Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-34

Collaborative Trust Framework Based on Hy-IDS, Firewalls and Mobile Agents to Achieve Effective Security Mechanisms in Cloud Environment

Hicham Toumi, Ahmed Eddaoui, Bouchra Marzak, Mohamed Talea

***Abstract*—The cloud has emerged as a successful computing paradigm allowing users and organizations to rely on external providers for storing and processing their data and making them available to others. Undoubtedly, security is one of the significant concerns in cloud computing. However, one of the major security concerns is to protect against network intrusions that affect confidentiality, availability and integrity Cloud resources and offered services. In this paper, we present a new framework, that allows collaboration between Hybrid Intrusion Detection System (Hy-IDS), Firewalls and Mobile Agents. Deploying security mechanisms in cloud computing environment to detect and stop intrusion attempts through our framework. However, the security mechanisms unfolds in four phases: using mobile agents in a virtual environment to collect malicious data in order to detect intrusions. Then, generation of appropriate response actions local and remote from malicious data, which were collected in the first phase. In addition, dynamic deployment of response actions through virtual or physical firewall. Finally, dynamic deployment of updates in cloud computing based on mobile agents. Therefore, the collaborative framework of security management could identify and address new distributed attacks more quickly and effectively**

***Keywords*— cloud computing, confidentiality, firewall, Mobile Agents, security.**

I. Introduction

Today, many organizations have begun to upload their vast quantity of essential information into public cloud. Nevertheless, the sensitive information uploaded into public cloud [1] is vulnerable to security risks such as availability, confidentiality and integrity of those organizations. Wherefore, the uninterrupted service of cloud technology attracts the intruders to gain access and misuse resources and services provided by Cloud service provider [2]. The anomaly or intrusion may be an attack to end user's private data, CPU utilization, bandwidth usage, processing power and storage capacity of the cloud system. Then, to protect the user's data and cloud resources from malicious activities, intrusion detection systems, firewall and mobile agents are the only permanent solutions [3]. Firewall is not suitable for detecting insider attacks. Some of the Denial of Service attacks, Distributed Denial of Service attacks and insider attacks are too complex to detect with firewall. In addition, a traditional network-based or host-based intrusion detection system does not suit virtual cloud environment [4].

Hicham Toumi, Ahmed Eddaoui, Bouchra Marzak, Mohamed Talea
Faculty of Science Ben M'sik, University Hassan II Casablanca
Morocco

In order to protect the cloud-computing environment, it is necessary to develop an anomaly detection component, which is suitable for detecting and reacting promptly to cyber threats in cloud computing systems [5]. Organizations are increasingly aware that they are likely to suffer a cyber-attack at any time, and that responding to the incident may cost them a considerable sum of money. However, the provider must protect and react promptly to cyber threats. Whether an attack is external or internal, most providers will focus on getting their firms back up and running. However, a robust response would also include an effective strategy to understand the nature of the incident and preserve evidence as to how the breach occurred, how they were able to bypass your cloud's controls and who was responsible. Understanding the incident provides a platform for enhanced security now and into the future. Nevertheless, if a cluster is infected, we could protect the other clusters the same attacks. Providers should have a combined approach of containing the breach, removing the threat, resuming the overall service and investigating the attack to learn from it and prevent it from happening again. The problem is these responses tend to remain quite separate, and we find that most of individual clients and organizations lack experience in evidence preservation, especially if the breach involves cloud service providers. Consequently, any recovery process undertaken by the victim organization, threatens to trample on important evidence that could be used to discover the details of the breach. However, to overcome this problem, we propose an intelligent framework, which is based on collaboration of Hybrid Intrusion Detection System (Hy-IDS), Firewalls and Mobile Agents [6][7][8]. Therefore, it allows reaching the following aims or objectives: detection intrusion in a virtual environment using mobile agents for collecting malicious data, generating new signatures from malicious data, which were collected in the first phase. Then, dynamic deployment of remote response actions using virtual firewall, dynamic deployment of updates between clusters in a cloud computing.

The rest of this paper is organized as follows: The section II presents theoretical background and discusses some related works. 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

Cloud service providers have to ensure that the cloud infrastructure and services provided are safe and secure. Besides, they have to assure that the consumers' data are protected unless and otherwise they use strong passwords and authentication mechanism. Trusting a cloud system depends strongly on the deployment model, as governance

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-34

of data and applications are outsourced and are out of user's control. Since the cloud service makes the accessibility of the data with any network devices such as public computers and mobile devices, this facility sometimes makes the situation still worse because some devices do not have the required level of security. Because of this increased exposure of the user's data, the security concern increases [9]. This may creates problems such as Loss of control, Lack of trust (mechanisms) and Multi-tenancy [10].

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 [6]: there are efficiency and reduction of network traffic, interaction with real-time entities, life cycle of mobile agent and convenient development paradigm.

A firewall is a software and/or hardware, which allows enforcing network security policy; it defines what types of communication allowed on this computer network. The main disadvantage of a firewall is that it cannot fully protect the network and subnet from attacks from the inside; it is unable to stop internal attacks [13][14]. However, the firewall provides the benefit of added security to strengthen a network when used in conjunction with an IDS/IPS [15]. Intrusion detection system is such a security model which examines the packet over the network and identifies the threats in the network [11]. IDS has been evolved from firewalls. Simply, firewalls are the predecessor of IDS. Even though firewall provides security, it has many shortcomings [12].

III. Trusted framework based on hy-ids and firewalling to improve security in cloud computing

Our designed dynamic network security architecture for IaaS platforms is based on the mechanisms of host investigation and policy management, security supporting services, and accords to the P2DR (Policy, Protection, Detection, and Response) framework and architecture. In our previous work, we presented an approach based on the improvement of collaboration among Hybrid Intrusion Detection System (Hy-IDS), Responses Generation Algorithm (RGA), Mobile Agents (MA). Then, we developed the attack detection concepts. However, we will focus more on the responses to attacks. It is not easily to detect the strong attacks, from where mitigating this threat requires greater intelligence on attacks and specialist resources in response to detection of an incident or threat. In addition, we start with the components of our framework, and their manner of reacting against attacks.

A. *Our proposed hybrid framework on cloud computing*

The collaborative framework proposed is based on Hybrid Intrusion Detection System (Hy-IDS), Mobile Agents and Firewalls. Therefore, our hybrid intrusion detection system consists of three types of IDS namely Intrusion Detection System Control (IDS-C), Intrusion Detection System center (IDS-Cr) and Intrusion Detection System Master (IDS-M), which are dispatched in the strategic security points of cloud.

- **IDS-C**: VMs are further managed by hypervisors, also known as Virtual Machine Monitor (VMM) and are basically installed on server hardware (Node Controller "NC"). Thus, as shown in figure 1, 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. However, 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).
- **IDS-Cr**: it is installed in the front-end Cluster (Cluster Controller "CC") for the monitoring of nodes. In addition, it generates new signatures. It consists of an Intrusion Detection System (IDS) and Responses Generation Algorithm (RGA).
- **IDS-M**: it is placed in the front-end Cloud (Cloud Controller "CLC") for the monitoring of Clusters and Management of Update (new signatures). The IDS-M is based on Intrusion Detection System (IDS) and Living Environment of Mobile Agents named Agents Agency (AA).

Cloud Controller is a network area that includes many cluster control domains. As shown in figure 1, it is equipped by an Intrusion Detection System Master IDS-M. IDS-M is responsible for distributing security patches or updating related security software in its administrative cloud computing domain. Cluster Controller (CC) is a trusted network area identified by an Intrusion Detection System Center (IDS-Cr). However, the IDS-Cr is a programmable node that can manage and control security systems, such as detect a breach of security, and the system response to the attacks. In addition, the IDS-Cr makes a decision about the security policy and distributes it to the security systems within its cluster control domain. It controls dynamic deployment of active security module in its domain. The IDS-Cr or The IDS-M is an active node that can adapt itself to different states in runtime. It can dynamically change its own functions. Finally, domain of protected nodes (NC) is composed of several classic nodes as physical servers and databases, which will be monitored and managed by IDS-C.

B. *Intrusion detection system in cloud computing environment*

We discuss the functioning of our framework based on figure 4. When the attacking host initiates an attack from external network, the framework reacts as depicted below:

Static Agent placed in VM will send an alert message to IDS-C. Then, IDS-C uses Investigative Mobile Agents (IMA) for collecting evidences of attack from all the attacked VMs for further analysis and auditing. In the case of an attack, IDS-C aggregate malicious data, then placing them in its temporary database. In order to present an initial protection, IDS-C executes initial local responses in virtual firewall, which is placed over hypervisor [16]. In addition, IDS-C generates Transfer Mobile Agents (TMA) for notifying IDS-Cr placed in the Front-end cluster. Moreover, IDS-Cr dispatches Investigative Mobile Agents to any IDS-

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-34

Cs those send TMA for aggregation and collection of their malicious data from the database temporarily.

As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response on at least automated notification is the best solution for this purpose. In order to control and allow easy and dynamic deployment of the active actions response. We propose a logical architecture, which permit to detect intrusions and reacting promptly to cyber threats.

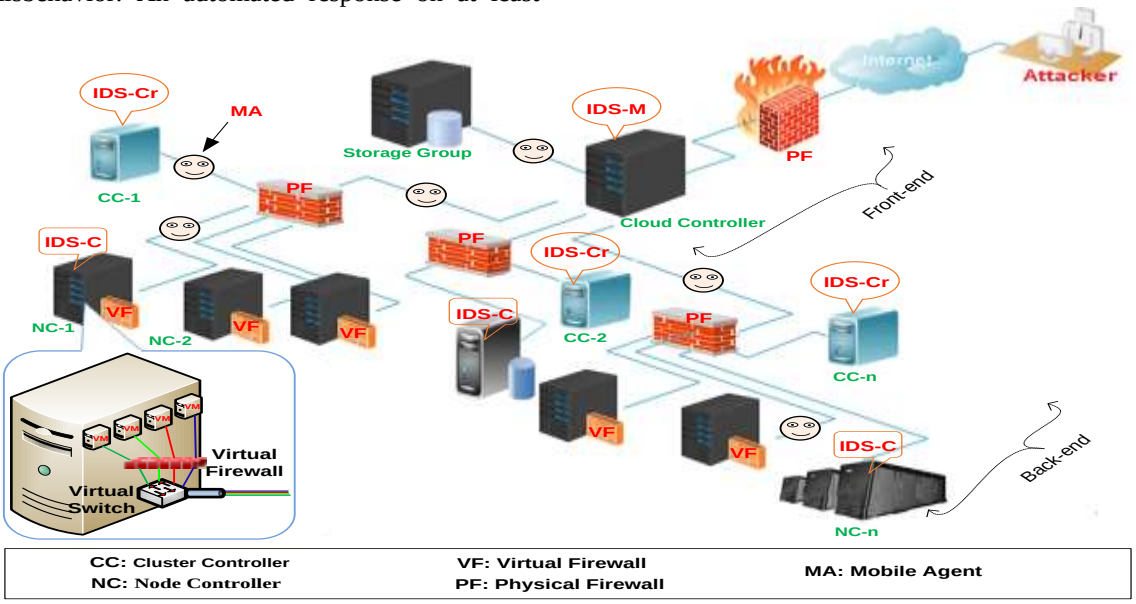

Figure 1. Collaborative trust framework in cloud computing

C. *Reacting promptly to cyber threats*

You will need to formulate a plan to have a good security policy. Therefore, we believe organizations need to ensure each of the responses (containment, eradication, restoration and investigation) are a priority and form part of a considered response strategy. In addition, achieving that takes careful preparation and a comprehensive incident response plan. In formulating an effective plan of our framework, we would suggest at a minimum the following:

- Analysis of the incident to identify the method of compromise and prevent further spread. Identify the root cause of the opportunity for the method of compromise and develop plans for remediation of security vulnerabilities discovered.
- Effective planning for business recovery that minimises downtime in the event of an incident. Investigate what information was placed at risk, what evidence is available/preserved and the implications the unauthorised access.
- Continual proactive testing of all elements ensures the strategic response planning remains relevant and fit for purpose.

It is only with a transparent, comprehensive plan in place that your organization can respond promptly, effectively to the rapidly evolving threat landscape and thereby freeing your business to grow, transform and expand [17].

D. *Using IDS-Cr to Process Global Action Responses*

If there is an attack detection, IDS-Cr receives report form IDS-C; this report provides a global picture of the data stream. Then, it uses IMA to recover malicious data from Database Temporary (DBT) existing in IDS-C.

1) Responses generation algorithm

In figure 2, different malicious data retrieved by the IMA, are given as input to Responses Generation algorithm (e,g: Apriori algorithm, Signature Apriori Algorithm) [18].

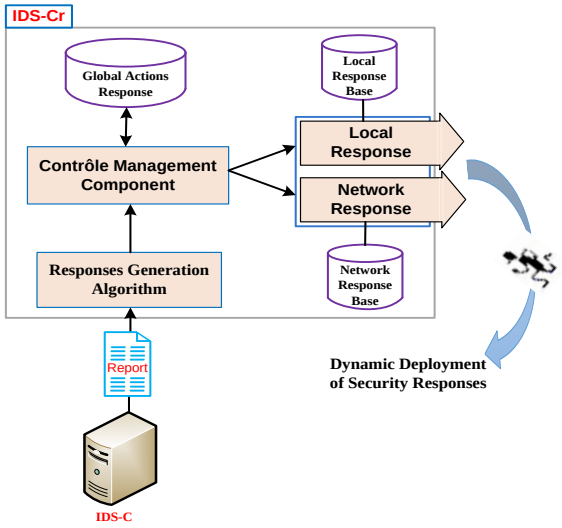

Figure 2. Processing of new responses of attacks

However, it searches the space of all possible patterns for rules that meet the user-specified support and confidence thresholds. As an output, it generates new global actions response like rule or signature, which will be used by NIDS and Firewall [19]. A Responses Generation Algorithm may result in a large number of rules, which may turn out to be unusable or inapplicable for analysis. Further, some rules may have no benefit on firewall action such as repeated

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-34

rules or rules, which does not yield any action. As a result, these rules are filtered for further analysis. The major objective is to generalize specific and unique rules to more general rules.

2) Control management component

It performs an initial check each new arrived security function or response to an attack. If these responses to attacks passes this checked, they are stored in Global Action Response. Then, it divides the security responses in two types: Local Action Response and Network Action Response (remotely). A security function or response to an attack could for example include signature detection functionality, anomaly detection algorithms or any kind of security action.

3) Local response component

The local or node security responses present a set of local response actions to attacks (e.g., disable the user account, install filtering rules, modify a host's policy, kill processes and connections and connections associated with attacks). They are based on the attack type and local policy constraints. We use local action response to ensure security management in hypervisor-based virtualization. Hypervisor is management tools and it is building a trust zone around hardware and the VMs. Other available Virtual Machines are under the probation of the hypervisor, and they could rely on it. The users are trusting that administrators will do what they can to do provide security to their virtual Machines. It presented in figure 3, by Protection of a Node. Therefore, our aim is to block the attacks near of their sources. Consequently, security policy will unfold in three phases namely: firstly, Protection of a Node, then Protection of Cluster and finally protection of cloud. The first is assured by responses local, which are created by IDS-Cr. However, protection of cluster and cloud is assured by Network Reponses, which will be presented as follow.

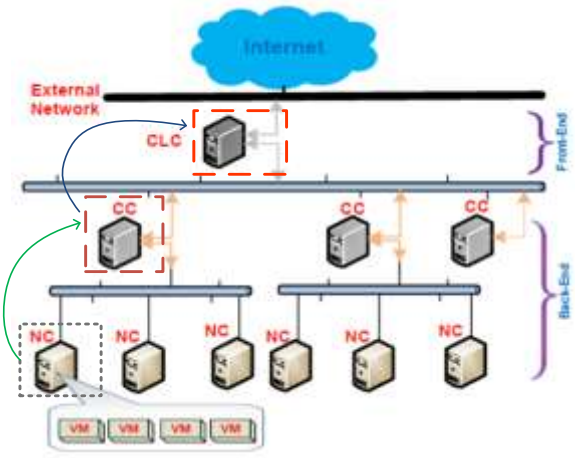

Figure 3. Progress of responses to attacks in cloud

4) Network response component

Then network security response to an attack. They are deployed and executed on the network. In order to dynamically deploy these responses, we use mobile agents that allow dynamic deployment of new programs into the network. With mobile agents in place, we can dynamically deploy the network security responses into the network whenever an attack is suspected. Nodes on the network in the cluster receive and execute the security responses, and possibly return values or forward it along the others nodes. The network security responses are deployed into the network and reprogram nodes, firewall, intrusion prevention system and routers. However, they can do more than that. They can update components of the security system node and keep it up to date about new attack signatures.

As shown in Figure 4, after the generation of local and network responses, IDS-Cr deploy the network responses in the physical firewall-cluster, which used to protect the cluster. In addition, it sent back the rectified local responses to virtual firewall over the hypervisor. Then, it sent the new network responses to cloud controller (IDS-M). Therefore, IDS-M prepares the network responses in the form of updates. Then, using the Update mobile agent to implement the new rules in physique firewall cloud. Thereafter, deploying update intra-domain of clusters and intra-domain of nodes.

IV. Discussion

For ensure a high level of trust in cloud computing, we propose a new framework based on cooperative of Hy- IDS, and mobile agents, which will be combined with firewalls. It has allowed us to achieve three objectives, namely: intrusion detection at the front-end as well as the back-end in Cloud environment. Then, using malicious data to generate new signatures and responses actions, which will be used by NIDS and Firewalls. In addition, dynamic deployment of updates in clusters of cloud. IDS-M sends the new actions of responses to physical and virtual firewall. Therefore, making use of VF at VM-level will help the VM customers to enhance the VM security during migration and protect them against attacks on the hypervisor. Thus, by using technology at their own disposal it is possible to create secure environment for VM migrations. Often misconfiguration leads to administrators' lack of motivation. However, in case of false or incomplete rule, the firewall can produce incorrect behavior. To overcome this issue, we could make the configuration automatic and dynamic of our virtual firewall, based on the updates sent by IDS-M. Provider could provide firewall-as-a-service and managed firewall to customers who do not have the necessary resources of security. Outstanding scalability is another strong point for this framework. If there is a migration of a VM from its server machine to another one, it is still possible to perform intrusion detection because our IMA can migrate just like VMs. Therefore, 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.

V. Conclusions and future works

Cloud Computing 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. There is a major need of bringing security, transparency and reliability in cloud model for client satisfaction. Therefore, we have presented security issues for model infrastructure as a service (IaaS) in cloud computing. As presented in this paper, communication

Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology - IPCT 2016.

ISBN: 978-1-63248-099-6 doi: 10.15224/ 978-1-63248-099-6-34

between VMs, storage, virtualization, and networks are the biggest security concerns in Cloud. Therefore, we propose an intelligent framework to secure them. It is based on the collaboration of the IDS-C, IDS-Cr, IDS-M, Firewalls and Mobile agents. As mentioned previously, mobile agents are used in our framework to investigate VMs, to transfer malicious data and exchange of update between different clusters in cloud. In addition, using mobile agents to conduct investigations of attacks without human intervention, learn a system to recognize new patterns of attacks. Therefore, this framework has several advantages. Then, it can be considered as an effective solution for the detection of intrusion into cloud computing. Thus, it will be used to protect people and property against risks of intrusion and aggression.

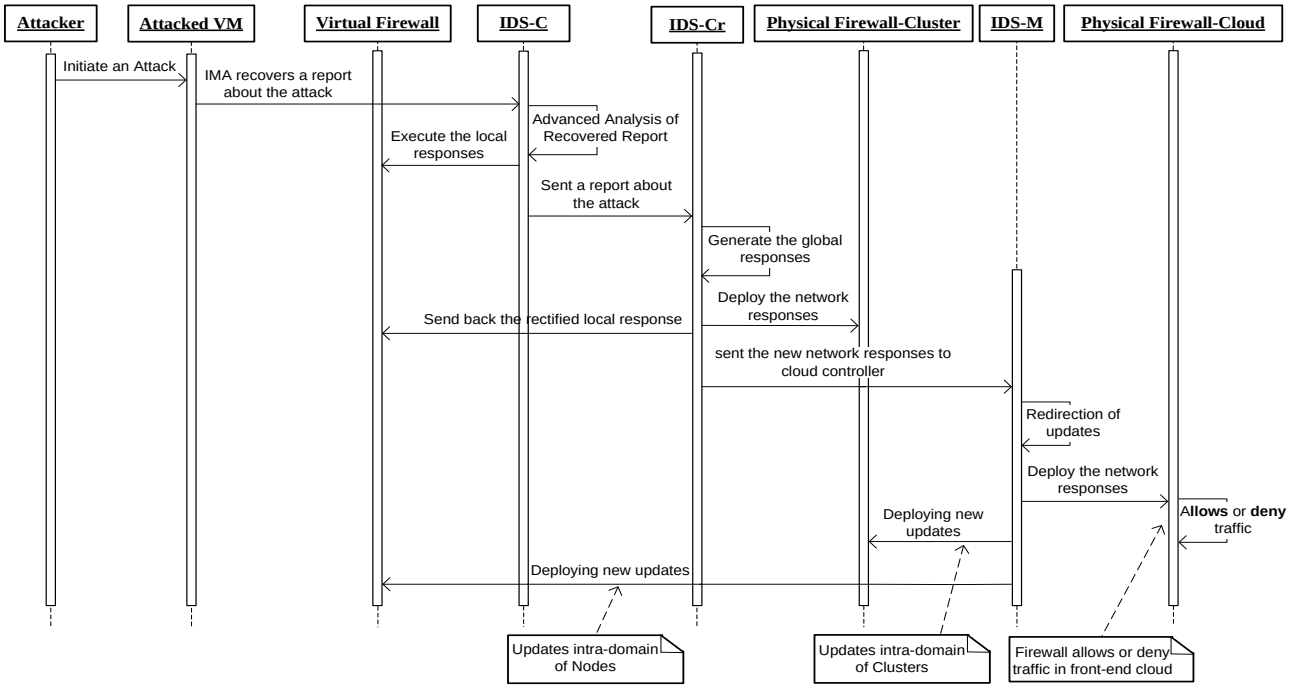

Figure 4. Principle of our framework

References

[1] N. Pandeeswari and Ganesh Kumar. "Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN", Mobile Networks and Applications, Springer, 2015.

[2] OktayU, Sahingoz. Attack types and intrusion detection systems in cloud computing. In: Proceedings of Sixth International Information Security & Cryptology Conference, 2013

[3] Hai J, Guofu X, Deqing Z, AVMM-based intrusion prevention system in cloud computing environment. J Supercomput Springer Sci, 2013.

[4] Vieira K, Schulter A, Westphall C, Westphall C, Intrusion detection techniques in grid and cloud computing environment. IEEE, 2010.

[5] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti and Rajkumar Buyya, 2015. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions ACM Comput. Surv. 1, 1, 2015.

[6] 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

[7] 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.

[8] H. Toumi, M. Talea, K. Sabiri, A.Eddaoui. "Toward a trusted framework for cloud computing", International Conference on Cloud Computing Technologies and Applications, IEEE, 2015.

[9] Kaaviyan Kanagasabapathi, S. Deepak and P. Prakash. "A Study on Security Issues in Cloud Computing", Springer India 2016.

[10] Keiko H, DavidGR, Eduardo FM, Eduardo BF. An analysis of security issues for cloud computing. J Internet Serv Appl, 2013.

[11] Vikas Mishra, Vinay Kumar Vijay and Satyanaryan Tazi, "Intrusion Detection System with Snort in Cloud Computing: Advanced IDS", Proceedings of International Conference on ICT for Sustainable Development, Advances in Intelligent Systems and Computing, Springer Science & Business Media Singapore 2016.

[12] J. Amudhavel, V. Brindha, B. Anantharaj, P. Karthikeyan, B. Bhuvaneswari, M. Vasanthi, D. Nivetha and D. Vinodha. "A Survey on Intrusion Detection System: State of the Art Review", Indian Journal of Science and Technology, March 2016

[13] S. Beg, U. Naru, M. Ashraf, and S. Moshin, "Feasibility of intrusion detection system with high performance computing: A survey." Int. J. Advances in Computer Science vol. 1, Dec 2010, pp. 26-35.

[14] C. Wang, Z. Zhang, and X. Song, "Research on the Information Security Technology of University Campus Network," in Advances in Computer Science and Information Engineering, Springer, 2012.

[15] Waleed Bul'ajoula, et al. "Improving network intrusion detection system performance through quality of service configuration and parallel technology". Journal of Computer and System Sciences. 2015.

[16] N. AFZALI SERESHT, R. AZMI. "MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach". Engineering Applications of Artificial Intelligence 35, 2014.

[17] Juan J. Villalobos, et al. "Energy-Aware Autonomic Framework for Cloud Protection and Self-Healing", International Conference on Cloud and Autonomic Computing, IEEE- 2014

[18] Shanshan Qi and Cora Un In Wong. "An Application of Apriori Algorithm Association Rules Mining to Profiling the Heritage Visitors of Macau". Information and Communication Technologies in Tourism- Springer International Publishing Switzerland 2015

[19] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, Mqhele Dlodlo. "Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework", Journal of Network and Computer Applications, Elsevier-18 January 2016