider may use the RSA algorithm for encryption and decryption to implement a security policy between the user and the provider cloud.

After the authentication stage, the access control area which consists of a firewall for traffic control, if it is a malicious traffic, it will be blocked, otherwise the traffic is allowed. Subsequently, the traffic is sent to the Honeywall that integrates our IDS-AM-Clust by upgrading and setting up snort IDS; which allows to monitor all this traffic. As we mentioned previously, Honeywall is a core component of the GEN III Honeynet.
The honeywall separates three areas:

- **Internal area**: Ethernet which client machines of the system has been.
- **Demilitarized zone**: where web servers was placed
- **Honeypot area**: this area consists of a client Sebek to decrypt encrypted traffic (it is capable of detecting encrypted attacks) subsequently it send this traffic to the sebek server placed in the honeywall.

The honeypot zone consists also of a Honeyd which aims to draw attention to pirates.

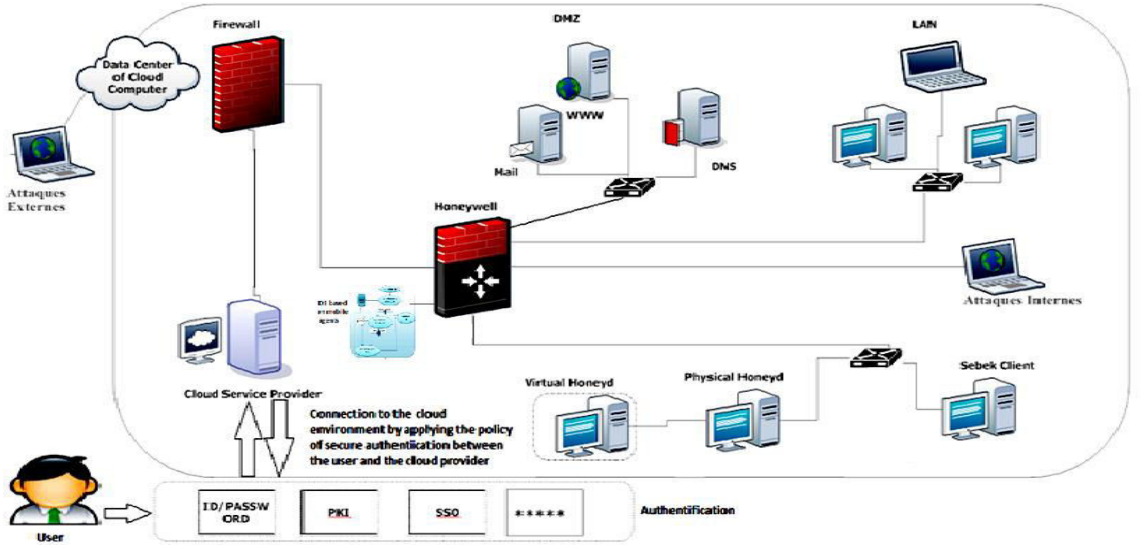

Figure 3: Proposed system implemented in cloud environnement

Approach illustrated by figure 3 offers a combination of security in a Cloud which includes the benefits of authentication with security policy techniques presented by the firewall of the Cloud provider and also the consolidation of effectiveness and robustness of our IDS-AM-Clust and two honeypots (Honeyd and Honeynet), allowing:

- Monitor and simulate the IP address and different operating simultaneously. That will attract the maximum of attacker.
- Provide real services forward to study the behavior of attackers.
- Using a Honeywall which provides various network security and detection tools.
- The Sebeka Server/client that is designed to detect all attacks encrypted.

4.2. Test and results

4.2.1. ***Distribution of attacks by source and destination***:
Tests performed by our architecture in the OpenStack environment produced the results presented in the tables below. Each line contains detailed information on the types of the used ports, including the filtered connection number and the detection rate brought to the connections for each port by the IDS-AM-Clust

Table 2 : Ports sources attacks

Port sources	Connexion	IDS event
54606	686	12
1037	3	2
1038	3	1

Table 3 : Ports destination attacks

Port destination	Connexion	IDS event
80	10	8
36131	68	0
53	5	2

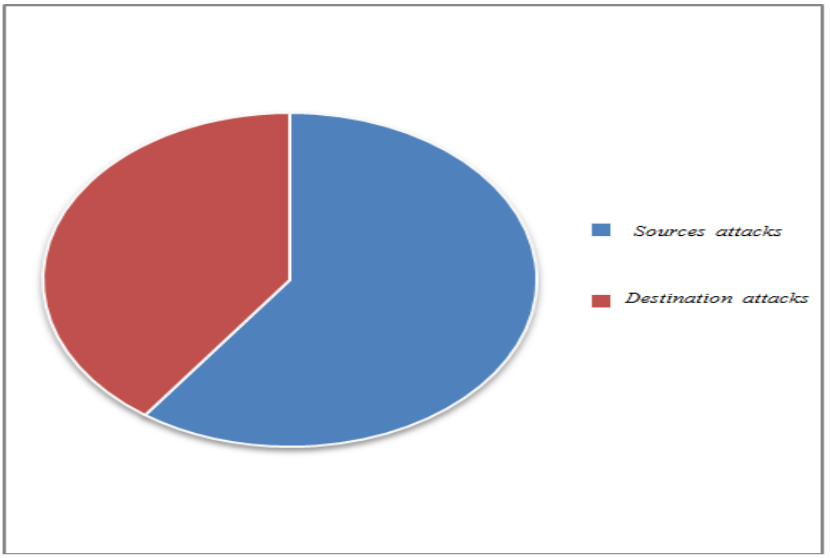

Figure 4 : Port sources and destination attacks

The previous Figure shows the distribution of alerts in terms of direction of the attacks (source and destination). Respectively, we find that the majority of alerts from the source ports. However they may be connected with attacks internal (from an internal attacker). However, attacks from the outside shows that our system is able to detect

different types of attacks.

1.1.1. Distribution by type of attacks and detection rate

The results obtained in the implementation of our architecture are presented in a model predictive 'log file' generated by the virtual honeywall. This data set contains a normal data type and other types of attacks and a minimum rate of false positive and negative shown in the following table (tab.3):

Table 4: Intrusion detection rate and false positive

Attacks Types	Normal	Abnormal				False positive	False negative
		DOS	U2R	R2L	Probe		
Cloud (Honeywall+ honeyd+IDS-AM-Clust)	31%	33%	10%	7%	19%	1%	0.5%

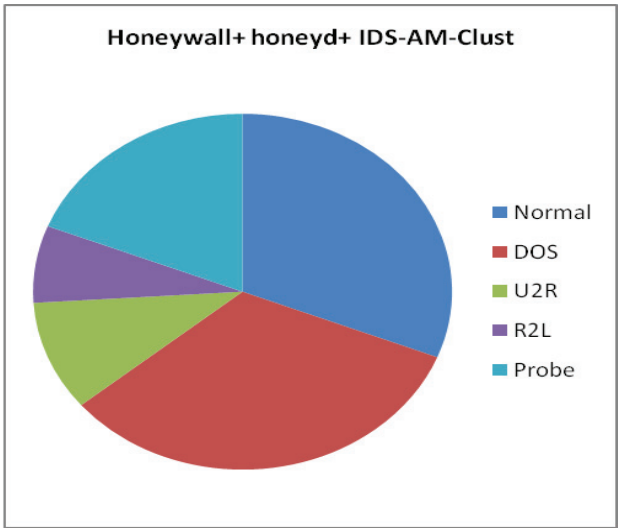

Figure 5 : Types of detected attacks

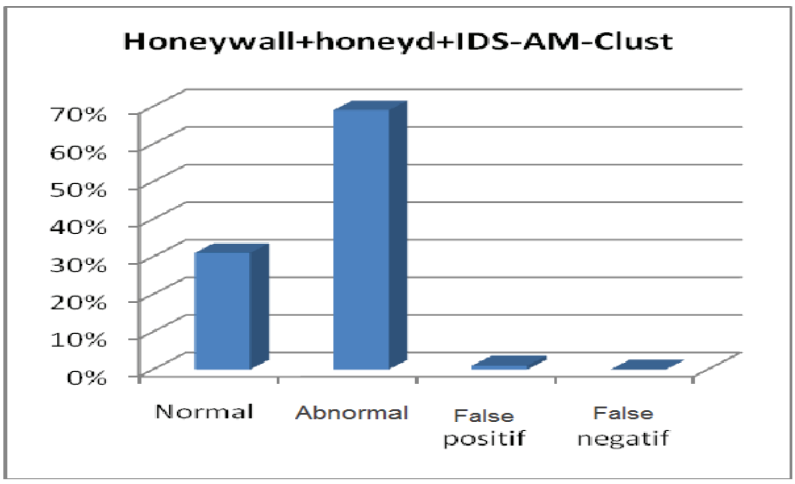

Figure 6: Rate of detection the FP and FN

The main objectives of our architecture can be summarized as follows:

- The discovery of the world of Cloud Computing Security
- The development and the Implementation of a higher secure system.
- Increase of the added value of the honeypots and IDS.
- The combination of the honeypot has weak interaction with high interaction honeypot.
- Use the information collected by honeypots to create scenarios of attacks.
- Increase the accuracy of IDS: reduce the rate of false negatives and false positives.

Conclusion

The use of the honeynet and the IDS in a Cloud environment became a vital necessity to ensure a high level of security. The use of a new architecture Cloud that merges the advantages of IDS, honeynet, honeypot and firewall techniques in a single Datacenter Cloud would be an ideal tool for the treatment of threats to computer networks. Indeed, this new architecture benefits of the used techniques, including intrusion detection, behavioral study of attacks and creation of attack scenarios. Thus, carried out analyses and the obtained results allowed us to show that our system has responded to some Cloud security problems through the effectiveness of detection of abnormal behavior by reducing the rate of false positive and negative.

References:

[1] Roschke, S., Cheng, F., Meinel, C.: Intrusion detection in the cloud. In: IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp.729–734, 2009.

[2] Grance, T., Mell, P.: The nist definition of cloud computing. National Institute of Standards & Technology (NIST) (2009), http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[3] Ramya. R Securing the system using honeypot in cloud computing environment International Journal of Multidisciplinary Research and Development Volume: 2, Issue: 4, 172-176April 2015.

[4] Costa DG, Guedes LA (2011) “Exploiting the sensing relevancies of source nodes for optimizations invisual sensor networks.” Multimed Tools Appl 55, 2003.

[5] Y. Sun, Y. Luo, and all, Fast live cloning of virtual machine based on xen. In High Performance Computing and Communications HPCC ’09. 11th IEEE International Conference on, pages 392 –399, June 2009.

[6] C. Kreibich and J. Crowcroft. Honeycomb — Creating Intrusion Detection Signatures Using Honeypots 2nd Workshop on Hot Topics in Networks (HotNets-II), 2003, Boston, USA.

[7] AmanBakshi, Yogesh B. Dujodwala, "Securing Cloud from DDoS Attacks Using Intrusion Detection System in Virtual Machine", Proceedings of the 2010 Second International Conference on Communication Software and Networks(ICCSN '10), P 260-264.

[8] Chi-Chun Lo, Chun-Chieh Huang and Ku, J “A Cooperative Intrusion Detection System Framework for Cloud Computing Networks”.In 2010, 39th International Conference on Parallel Processing Workshops.

[9] Nithin Chandra S.R, Madhuri T.M Cloud Security using Honeypot Systems International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.

[10] Hwan-Seok Yang A study on attack information collection using virtualization technology Springer Science+Business Media New York 2013 Multimed Tools Appl DOI 10.1007/s11042-013-1487-8.

[11] Ryung Rae Cha ,Jongwon Kim “Security Tactics for Secured Cloud Computing Resources” Procceding IEEE ICOIN 2013pages(473-475).

[12] Eman Al Awadhi and all « Assessing the Security of the Cloud Environment” 2013 IEEE GCC Conference and exhibition, November 17-20, Doha, Qatar.

[13] Renu Meghani, Sanjay Sharma, "Security from various Intrusion Attacks using Honeypots in Cloud" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 5, May 2014.

[14] Chaimae Saadi and Habiba Chaoui, Security Analysis Using IDs Based on Mobile Agents and Data Mining Algorithms / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 597- 602, 2015.

[15] Chaimae Saadi, Habiba Chaoui and Hassan Erguig, Contribution to Abnormality Detection by Use of Clust-Density *Algorithm* DOI: http://dx.doi.org/10.15866/irecos.v10i4.5699 in 2015

[16] Chaimae saadi and Habiba Chaoui, Security by IDS-AM-Clust, honeyd and honeycomb International Journal of Engineering Works Kambohwell Publisher Enterprises ISSN: 2409-2770 Vol. 2, Issue 9, PP. 84-92, Sept. 2015

[17] Jacoby et al., 2006 SmartPot: Creating a 1st Generation Smartphone Honeypot Originally published in the Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd, 2009.

[18] Nadya elmoussaid and all, Intrusion Detection Based On Clustering Algorithm International Journal of Electronics and Computer Science Engineering 1059 Available Online at www.ijecse.org ISSN- 2277-1956/V2N3-1059-1064, 2013.

[19] Nahla Ben Amor and all, Réseaux bayésiens naïfs et arbres de décision dans les systèmes de détection d'intrusions LARODEC, Institut Supérieur de Gestion Tunis RSTI-TSI. Volume 25 – nÆ 2/2006, p. 167- 196.

[20] Vusal Aliyev, Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network Department. Thesis memory of Computer Science and Engineering Division of Computer Security Chalmers University of technology Göteborg, Sweden, 2010.

[21] The honeynet project "capture et étude de plusieurs attaques en utilisant des honeynets de 1ère génération (GenI) » 1999-2001**.**

[22] The honeynet project "Pot de miel-Pham QuyetThang, Victor Moraro 2002-2003 GenI et des honeynets virtuels » 1999-2001**.**

[23] N. Provos and T. Holz. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley Professional, GenIIet des honeynets virtuels.**2007.**

[24] The honeynet project :http://old.honeynet.org/papers/cdrom/roo/index.html

[25] The Honeynet Project, "Honeywall CDROM," available online: http://honeynet.org/tools/cdrom/.

[26] the OpenStack projecttutoriel IEEE CloudCom 2010-Bret Piatt

[27] the Openstackproject Beginner's Guide-v3.0, 7 May 2012

[28] the cloud computing project :https://www.openstack.org/

[29] IBM United States Software Announcement 215-106, dated February 24, 2015

[30] ByungRaeCha ,Jongwon Kim "Security Tactics for Secured Cloud Computing Resources" Procceding IEEE ICOIN 2013, pages(473-475).

[31] Richard Chow "Authentication in the Clouds: A Framework and its Application to Mobile Users" CCSW'10, October 8, 2010, Chicago, Illinois, USA. Copyright 2010 ACM 978-1-4503-0089-6/10/10.

[32] Honeypnet project . Lance Spitzner. 2002 «Traching Hacker »: Addison Wesley Lance Spitzner, "Honeyd," *Honeypots—Tracking Hackers*, Addison Wesley, 2002, pp. 141-166.

[33] B. Schneier, Cryptographie appliquée : protocoles, algorithmes et codes sources en C, J. Wiley, 1997.

[34] Chaimae Saadi and Habiba Chaoui. 'Improving Intrusion Detection System using IDS-AM-Clust, Honeyd, Honeycomb and Honeynet' European Journal of Scientific Research Volume 135 No 1 October, 2015 pages 61-70.