ASA-based framework for detecting intrusion in Cloud Computing Environment

Amal BENFATEH†, FATIM GHARNATI†, Tarik Agouti††

†Intelligent management of energies and information systems laboratory, Physics Department, Faculty of Sciences, Cadi Ayyad University, Marrakesh, Morocco
††Computer Science Department, Faculty of Sciences, Cadi Ayyad University, Marrakesh, Morocco

Summary
The distributed and open structure of cloud computing and its services become an attractive target for potential cyber-attacks. The aim of using initially agents in the cloud is to exploit their speed of treatment and their negotiating process to choose the best resource for the Cloud subscriber. Therefore, in this paper, we propose a cooperative framework based on the concept of an artificial security administrator (ASA) to monitor and manage system incidents on behalf of a security human expert by bringing together the sense of analysis and learning ability of humans, moreover, the speed of computing and complexity management of multi-agent system.

Keywords
Cloud Computing, intrusion detection, cognitive agent, mobile agent, gap evaluation, artificial security administrator, cooperative system.

1. Introduction

The field of information security has become vitally important to the safety and economic well being of society as a whole. The rapid growth and widespread use of electronic data processing and electronic business conducted through the massive use of the wired and wireless communication networks, Internet, Web application, cloud computing along with numerous occurrences of international terrorism, raises the need for providing information security systems through the use of tools as: firewalls, intrusion detection and prevention systems, encryption, authentication and other hardware and software solutions [1, 2, 3].

What we call intrusion means information system penetration, but also attempts of local users to gain higher privileges than those attributed to them, or attempts of administrators to abuse their privileges.

The fully distributed and open structure of cloud computing and services becomes an even more attractive target for potential intruders. This kind of systems can be exposed to several threats including threats to the integrity, confidentiality and availability of its resources, data and the virtualized infrastructure which can be used as a launching pad for new attacks as indicated in [4]. The problem becomes even more critical when a cloud with massive computing power and storage capacity is abused by an insider intruder as an ill-intention party which makes cloud computing a threat against itself. Lack of full control over the infrastructure is a major concern for the cloud services' consumers. It signifies the role of intrusion detection system in protecting the users' information assets in cloud computing.

The use of artificial intelligence as well as distributed artificial intelligence can give a new breath to the cloud computing environment (CCE) by the possibility of integrating new parameters favoring a better adaptation to the CCE customer's need.

In the literature, there are some works that have taken this area into account in their research like in [5], where the authors propose and test four different distributed intrusion detection methods, and in [3], Venkateshwaran and al suggest algorithms to solve some security Cloud Computing issues to ensure that there will be no intervention of any malicious activities during the agent interaction. However, in [6], Demer and al propose enhancement of the DoS/DDoS detection by optimizing agent location by focusing on a problem of the determining of the true origins and mechanisms of attacks. In [7], Zamani and al presented a new model of artificial immune system AIS to overcome some unsolved problems in IDSs like weakness against DDoS attacks, suffering from high false positive and high false negative rates. As for [8], Duraipandian and al propose an Intelligent Agent Based Defense Architecture for DDoS Attacks in order to verify the hop-count information used by the hop count filtering mechanism. Yet, in [9], Madeson and al describe a new approach to parallelization of the conditional independence testing as experiments illustrate that this is by far the most time consuming step, this makes it possible to take advantage of multi-agents systems to improve time efficiency of structure learning.

This paper proposes an artificial security administrator - based framework in order to automate intrusion detection process using a cooperative-agent system. Some background information about cloud computing

Manuscript received October 5, 2017
Manuscript revised October 20, 2017

environment, Intrusion detection systems, mobile agent are giving in Section 2. Section 3 presents related studies. Section 4 describes in detail the architecture of proposed model and graphical representation of the interactions between the different system components in chronological order. Section 5 contains some analysis and discussion of this work. Section 6 describes the conclusion reached after evaluating the model and some future work.

2. Material and methods (backgrounds)

2.1 Cloud Computing Environment:

Cloud Computing is a fast developing technology which provides scalable data storage to large and various services without the hassle of installation and maintenance. Since there is an increase in number of users for the Cloud services, there is a demand on Cloud service providers. Hence, there is a need for dynamic and automated Cloud service composition. [1, 2]

The National Institute of Standards and Technology's definition of cloud computing identifies five essential characteristics: [10] On-demand self-service, large network access, Resource pooling: cloud, measured service, Rapid elasticity.

The costumer has to begin by deciding the appropriate service model to select a cloud solution. The most popular services that cloud offers are: Software as a service (SaaS) Platform as a service (PaaS), Infrastructure as a service (IaaS) .

After the service model, the future consumer might think about how he would benefit from the Cloud. So we have four models of the cloud deployment: Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud.

Basically, Cloud is a good IT infrastructure well maintained. Its main objective is to discharge clients from the infrastructure management. This will help the clients to focus only on their activities. However, besides security issues of IT systems, the cloud Computing brings some more specific issues such as: Data security (confidentiality, access controllability, integrity), Network security (packet sniffing, man in the middle, IP spoofing, Port scanning, network penetration), Web application security (injection, broken authentication and session management, cross-site scripting, invalidated redirects and forwards), and Virtualization security (misconfigurating virtual hosting platforms, guests and networks, lack VM visibility across the enterprise, failure to consider user-installed VMs).

2.2 Intrusion detection System:

Intrusion detection is a mechanism of monitoring a network or systems for malicious activity or policy violation. In recent years, IDSs are changing gradually from host-based OS dependent systems to distributed systems that often run multiple operating systems [11]. The first generation of distributed IDSs has client-server architecture while the second one presents a hierarchical architecture. In the latter one, data collected at leaf nodes are sent to intermediate nodes to be pruned and aggregated. The neat data are then conveyed to the higher levels to reach the server(s). In modern generation of IDSs, agents are used to collect data in various nodes and interact with each other in the network to make local and ubiquitous detections possible.

IDSs are often divided into two categories: misuse detection and anomaly detection. Misuse detection techniques examine both network and system activity for known instances of misuse using signature matching algorithms. This technique is effective at detecting attacks that are already known. However, new attacks are often missed giving rise to false negatives. Anomaly detection systems rely on constructing a model of user behavior that is considered “normal”. The detection of new attacks is more successful using the anomaly detection approach as any deviant is classified as an intrusion. [7]

2.3 Agent System:

A mobile agent is a program which can move from a computer to another autonomously and executes a task on behalf of a user. It has a capability of traveling through networks, interacting with machines, collecting information and returning to its dispatcher after it is done. It is used in order to reduce the network load, overcome network latency, adapt to the environmental changes. Mobile agents help to move the intrusion detection code to the data instead of moving data between hosts for analysis. Since they can execute their tasks even when they are disconnected from their dispatchers, the failure of the controller unit of mobile agents doesn’t stop the ongoing intrusion detection tasks. This makes the system more reliable.

3. Proposed framework:

3.1 Framework principle:

We need a model that could supervise and monitor a system especially complex system on behalf of a human security administrator. This mode allows us to gather professional expertness and heuristic strategies of security administrators. Human is aware and mindful entity.

Moreover, he doesn't have just intellectual dimension but also intuition. It is this latter quality that we are looking for in modern generations of intelligent agents. Our system should be:

- Reactive and autonomous because it is necessary to respond immediately and dependently of events.
- Cooperative and Communicative with reports and logs which are made in relation with other databases and past experiences.
- Flexible, because the factors and parameters may change during the time or special circumstances.

Learning ability is very significant in this framework owing to the fact that its components should learn and benefit of past incidents.
We can touch that in to two distinguished architectures: reactive and cognitive. For reactive architecture or reactive agent, each behavior continually maps perceptual input to action output. There is neither memory of his history, nor explicit purpose, nor explicit representation of the environment or restricted means of communication. However, a cognitive architecture refers to explicit symbolic model of the environment in which decisions are made via logical reasoning, based on pattern matching and symbolic manipulation.
Hence, we use both architectures in components framework in order to cover whole human aspects. Thereby, we conceive some agents as reactive agent, like supervisors, to perform specific missions without developing learning aspects. It is the case of costumer agent, virtual machine agent and provider agent.
As for the remaining agents, we conceive some of them as cognitive architecture like evaluator agent and security depository agent, and hybrid architecture like master agent. For this latter, we choose it to be hybrid because, first of all, it is conceived as reactive agent tentatively, virgin of all acquired skills and then, in the course of time, scenarios and plights, it develops and acquires experiments.

3.2 Components of framework:

The purpose of this work is enhancing a process of detecting, best as possible, errors and risks, named here a gap, in the Cloud in real time.

For ending up at this aim, a proposed framework consists of the following components (figure 1): Detectors (Provider agent (PA), Hypervisor detector agent (H-DA), customer agent (C-DA)), Master agent (MA), security depository agent (SDA), Evaluator agent (EA), and Log editor agent (LEA).

Detectors: mobile agents who is responsible on looking for any gaps during running tasks by simple knowledge of pattern matching. There are two detectors in the framework: customer detector agent (C-DA) and hypervisor detector agent (H-DA). These latter have as function catching as fast as possible any abnormal conduct. After detecting a gap, they dispatch an alarm signal to the master agent to seek the true meaning of the alarm and waits for its acknowledgment.

Customer-Detector Agent (C-DA): a reactive mobile agent of detector type endowed in every subscriber's reserved system in the cloud. Its main task is to look for if there is any suspicious process.

Observer agent (OA): it's the nearest agent from activities of subscriber in order to closely monitor his behavior to find its slips, and then to build its generic error profile named subscriber's generic error profile (SGEP). This latter will be at disposal of the master agent to, on the one hand to evaluate the detected gap, and on the other hand to choose the appropriate secure solution. Moreover, this agent edits security requirements recommended by the user in the requirement subscriber's entity (RSE).

Hypervisor detector agent (H-DA): a reactive mobile agent of type detector endowed in the hypervisors of the cloud. It keeps eye on hypervisors activities. Hypervisor is the software that controls the layers between the hardware and the operating systems.

Provider agent (PA): it is a reactive agent that is endowed in a system provider to propose manual or occasional corrections or notify him about missed resources that are required by SDA.

Security depository agent (SDA): an agent who is responsible firstly on choosing a security appropriate solution according to declared alert especially in case of virgin MA and then implementing this choice from SRL to overcome a current risk. But if it doesn't find the suitable tool, it sends to the provider agent for missing resources.

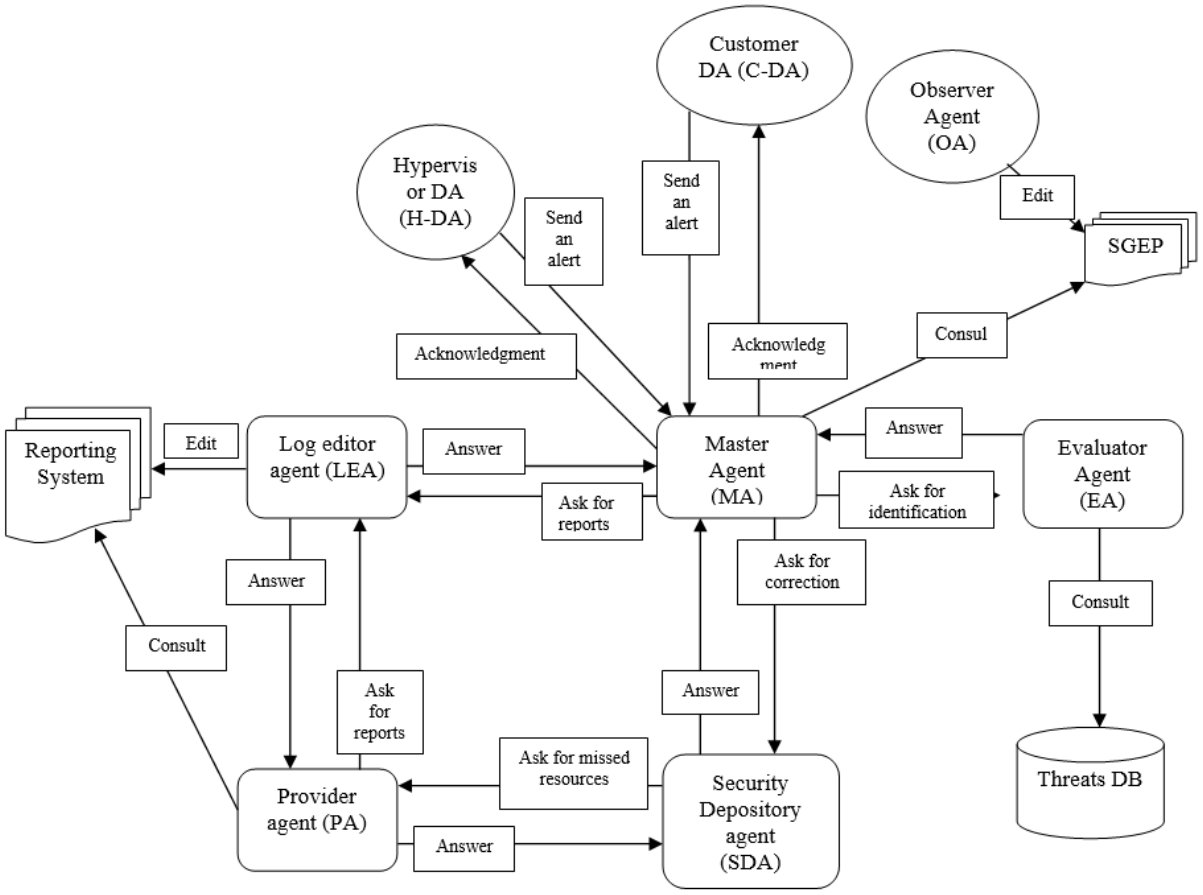

Fig. 1: ISAA-based framework for cloud computing environment

Evaluator agent (EA): it is an agent that remains in contact with the threat databases and vulnerabilities. It is to him to judge and to give a gravity degree of the gap in question, taking into account the security requirements specified by the subscriber in his RSE (requirement subscriber's entity).

Log editor agent (LEA): it is an agent which receives reports from the MA and updates its report system.

Master agent (MA): it is the lever of the framework. It is a hybrid agent endowed by a memory in order to learn from every past event. After receiving an alarm signal, it sends back an acknowledgment to the detector to say that was received. If it has no acquaintance about it, it communicates with the EA to qualify the gap in question. If it is negligible, it doesn't intervene. But if it corresponds to a classic event, MA tries again to resolve the problem itself else it asks SDA for help about available resources to remedy this gap. For Each action, it point out it in the LEA as a report.

3.3 Scenarios of components:

- A case of virgin MA:

As shown in figure 2, once one of the detectors has observed an inappropriate gap in the cloud, it sends an alert signal to MA, this latter has no experience or acquired acquaintance; therefore he sends a request for identification to the EA. This agent connects to the different threats databases and then sends its reply.

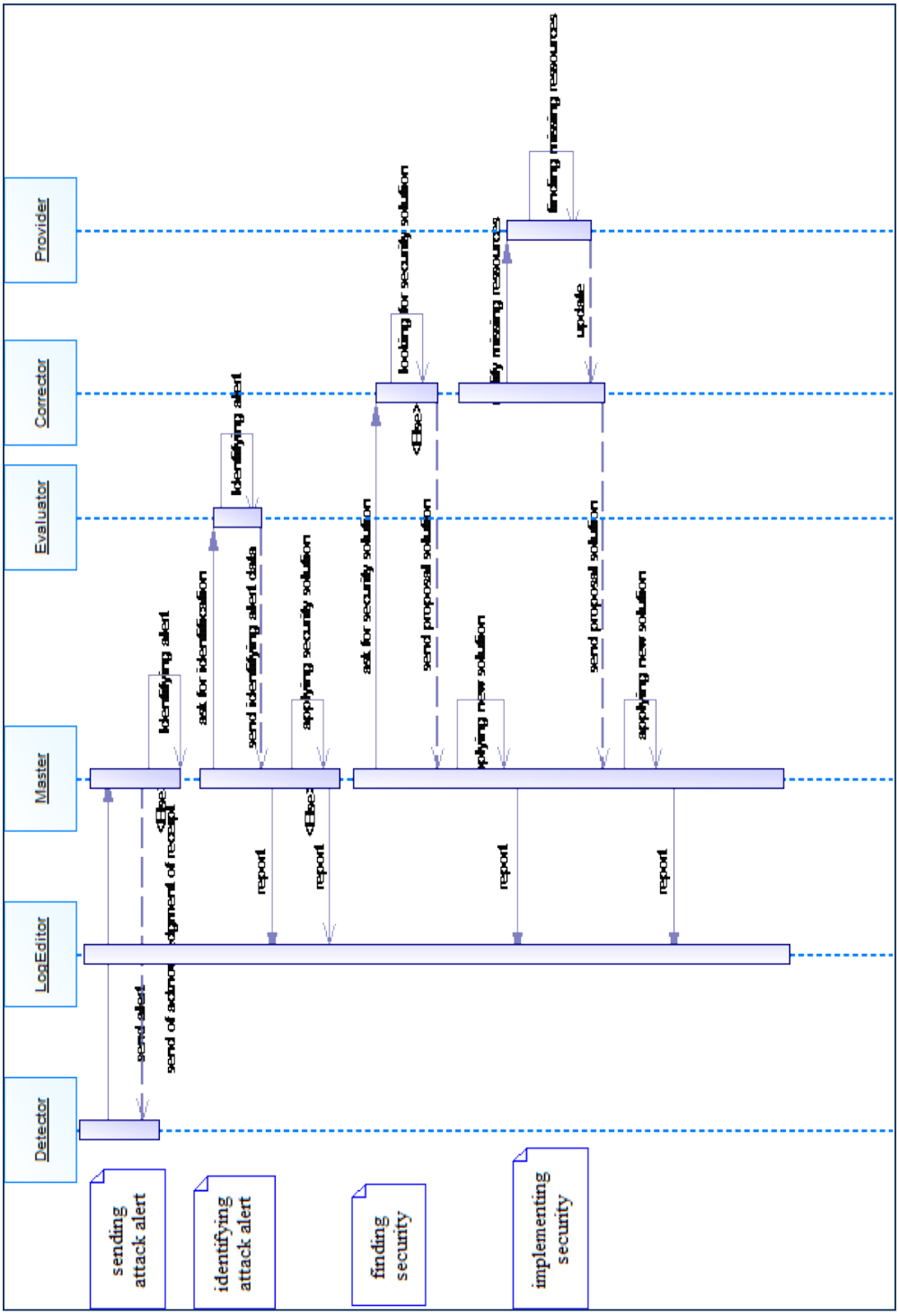

Fig. 2: interaction diagram of proposed framework

MA takes it into account by memorizing it and notifying its type to LEA and then sends another request to the SDA asking for the appropriate solution to overcome this error. This last agent answers after automatically applying the proposed solution. The master receives the answer by memorizing it as usual and informs the tracer that the problem is solved.

3.4 Intervention mechanisms:

Our framework has three main roles to fulfill its mission: observation of running components, detection of gaps, evaluation of the gap and evaluation of its gravity in case of a negative detection.

3.4.1 Observation mechanism:

The proposed framework is based in the first level on establishing of a set of mobile agents moving along a system to monitoring its working and subscriber's conduct. Each mobile agent is specialized in one type of gap. This mechanism concerns especially detectors (C-DA, H-DA).

3.4.2 Detection mechanism:

Some errors are easily detectable by the shape or some characteristics. Others are much more complex to be detected. For this reasons, the detection phase is based on a three-level architecture inspired by the Rasmussen model on human reasoning (figure 3). The first level, from the bottom to the top, concerns detectives (C-DA and H-DA). The remaining levels concern MA in cooperation with other agents like SDA, OA and EA.

3.4.3 Evaluation Mechanism:

Once a gap is detected, the next step begins: the evaluation. In the case of a virgin MA, this phase is managed by EA through its links with local and external databases, in which a transaction flow is established between the mentioned agents to qualify the nature of the gap and Its severity in case of a real error. In the case of a cognitive MA, it is this latter who takes over the evaluation by his leaning ability from the past incident.

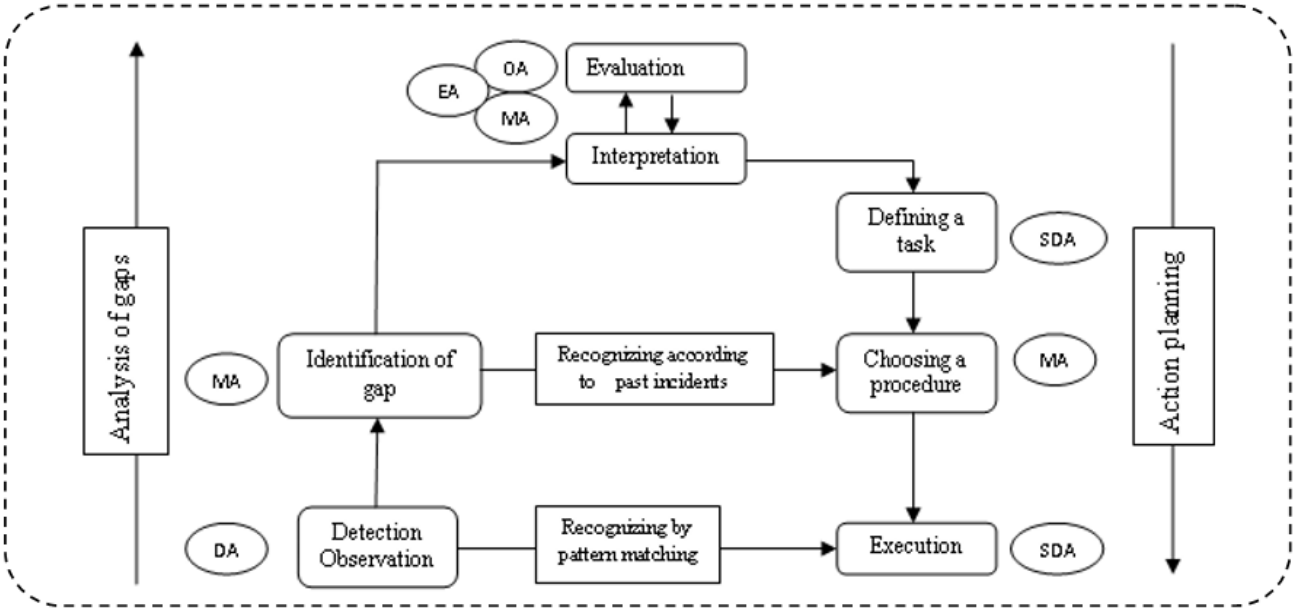

Fig. 3: Graphical representation of the different behavioral aspects of the agents in the face of the gap detection.

4. Discussion:

This paper adopts the learning capacity approach for the new generation of cognitive agents, in order to implement it in a system whose aim is, firstly, detecting intrusions and, secondly, placing proper security solution.

4.1 Detectors focus:

This framework makes use of the mobility of the detectors (C-DA, H-DA, and OA) to closely monitor the flow of the cloud taking into account the behavior of the user against the system to generate what is called its error profile. This latter sometimes allows us to anticipate some risks by knowing how to copes with the normal state and the critical state. But that does not prevent that there are challenges to be overcome such as detection mistakes. We mean by this term the false-positive detection: to detect an self object as an intruder and then to put it in quarantine; And false-negative detection: to consider a malicious object as an self object and then ignore it. To overcome this problem, we consider creating a training mechanism (maturation) of the detectors.

4.2 MA focus:

The fact of having a cognitive agent in a distributed system like Cloud is very beneficial because of its learning ability. This quality makes it a mastermind which reigns the system in its both interventions (evaluation and correction) that looks much like the conduct of a human administrator. But this progress brings us back to a centralized architecture. The virginity (the initial state) of MA gives the system some equilibrium due to fairly tasks distributing on the different components; but as soon as the MA learns from the past incidents and the scale is leaned substantially towards him.

5. Conclusion

In this paper, we have presented a cooperative framework based on many gender of agents like mobile agent (detectors), reactive and cognitive agent (MA) in order to secure the cloud based system on behalf of security human expert. These agents have to ensure task management, detection and evaluation of gaps and then management of incidents… therefore, this cooperative work brings together, firstly, the sense of analysis and learning ability nearly like humans and secondly, the speed of computation due to using cooperative framework based on multi-agent system. In the future work, we consider developing the instantiation capacity of agents so as not to burden and disrupt the functioning of subscriber's cloud system in case of overloading for example.

References

[1] Kwang Mong Sim, J OctavioGuetierrez-Garcia, "Agent-based cloud service composition," Springer Science + Business Media, LLC2012.

[2] Kwang Mong Sim, "Agent-based cloud commerce," Proceedings of the 2009 IEEE IEEM, 978-1-4244-4870-8/09

[3] Venkateshwaran K and Anu Malviya and Utkarsha Dikshit and S.Venkatesan. "Security Framework for Agent-Based Cloud Computing". International Journal of Interactive Multimedia and Artificial Intelligence. Volume 3, number 3, 2015.

[4] Cloud Computing Alliance, top threats to Cloud Computing V1.0, March 2010.

[5] U. Akyazi and A.S.E. Uyar. Distributed intrusion detection using mobile agents against ddos attacks. In Computer and Information Sciences, 2008. ISCIS '08. 23rd International Symposium on, pages 1-6, Oct 2008.

[6] O. Demir, B. Khan, G. Ben Brahim, and A. Al-Fuqaha. Optimizing agent placement for flow reconstruction of ddos attacks. In Wireless Communications and Mobile ComputingC onference (IWCMC), 2013 9th International, pages 83-89, July 2013.

[7] M. Zamani, M. Movahedi, M. Ebadzadeh, and H. Pedram. A ddos-awareids model based on dangertheory and mobile agents. In Computational Intelligence and Security, 2009. CIS '09. International Conference on, volume 1, pages 516-520, Dec 2009.

[8] M. Duraipandian and C. Palanisamy. An intelligent agent based defense architecture for ddos attacks. In Electronics and Communication Systems (ICECS), 2014 International Conference, pages 1-7, Feb 2014.

[9] Anders L. Madsen, Frank Jensen, Antonio Salmerón, Helge Langseth, Thomas D. Nielsen, A parallel algorithm for Bayesian network structure learning from large data sets, Knowledge-Based Systems, 0950-7051/ 25 July 2016.

[10] OWASP: the open web application security project, "the ten most critical web application security risks. 2013

[11] A. Patcha and J.-M. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", Computer Networks, vol. 51, pp. 3448-3470, 2007.