Use Trust Management Framework to Achieve Effective Security Mechanisms in Cloud Environment

Hicham Toumi[1], Bouchra Marzak[1], Amal Talea[2], Ahmed Eddaoui[2], Mohamed Talea[1]

[1]*Information Processing Laboratory, Department of Physical, University Hassan II Casablanca, Morocco*
[2]*Department of Mathematics and Computer Science, University Hassan II, Casablanca, Morocco*

***Abstract* — Cloud Computing is an Internet based Computing where virtual shared servers provide software, infrastructure, platform and other resources to the customer on pay-as-you-use basis. Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, with the enormous use of Cloud, the probability of occurring intrusion also increases. There is a major need of bringing security, transparency and reliability in cloud model for client satisfaction. One of the security issues is how to reduce the impact of any type of intrusion in this environment. To address this issue, a security solution is proposed in this paper. We provide a collaborative framework between our Hybrid Intrusion Detection System (Hy-IDS) based on Mobile Agents and virtual firewalls. Therefore, our hybrid intrusion detection system consists of three types of IDS namely IDS-C, IDS-Cr and IDS-M, which are dispatched over three layer of cloud computing. In the first layer, we use IDS-C over our framework to collect, analyze and detect malicious data using Mobile Agents. In case of attack, we collect at the level of the second layer all the malicious data detected in the first layer for the generation of new signatures using IDS-Cr, which is based on a Signature Generation Algorithm (SGA) and network intrusion detection system (NIDS). Finally, through an IDS-M placed in the third layer, the new signatures will be used to update the database NIDS belonging to IDS-Cr, then the database to NIDS belonging of IDS-Cr the cluster neighboring and also their IDS-C. Hardware firewall is unable to control communication between virtual machines on the same hypervisor. Moreover, they are blind to virtual traffic. Mostly, they are deployed at Virtual Machine Monitor- level (VMM) under Cloud provider's control. Equally, the mobile agents play an important role in this collaboration. They are used in our framework for investigation of hosts, transfer data malicious and transfer update of a database of neighboring IDS in the cloud. With this technique, the neighboring IDS will use these new signatures to protect their area of control against the same type of attack. By this type of close-loop control, the collaborative network security management framework can identify and address new distributed attacks more quickly and effectively.**

***Keywords* — Cloud Computing, Virtual Firewalls, Mobile Agents, Security.**

I. Introduction

Cloud computing represents a distributing computing mechanism that by the use of the high speed network and highly scalable distributed computing platforms in which computational resources are offered 'as a service'. Cloud computing architecture introduces many technologies including server virtualization, Network Virtualization (NV), and Network Function Virtualization (NFV) to enhance the essential characteristics of cloud computing [1][2]. Cloud services allow individuals and enterprises to use software and hardware that are managed by providers at remote locations. It is a model for enabling scalable, on demand network access to a shared pool of configurable computing resources that can be provisioned ubiquitously and released with minimal management effort and cloud service provider interaction [3][4]. At the same time, the transformational nature of the cloud is associated with significant security and privacy risks [5][17].

Therefore, the intrusion detection or confidentiality of data over Cloud is one of the glaring security concerns. The fast growth of cloud computing technology introduces more of the vulnerabilities. Security is considered to be one of the most critical aspects in cloud computing environment due to the confidential and important information stored in the cloud [5][6]. Network security appliances, such as Intrusion Detection Systems (IDS) is widely deployed in advantage points and play an important role in protecting the network from attacks. That is why; it is nowadays widely deployed for securing critical IT-Infrastructures. Due to different deployment mechanisms, we can distinguish different types of IDS; IDS can be categorized as software-based IDS, hardware-based IDS, and VM-based IDS [7]. Most of these appliances work without collaboration, their detection results are isolated and cannot be collected and analyzed systematically. Therefore, we thought of a new security policy that allows the detection of distributed attacks such as deny of service (DoS) and Distributed Denial of Service (DDoS) [6].

In this paper, we will deepen the development of our approach based in principle on the cooperation of the Hybrid Intrusion Detection System (Hy-IDS), Firewall and mobile agents. The cooperation between Hy-IDS, Firewall and mobile agents present what is called a Framework. This framework allows to reach four objectives: the first, detection intrusion in a virtual environment using mobile agents for collecting malicious data. The second, generating new signatures from malicious data, which were collected in the first phase. The third, dynamic deployment of remote response actions using virtual firewall. Finally, dynamic deployment of updates between clusters in a cloud computing, using the newest signatures previously created.

The rest of this paper is organized as follows: The section II presents theoretical background and discusses some related works in the area of Mobile Agent-based IDS and NIDS. The section III forms the core of this paper explains and describes in detail our approach. Whereas the proposed framework is discussed in section IV. Finally, we give conclusion, perspective and references in section V.

II. Theoretical Background and Related Work

In this section, we start with theoretical background include cloud computing, mobile agent technology in cloud computing and Signature Generation Algorithm as the first part, and Related Work as a second part.

DOI: 10.9781/ijimai.2017.4311

A. Cloud Computing

Cloud computing allows accessing resources and services offered by servers from different places. Therefore, it is a model of distributed computing [5] [8][9]. It is undergoing an incontestable success, which could be indeed compromised by concerns about the risks related to potential misuse of this model aimed at conducting illegal activities. To provide secure and reliable services in cloud computing environment is an important issue. Then, there have been a great deal of inherent issues in cloud computing such as data security, vulnerability management, disaster recovery system, and business continuity process and identity management [10]. Then, there are numerous security issues in cloud computing as it encompasses many technologies including networks, virtualization, load balancing, operating systems, transaction management, resource scheduling, concurrency control and memory management [11]. Virtualization enables customers to run multiple operating systems concurrently on a single physical server, where each of the operating systems runs as a self-contained computer [12][13]. More recently, virtualization at all levels became important again as a way to improve system security, reliability and availability, reduce costs, and provide greater flexibility.

B. Mobile Agent Technology in Cloud Computing

The Mobile Agent has its applications in many areas including network management, mobile computing, information monitoring, searching information, remote software management and others. Mobile Agents enhance the performance in these areas by providing the following services [14][6]: there are efficiency and reduction of network traffic, interaction with real-time entities, life cycle of mobile agent and convenient development paradigm.

C. Signature Generation Algorithm (SGA)

Different sessions of attacks are given as input to Signature Generation Algorithm (e.g, Apriori Algorithm and Signature Apriori Algorithm). According to support and confidence value rule are generated by Signature Generation Algorithm. These rules are given to IDS. When attack is generated for which signature is stored in IDS, it generates alarm [5].

D. Relevant Works and Limitations

In the literature there are few works that use IDS, NIDS (Snort and signature apriori algorithm) and mobile agents in the cloud computing.

Chirag N. Modi et al propose a framework integrating network intrusion detection system (NIDS) in the Cloud. Then, NIDS module consists of Snort and Signature Apriori Algorithm. It generates new rules from captured packets. These new rules are appended in the Snort configuration file to improve efficiency of Snort. The objective of this approach is to reduce impact of network attacks (known attacks as well as derivative of known attacks). Derivative attacks can be detected by Snort [15]. However, this work is unable to detect intrusion at the hosts, and Distributed denial of service attacks (DDOS) [6].

In [16] the VMs are attached to MA, which collects evidences of an attack from all the attacked VMs for further analysis and auditing. Then, they have to correlate and aggregate that data to detect distributed attacks. This work tried to offer a line of defense by applying mobile agent's technology to provide intrusion detection for cloud applications regardless of their locations. Thus, it builds up a robust distributed hybrid model scalable, flexible and cost effective method based on mobile agents (MA).

After that, we found the need for collaboration between several security solutions. This collaboration is mainly based on mobile agents. Then we exploit mobile agents for security against intrusion attacks and at the same time as a communication tool between different layers of cloud computing.

III. Our Framework for Trust Management in Cloud Environments

The designed dynamic network security architecture for IaaS platforms is based on the mechanisms of VM traffic redirection and policy management, security-supporting services. Our previous works [5][6]. Today, we present a new approach based on the improvement of collaboration among Hybrid Intrusion Detection System (Hy-IDS), Signature Generation Algorithm (SGA), Mobile Agents (MA) and Firewall. It follows the principle the P2DR (Policy, Protection, Detection, and Response).

A. Challenges of the Framework Proposed

The objectives of our framework are grouped into four main Points as follows:

1. Intrusions detection in a virtual environment using mobile agents in order to collect malicious data.
2. Generating new signatures from malicious data, which were collected in the first part.
3. Dynamic deployment of updates between clusters in a cloud computing, using the newest signatures previously created.
4. Dynamic deployment of remote response actions using virtual firewall.
5. Dynamic deployment of updates between clusters in a cloud computing, using the newest appropriate response actions previously created.

B. Our Proposed Hybrid Framework and Cloud Computing

1) Components of our framework

Our framework based on many concepts and components as follows: Hybrid Intrusion Detection System (Hy-IDS) combines Intrusion Detection System Center (IDS-Cr), Intrusion Detection System Control (IDS-C) and Intrusion Detection System Master (IDS-M). The IDS-Cr based on an Intrusion Detection System (IDS) and Signature Generation Algorithm (SGA). However, IDS-C is based on the combination of IDS with the living environment of mobile agents named Agents Agency (AA). The IDS-M is based on Intrusion Detection System (IDS) and Living Environment of Mobile Agents named Agents Agency (AA). Concerning the types of IDS; there are network based (NIDS) and host based (HIDS) intrusion detection systems. Then, some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Finally, using mobile agents to ensure communication between the IDS-C, IDS-Cr and IDS-M [6].

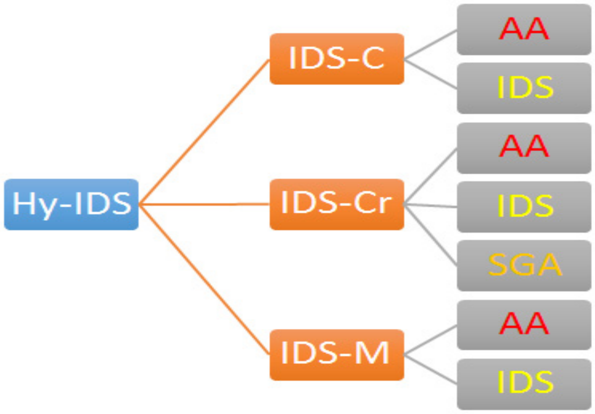

Fig. 1. Components of our Hy-IDS.

2) *Proposed framework over cloud computing*

Cloud architecture used with our framework is presented as a front-end and back-end. Front-end is connected to both external network as well as internal network. Then, It is presented in the figure 2 by the Cloud-layer include only the Cloud Controller (CLC). It is used by the user for communicate with Cloud Computing. It allows management of cloud security. However, back-end consists of computer hardware and software (servers, storage), that are designed for the delivery of services. The CLC acts as the administrative interface for cloud management and performs high-level resource scheduling, and handles reporting, authentication and accounting. The Cluster Controller (CC) acts as the front-end for a cluster within a cloud computing and communicates with the Cloud Controller and Node Controller. Finally, the Node Controller (NC) at level of physical server; it hosts the virtual machine instances and manages the virtual network endpoints.

We have just presented the cloud architecture and the components of our Hy-IDS. Therefore, we proceed to the establishment or distribution of the components of our framework on this architecture according to our strategy the protection. However, Our Hybrid Intrusion Detection System (Hy-IDS) combines Intrusion Detection System Control (IDS-C) and Intrusion Detection System Center (IDS-Cr), which are placed in the back-end. Finally, Intrusion Detection System Master (IDS-M), which is placed in the front-end. Then, the general architecture of our framework, shown in Figure 2, is divided into four main layers interact.

IDS-C: VMs are further managed by hypervisors, also known as Virtual Machine Monitor (VMM) and are basically installed on server hardware. Thus, we use VMM in our framework to ensure a new level of trust in the VMs. Then, we place the components of IDS-C at the level of nodes (physical server) for monitoring virtual machines. For more details, we place IDS-C at the level of VMM. At the same time, we place specific static agent detectors (SA) at the level of VMs. Our IDS-C is based on the cooperation of IDS with the living environment of mobile agents named Agents Agency (AA).

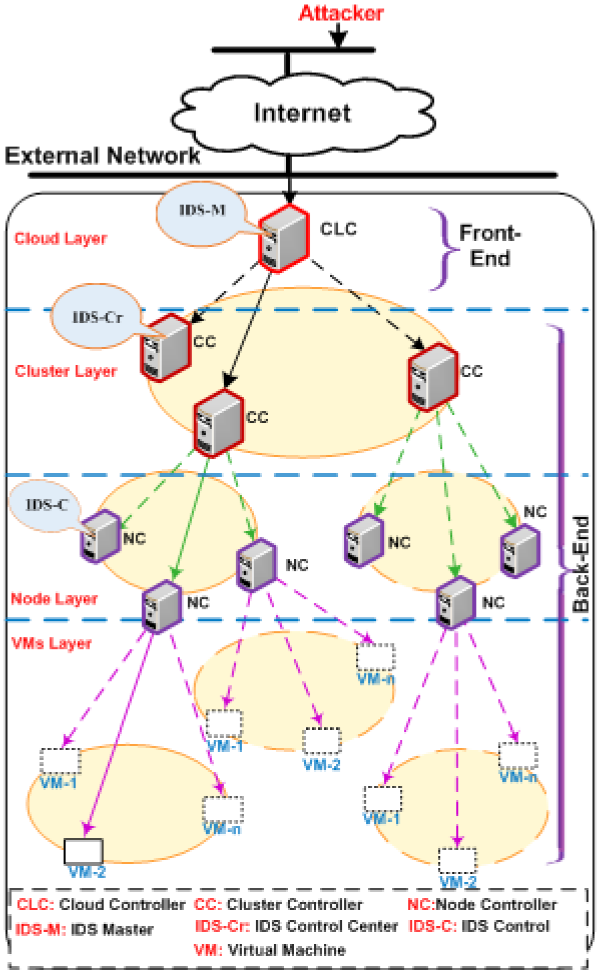

Fig. 2. The Hierarchy of our cloud computing.

IDS-Cr: it installed in the front-end Cluster for the monitoring of nodes. It also generates new signatures. It consists of an Intrusion Detection System (IDS) and Signature Generation Algorithm (SGA).

IDS-M: it is placed in the front-end Cloud for the monitoring of Clusters and Management of Update (new signatures). The IDS-M is based on IDS and Living Environment of Mobile Agents named Agents Agency (AA). Finally, all communication between these components is provided by mobile agents.

3) *Intrusion detection management based on our Hy-IDS*

VM-layer and Node-layer constitute the fundamental design of our proposed framework. Then, each node consists of three main components namely IDS Control (IDS-C), Agents Agency (living environment of mobile agents), Specific Static Agent Detectors (SA) [6].

Static Agents (SA) placed at the level of virtual machines. It generates an alert whenever they detect suspicious activities, then send alert's ID to IDS-C. In this case, IDS-C will send investigative Mobile Agent (IMA) with a specific task, to each agency (VM) that sent similar alerts. The IMA visit and investigate all those VMs for collecting information, who affirm the existence of an intrusion. It carries back the result at to the IDS Control to perform advanced analysis.

In case of attack, IDS-C aggregate malicious data, then placing them in a temporary database. After, IDS-C uses Transfer Mobile Agents (TMA) for notifying IDS-Cr placed in the cluster layer as shown in the figure 3 [6]. After, IDS-Cr dispatches Investigative Mobile Agents (IMA) to any IDS-C those send TMA, for aggregation and collection of their malicious data from the database temporarily. Then, IDS-Cr uses all malicious data collected by IMA and using them to generate new signatures through a Signature Generation Algorithm (SGA) at level of IDS-Cr.

Finally, these new signatures will be used to update the database IDS belonging to this IDS-Cr. after that, IDS-Cr sends these new signatures toward IDS-M. Thus, IDS-M uses these new signatures to update databases of neighboring cluster (eg: IDS in CC_2 and CC_3) based on update mobile agents (UMA) as shown in figure 3.

These updates go through the IDS-M, to maintain a hierarchical structure in our framework. Then, our framework protects neighboring clusters of the same type of attack. Thus, among the advantages of our approach, other clusters are protected against the same category attack.

C. *Responses to Attacks Using Virtual Firewall*

The essential role, which can perform a firewall is that of securing the connections between the tenant network and the cloud infrastructure network. The cloud infrastructure network really hosts a number of traffic profiles, such as management traffic, storage traffic, and management traffic, Cluster/CSV traffic and Live Migration traffic. However, these traffic profiles must be totally analyzed and controlled using firewall. In our approach, we use the firewall to respond to incoming and outgoing attacks in a hypervisor. Consequently, the virtual firewall is a network security system, which controls incoming and outgoing network traffic based on a set of rules.

However, the firewall could be used to control access between virtual machines and Internet access. Virtual traffic between two virtual machines may never leave the physical host hardware, which

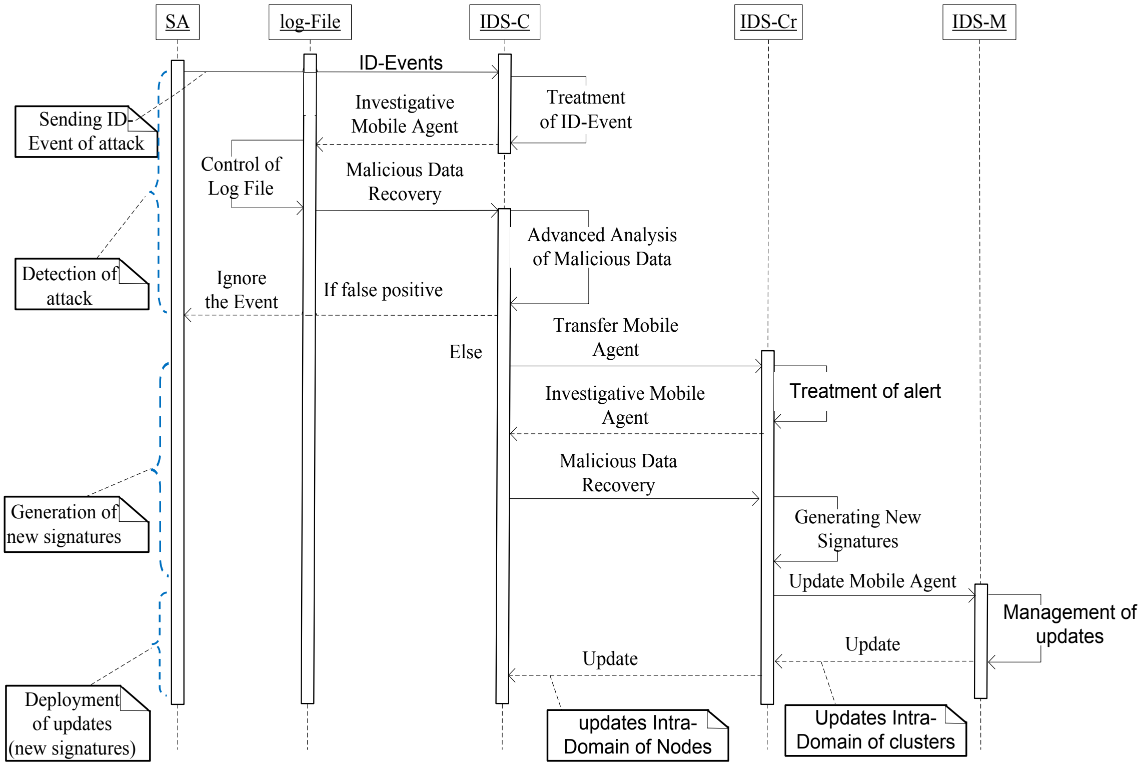

Fig. 3. Principle of our framework

use traditional physical firewalls unsuccessful to secure and monitor this traffic. Then, the best solution to this problem is the use of virtual firewalls over hypervisor. As shown in figure 4, a virtual firewall is a firewall service running in a virtualized environment, providing the usual packet filtering and monitoring services that a physical firewall would provide. Thus, we will have a hypervisor-based on virtual firewall. This virtual firewall is implemented on the VMM and it is responsible to capture malicious VM activities including packet injections. the implementation of the virtual firewall based on a modification to the physical host hypervisor kernel to add rules or modules allowing the VF system access to VM information and virtualized network interfaces moving packet traffic between VMs as well as and direct access to the virtual network switches. The Virtual Firewall can use the same features to then perform all firewall functions like forwarding, dropping and packet inspection, but without actually using the virtual network at any point.

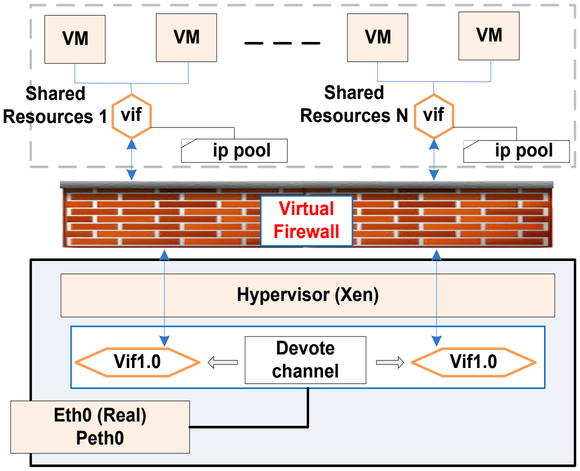

Fig. 4. Virtual firewall for securing the virtualized cloud computing infrastructure

IV. Discussion

Detection intrusion is major security concern in the Cloud. For ensure a high level of trust in cloud computing, we propose a new framework based on cooperative of Hy-IDS and mobile agents. This framework, allowed us to achieve three objectives, namely: intrusion detection at the front-end as well as the back-end of Cloud environment (i.e IaaS) of manner autonomous. Then, generating new signatures from malicious data or responses actions used by the firewall. Finally, dynamic deployment of updates between clusters in a cloud computing, using the newest signatures previously created. We used the signature generation algorithm and exchange of updates between clusters to achieve new knowledge and detect new kind of intrusion. About the virtual firewall, it receives its actions rules as signatures from IDS-M. Outstanding scalability is another strong point for this framework. When for example our VM migrates from server machine to another one (e.g. from Cluster-1 to Cluster-2), it is still possible to perform intrusion detection as our IMA can migrate just like VMs, and the same rule applies to other mobile agents (Transfer Mobile Agents and Mobile Agent Update). Moreover, this is the strength of our framework, which gives the IDS and NIDS great scalability and flexibility. Therefore, we have met almost all the mentioned challenges in our framework. Therefore, this framework has several advantages, it can be considered as an effective solution for the detection of intrusion into cloud computing. Thus, it can be used to protect people and property against risks of intrusion and aggression.

V. Conclusions

There is a major need of bringing security, transparency and reliability in cloud model for client satisfaction. Then, one of the security issues is how to reduce the impact of any type of intrusion in this environment. Thus in this paper, we propose an intelligent framework, which is based on the collaboration of the IDS-C, IDS-Cr, IDS-M and Mobile agents to detect attacks, and using the virtual firewalls to drop and block all types of attacks over hypervisor. As mentioned previously, mobile agents are used in our framework to investigate the VMs, transfer of malicious data, and exchange of update between different clusters in cloud computing.

Acknowledgment

We are thankful to God Almighty for giving us the knowledge and wisdom to complete this work. We are also thankful to our teachers and parents for their encouraging support.

References

[1] P. Mell and T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, Gaithersburg, USA, 2011.

[2] Venkateshwaran K, Anu Malviya, Utkarsha Dikshit, S.Venkatesan. "Security Framework for Agent-Based Cloud Computing", International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 3, Nº 3. 2015

[3] Priyank Singh Hada Ranjita Singh Mukul Manmohan. "Security Agents: A Mobile Agent based Trust Model for Cloud Computing". International Journal of Computer Applications, December 2011.

[4] A. Pandey, S. Srivastava. "An Approach for Virtual Machine Image Security". International Conference on Signal Propagation and Computer Technology (ICSPCT), 2014.

[5] H. TOUMI, A. EDDAOUI and M. TALEA." Cooperative Intrusion Detection System Framework Using Mobile Agents for Cloud Computing". Journal of Theoretical and Applied Information Technology 10th December 2014. Vol.70 No.1

[6] H. TOUMI, A. TALEA, B. MARZAK, A. EDDAOUI, M. TALEA, "Cooperative Trust Framework for Cloud Computing Based on Mobile Agents". International Journal of Communication Networks and Information Security (IJCNIS) Vol. 7, No. 2, August 2015.

[7] S. Roschke, Feng Cheng, C. Meinel. "Intrusion Detection in the Cloud". Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.

[8] Jean-Henry Morin, Jocelyn Aubert, Benjamin Gateau. "Towards Cloud Computing SLA Risk Management: Issues and Challenges", 45th Hawaii International Conference on System Sciences, 2012.

[9] Y. Jadeja, K. Modi. "Cloud Computing - Concepts, Architecture and Challenges". International Conference on Computing, Electronics and Electrical Technologies, 2012.

[10] Michael Armbrust , Armando Fox , Rean Griffith , Anthony D. Joseph , Randy Katz , Andy Konwinski , Gunho Lee , David Patterson , Ariel Rabkin , Ion Stoica , Matei Zaharia. "Above the Clouds: A Berkeley View of Cloud Computing", UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February 10, 2009.

[11] K. Benzidane, S. Khoudali, A. Sekkaki. "Autonomous Agent-based Inspection for inter-VM Traffic in a Cloud Environment". The seventh International Conference for Internet Technology and Secured Transactions, 2012.

[12] A. Elsayed, N. Abdelbaki. "Performance Evaluation and Comparison of the Top Market Virtualization Hypervisors". Eighth International Conference on Computer Engineering & Systems 2013.

[13] V.Nandgaonkar, A. B. Raut. "A Comprehensive Study on Cloud Computing". International Journal of Computer Science and Mobile Computing, April- 2014.

[14] Yashpal Singh, Kapil Gulati, S. Niranjan." Dimensions and issues of mobile agent technology". International Journal of Artificial Intelligence & Applications (IJAIA), 2012.

[15] Chirag N. Modi, Dhiren R. Patel, Avi Patel, Muttukrishnan Rajarajan, «Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing». Second International Conference on Communication, Computing & Security. 2012

[16] Dastjerdi, Amir Vahid, Kamalrulnizam Abu Bakar & Sayed Gholam Hassan Tabatabaei. "Distributed Intrusion Detection in Clouds Using Mobile Agents", In Proceedings of the 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences. ADVCOMP '09 pp. 175–180, 2009

[17] Lin Chen, Xingshu Chen, Junfang Jiang, Xueyuan Yin, and Guolin Shao, "Research and Practice of Dynamic Network Security Architecture for IaaS Platforms". Tsinghua Science and Technology. October 2014.

Hicham TOUMI received the MASTER degree in Network and Communication from Faculty of Sciences, CHOUAÏB DOUKKALI University El Jadida in 2013. He is preparing his PhD degree in the field of networks security in cloud computing using mobile agents approach at Faculty of Science Ben M'sik, MITI Laboratory, HASSAN II University.

Bouchra MARZAK was born in Casablanca, Morocco in 1989, received the MASTER degree in information processing from Faculty of Science Ben M'sik, Hassan II University Mohammedia-Casablanca in 2013. She is preparing her PhD degree in the field of clustering and dissemination data in vehicular networks at Faculty of Science Ben M'sik, MITI Laboratory, Hassan II University.

Amal TALEA is a graduate from Ecole Centrale Paris / specialized master in information system management. She also holds an engineering degree in computer and networking from National School of Engineer southern Alsace. Through her missions, she gained experience in project management, information systems governance, project portfolio management. Actually, she is preparing her PhD degree in Laboratory of Modeling and Information Technology, Department of Mathematics and Computer Science, Faculty of Sciences Ben M'sik, Hassan II University.

EDDAOUI Ahmed is a Professor-Researcher in Cloud Computing Security and resources management, Department of math and Computer sciences Faculty of sciences Ben M'Sik Hassan II University Morocco. PhD in Computer sciences (Information Security)

Mohamed TALEA was born in Casablanca, Morocco in 1964, Professor of Higher Education at the Faculty of Sciences Ben M'Sik, UNIVERSITY HASSAN II MOROCCO CASABLANCA. He obtained his PhD in collaboration with the LMP laboratory in Poitiers University, FRANCE in 2001. He obtained a Doctorate of High Graduate Studies degree at the University Hassan II in 1994. Actually, he is the Director of Information Treatment Laboratory. He has published twenty papers in conferences and national and international journals. His search major field is on Systems engineering, in security of system information.