ISA-based model for risk detection in Cloud Computing environment

Amal BENFATEH*
Department of Physics;
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

F. GHARNATI
Department of Physics;
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

T. AGOUTI
Computer Science Departement
Telecommunication & computer Network Team;
Samlalia Science faculty;
Cadi Ayyad University
Marrakech, Marocco

Abstruct—Cloud computing is the result of the evolution and the adoption of existing technologies and paradigms. Because of its accessibility via internet, that makes it subject to a large variety of attacks. In present paper, we focus on risk assessment by using an intelligent software agent to develop an immune system of cloud.

Key-Words: -Cloud computing; risk assessment; intelligent software agent; intrusion detection

1 INTRODUCTION:

Today's organizations are a target of information security attacks. More we use e-service, more we are in penetration danger. Attacks could be due to a human or software treat… maybe it is difficult to discover the kind of attacks but we know it would lead to harm our data or our system, or worst, lose a large amount of money; that's why organizations spend millions of dollars on security of technical equipments such as firewalls, intrusion detection systems, encrypting systems, anti-virus tools to protect their systems against threats. Nevertheless, there is always a cleaver intruder that succeeds in sneaking or exploits unknown vulnerability. Therefore, organizations need to manage their information security risks to protect their assets and thus their business values.

Regarding to CSI/FBI survey 2007, 13% of companies which are participated in the survey have no idea that how much they spent for security in last year. The 48% of them suppose that they should invest just 1% of IT budget for security awareness but just 39% are using ROI (Return on Investment) to ensure how much is enough to spend on security. The 46% of companies have obviously found at least one security incident in the past 12 months but only 29% of them have security risk management techniques in progress. What is the most challenge for these companies?

The answer is simple. They don't know about what they have, and what they need. They want to know which asset or technology has a security risk and for which one, they have enough security control to protect. [1]

On the other hand, risk management is usually human activity that includes assessing task and developing security strategy… the important part of the risk management is identifying treats and vulnerabilities by taking into account all past incidents and their impacts on system. To manage this challenge we propose exploit advantages and benefits of software agents to automate this important activity.

2 CLOUD COMPUTING ENVIRONMENT:

2.1 Cloud characteristics :

The National Institute of Standards and Technology's definition of cloud computing identifies five essential characteristics: [2]

- On-demand self-service: give the customer the possibility to provision power of computing as needed without any human interaction.
- Large network access: make the cloud available from any type of network using any client platform.
- Resource pooling: cloud uses a multi-tenant model to serve multiple consumers. The resources have to be pooled to maximize the number of consumers.
- Measured service: cloud systems must monitor resources usage appropriate to the type of service. This can be done by using a metering capability.
- Rapid elasticity: capabilities can be elastically provisioned and released, in some cases automatically,

to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

2.2 Service models:

The costumer has to begin by deciding the appropriate service model to select a cloud solution. The most popular services that cloud offers are (as shown in Figure 1):

- Software as a service (SaaS): the users can rent a set of applications running on the cloud by the provider.
- Platform as a service (PaaS): the users have the service of implementing their applications on the cloud and run it.
- Infrastructure as a service (IaaS): the users can rent a specific infrastructure from the cloud and run any kind of applications even the operating system.

2.3 Deployment model:

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: the cloud system will be used by a single consumer. The system can be maintained in the client's local or by a third party.
- Public Cloud: the cloud is deployed by a Cloud provider for any client who wants to consume.
- Hybrid Cloud: it is the composition of two or more deployment model.
- Community Cloud: the system will be used by a set of clients that share a common interest. The infrastructure can be deployed in the clients' locals like it can be managed by a third party.

1 Security issues in Cloud Computing:

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…
- Virtualization security: misconfigurating virtual hosting platforms, guests and networks, lack VM visibility across the enterprise, failure to consider user-installed VMs.

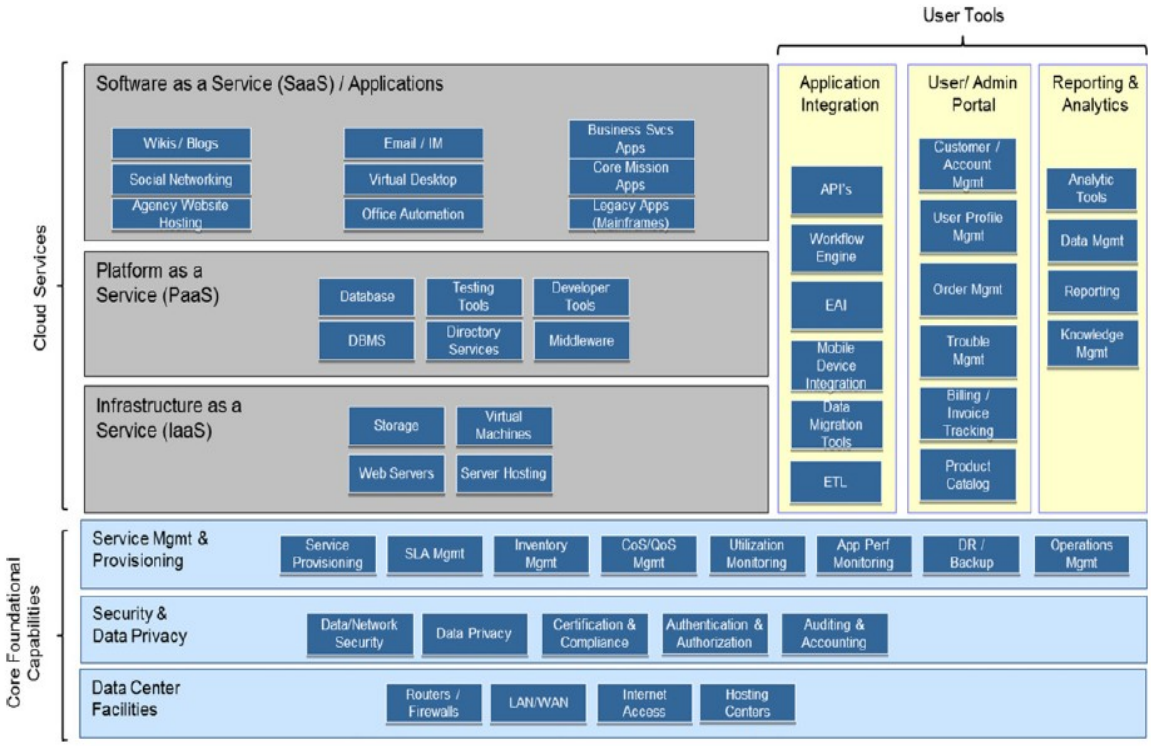

Fig.1: cloud computing services and architecture

3 INTELIGENT SOFTWARE MULTI-AGENT SYSTEM (ISMAS):

We need a system that could help on behalf of experts to assess the risks during normal working processes. The system should be reactive and autonomous because it is needed to respond immediately and independently of events. It should also be communicative and cooperative with logs and reports which are made in relation with other databases and past experiences. The learning ability is very significant for this system because it should learn from past incidents and others which made by itself. The flexibility is also important because the factors and parameters may change during the time or special circumstances.

3.1 Agent*:*

Ferber [3] defines an agent as a physical or virtual entity:

- Able to act in an environment.
- Able to communicate directly with other agents.
- Driven by a set of tendencies (as individual Goals or function of satisfaction, even survival, it seeks to optimize).
- Having its own resources.
- Able to perceive (but to a limited extent) its environment.
- Having only a partial representation of this environment (and possibly none).
- Having qualifications and provides services.
- Able eventually to reproduce.
- Having behavior that tends to meet its objectives, taking into account the resources and its available expertise, and according to its perception.

3.2 Types of agent:

There are two types of agents according to their behavior and to the level of their intelligent. The two ultimate types are cognitive and reactive agents.

- Reactive agent: behavior stimulus/ response no memory of its history, or explicit purpose, no explicit representation of the environment, and with restricted means of communication.
- Cognitive agent: explicit representation of the environment and the other agents; may consider his past and has an explicit goal "social" organization mode (planning , commitment). Interactions between agents are established based on collaborations necessity to resolve the problem.

As for the other types we enclose theme on hybrid agent, they are namely: intentional agent, rational agent, adaptive agent, decisional agent…etc each of them corresponds to a situation and a specific context. [4]

3.3 Multi-agent system:

Multi-agent may be: [4]

- Open: agents enter it and come out freely.
- Closed: set of agents is the same.
- Homogeneous: all agents are build on the same model.
- Heterogeneous: agents of different models of different granularity.

3.4 Software agent system:

In [4], the author defines an agent as a software system located in a certain environment, able to practice independently actions on this environment to achieve its objectives. By this definition an intelligent agent is characterized by the following properties:

- Autonomy: an agent has an internal state (not accessible to others) in terms of which it takes action without human intervention or other agents;
- Reactivity: an agent receives stimuli from its environment and responds according to them;
- Ability to act: an agent is driven by a number of objectives that guide his actions, he does not merely answer demands of its environment;
- Sociability: an agent communicates with other agents or humans and may be engaged in social transactions (negotiate or cooperate to solve a problem) to fulfill its objectives.

Multi-agent system is ideal to represent problems with multiple solving methods, multiple perspectives and / or multiple resolvers [4]. These systems have the traditional benefits of distributed and concurrent resolution of problems such as modularity, rapidity (with parallelism), and reliability (due to redundancy). They also inherit the possible benefits of artificial intelligence such as symbolic treatment (in terms of knowledge), ease of maintenance, reuse and portability but especially, they have the advantage of involving sophisticated patterns of interaction. Current types of interaction include cooperation (working together to solve a common goal); Coordination (organizing the resolution of a problem so that harmful interactions are avoided or that the beneficial interactions are exploited); and negotiation (reach an acceptable agreement of all concerned parties).

4 Risk assessment:

The first step in risk management is asset identification and establishing risk assessment. The potential risk identification could run after this assessment. A risk is the probability of cause of a problem when a threat triggered by vulnerabilities. The source of the problem is vulnerability and the problem itself is threats. Threats are much related to the characteristics of the assets and vulnerabilities are relevant to the security controls. [5][6].

4.1 Risk concepts:

An asset is defined as any element of an information system that possess a value [7]. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, technical factors). In risk process an object is called asset when there is an effect in objects value when risk emerges. A threat is defined as any possible harm to the system, including network failures and natural disasters. Vulnerability is a weak point where the system security is susceptible to attack [8], [9]. Threats need to exploit certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk. This is given in the following figure (figure2). [10]

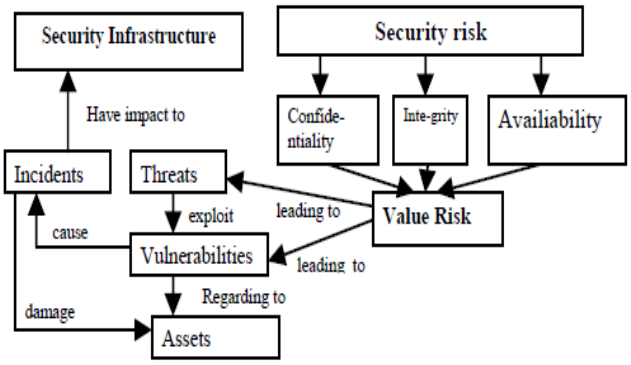

Fig.2: Risk process

4.2 Risk estimation metrics review:

4.2.1 Simplest form: [10]

Risk (R) in the simplest form is the product between event probability P(E) and the possible damage, mostly described as an Impact (I) [11]:

R(E) = Pr(E) * I(E) (1)

Where:

R(E) = risk of an event,

E = Event,

P = Probability

I = Impact.

4.2.2 Estimation of annualized loss expectancy ALE: [10][6]

We need to calculate it:

Asset Valuation (AV): The process that distributes every information financial value.

Exposure Factor (EF): Is expressed within a range from 0 to 100 percent that an asset's value will be destroyed by risk.

Single Loss Expectancy (SLE): Is the calculation of expected monetary loss every time a risk occurs.

The Single Loss Expectancy, Asset Value(AV), and exposure factor(EF) are related by the formula:

SLE = asset value (AV) x exposure factor (EF) (2)

Next we find Annualized Rate of Occurrence (ARO): The probability that a risk will occur in a particular year.

Annualized Loss Expectancy (ALE): is the annually expected monetary loss that can be expected for an asset due to a risk. It is determined by the two input values: the cost of the damage and the probability that the loss will occur. It's calculated as:

ALE = SLE * ARO (3)

4.2.3 Risk assessment by using Bayesian Learning Technique: [6]

According to BSI PD-3002:2002 and Data-Centric Quantitative Computer Security Risk Assessment research

[12] the risk of an information system's asset could be determined by the following formula:

Risk = Impact × Occurrence Rate × (Threat × Vulnerability).

Impact is the weight cost of losing an asset. This cost depends on the asset characteristics and its value for organization. The asset's value for organization could be presented by its classification (C). The occurrence rate (ARO) is the count of a threat which is occurred in one year (Annualized Rate of Occurrence).

By using Bayesian Belief Network (BBN) we could determine the relationship between these factors and their probabilities to risk evaluation. The BBN diagram is presented in figure 3 below.

According to the BBN diagram:

P (Risk) = P (Impact) × P (Occurrence Rate) × P (Probability) (4)

P (R) = (P (Asset Value) × P (Classification)) × P (Occurrence Rate) × (P(Threat) × P(Vulnerability))

P (R) = (P (AC1) × P(AC2) × P(AC3) × P(AC4) × P(AC5) × P(C)) × P (ARO) × (P(T1) × P(T2) × P(T3) × P(T4) × P(V1) × P(V2) × P(V3) × P(V4))

AC1, AC2, AC3 are factors related to asset value such as each asset could have one or more factors of the preceding.

T1, T2, T3 are the common threats in the information system that could be categorized, according to BSI PD.

V1, V2, V3 are the common vulnerabilities from the same guideline.

4.2.4 Mean cost failure: [13]

In [14] the author presents a quantitative infrastructure that estimates the security of a system. The model measures the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. The infrastructure in question reflects the values that stakeholders have in each security requirement, the dependency of security requirements on the operation of architectural components, and the impact that security threats. Given the stakes matrix ST, the dependability matrix DP, the impact matrix IM and the threat vector PT, we can derive the vector of mean failure costs (one entry per stakeholder) by the following formula:

MFC = ST o DP o IM o PT (5)

Where matrix ST is derived collectively by the stakeholders, matrix DP is derived by the systems architect, matrix IM is derived by the security analyst from architectural information, and vector PT is derived by the security analyst from perpetrator models. All matrixes are related by using the matrix product (o). In Figure 4 illustrates these matrices and their attributes (size, content, indexing, etc.).

4.3 Risk management framework for Cloud computing environments: [13]

The qualitative risk analysis proposed method is used to approach risk assessment and rank severity of threats by using classes such as low, medium and high of probabilities and damages for cloud providers. That is, to help providers to control their security position and then to proceed to risk mitigation [15]. The framework has seven processes including: selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step.

5 Related works:

Akyazi and Uyar proposed four different distributed intrusion detection methods to detect distributed denial of service attacks DDoS and tested them by using some tools like JADE (java agent development environment) as a mobile agent plateform, Snort as a network intrusion detector of static agent, MIT DARPA LLDOS dataset. Their experiment resulted that the fourth method was determined as the best one when the importance order of the comparison criteria was taken as reliability, network load then mean detection time.[16]

In different context where the cloud becomes teeming with services which led to find a dynamic and automated cloud services composition, Venkateshwaran and al consider that agents are introduced in the cloud environment to make decision making process easier for consumers like consumer agent CA, broker agent BA, service provider agent SPA and then resource agent RA. According to this model, the authors propose some algorithms to overcome some security issues like injection of malicious agents, denial of service and corrupted agent interaction protocols.[17]

However, Demer and al are keen on placement of agents within the system to improve the effectiveness of this latter and provide better a tradeoff between system parameters and the quality of structural information. For this reason, they 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. [18]

Basing on immunological researches especially danger theory, 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. Hence they proposed an immunology based model where two types of security agents are defined: a group of stationary agents TM, BM, LN, LT) and a group of mobile agents (BC, TC, APC) as well as the third one named framework which provides common functionalities and interfaces of other components and simplifies system deployment.[19]

As for Duraipandian and al, they proposed an architecture based on autonomous agents where there is an authenticator placed between the victim and the server in order to verify the hop-count information used by the hop count filtering mechanism. [20]

6 PROPOSED FRAMEWORK:

The purpose of this work is a capacity of detecting at best errors and risks, named here a gap, in the system in real time. Hence it could overcome as fast as possible the most risks or errors taken place in the system.

For this aim, a proposed framework consists of the following components: Detector, Provider agent (PA), Hypervisor detector agent (H-DA), operating-system

detector agent (OS-DA), Master agent (MA), Corrector agent (CA), Evaluator agent (EA), and Log editor agent (LEA).

A detector agent or merely a detector: it is an agent which is responsible on looking for any gap on performing tasks. It consists of H-DA and VM-DA. These latter have as function catching as fast as possible any abnormal conduct. After detecting a gap, it dispatches an alarm signal to the master agent to seek the true meaning of the alarm and waits for its acknowledgment.

OS-DA: a stationary agent of type detector endowed in every subscriber's operating system in the cloud. It's the nearest agent from the subscriber and from his activities. Therefore it verifies that the subscriber's system correctly performed its tasks and in the other part, it is to him to edit the security requirements recommended by the user in the requirement subscriber's entity (RSE). Cloud computing servers can contain many VMs and so OSs, hence they are vulnerable to attack. Active OSs are vulnerable to all of the security attacks that a conventional physical service is subject to. However, once an OS has been compromised by an attack residing on the same physical machine, they become all vulnerable to the same attack due to the fact that each machine shares memory, disk storage, driver software and hypervisor software.

H-DA: a stationary 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. The system administrator or other authorized user can make changes to the components of one or more virtual machines (VMs), generating a security risk, it is for him to monitor this component.

MA: (master agent) it is the lever of agents system. It is a cognitive agent that tries to learn from every past event. After receiving an alarm signal, it sends back an acknowledgment to the detector to say that is 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 CA for help about available resources to remedy this gap. For Each action, it point out it in the LEA as a report. On the other hand, it is in charge of the risk assessment all the time due to his sensitive and strategic position in the system thus it is endowed by one of a security assessment approach mentioned previously.

PA: it is a stationary agent that accompanies the provider to propose manual or occasional corrections or notify him about missed resources or required by CA.

CA: it is an agent responsible on security resources library in case if MA may need to use them. Else it is itself who choose the best security solution to overcome the risk. But if it doesn't find the suitable tool, it send to the provider agent for a missing resources.

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

LEA: it a stationary agent which receives reports from the MA and updates its report system.

7 ILLUSTRATION:

The proposed model is presented in figure 3.

In the figure, we used the PowerDesigner to simplify the presentation of agents. For this aim, we have represented agents by circles, transaction or communication flow with arrows and different kind of entities are represented by the squares it is the case of CSR and DB-threat database that exists outside of the system.

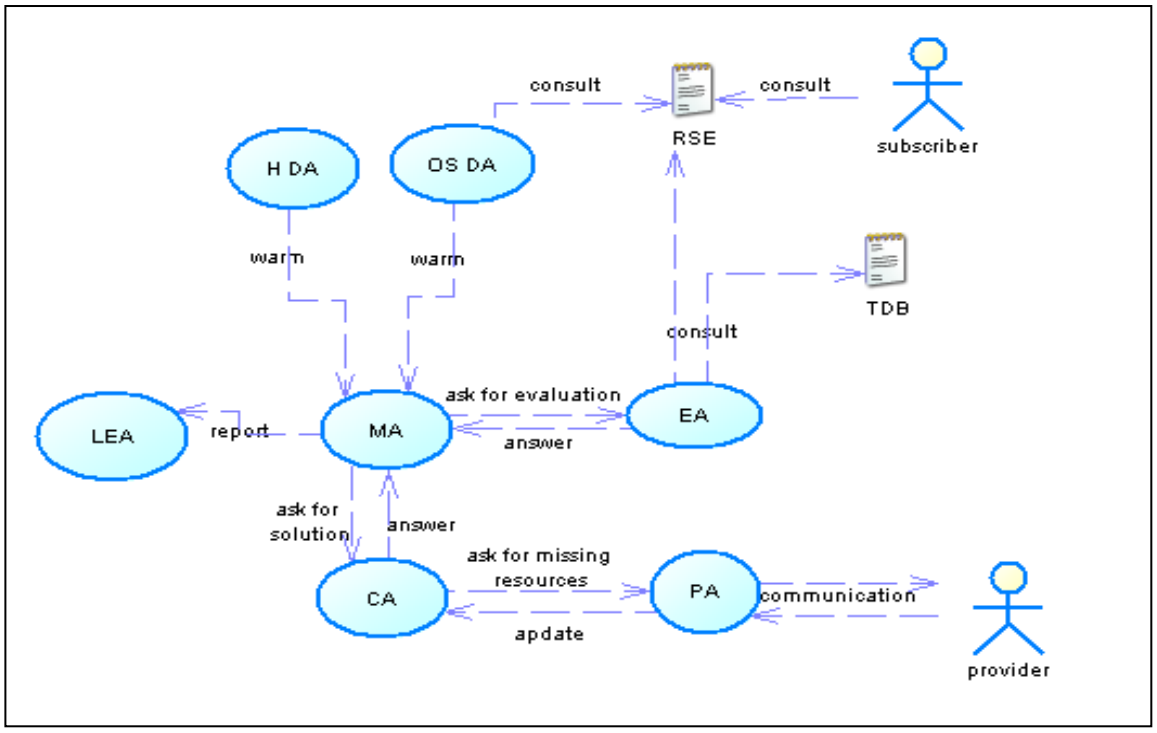

Fig.3: Software agent based model in cloud computing environment.

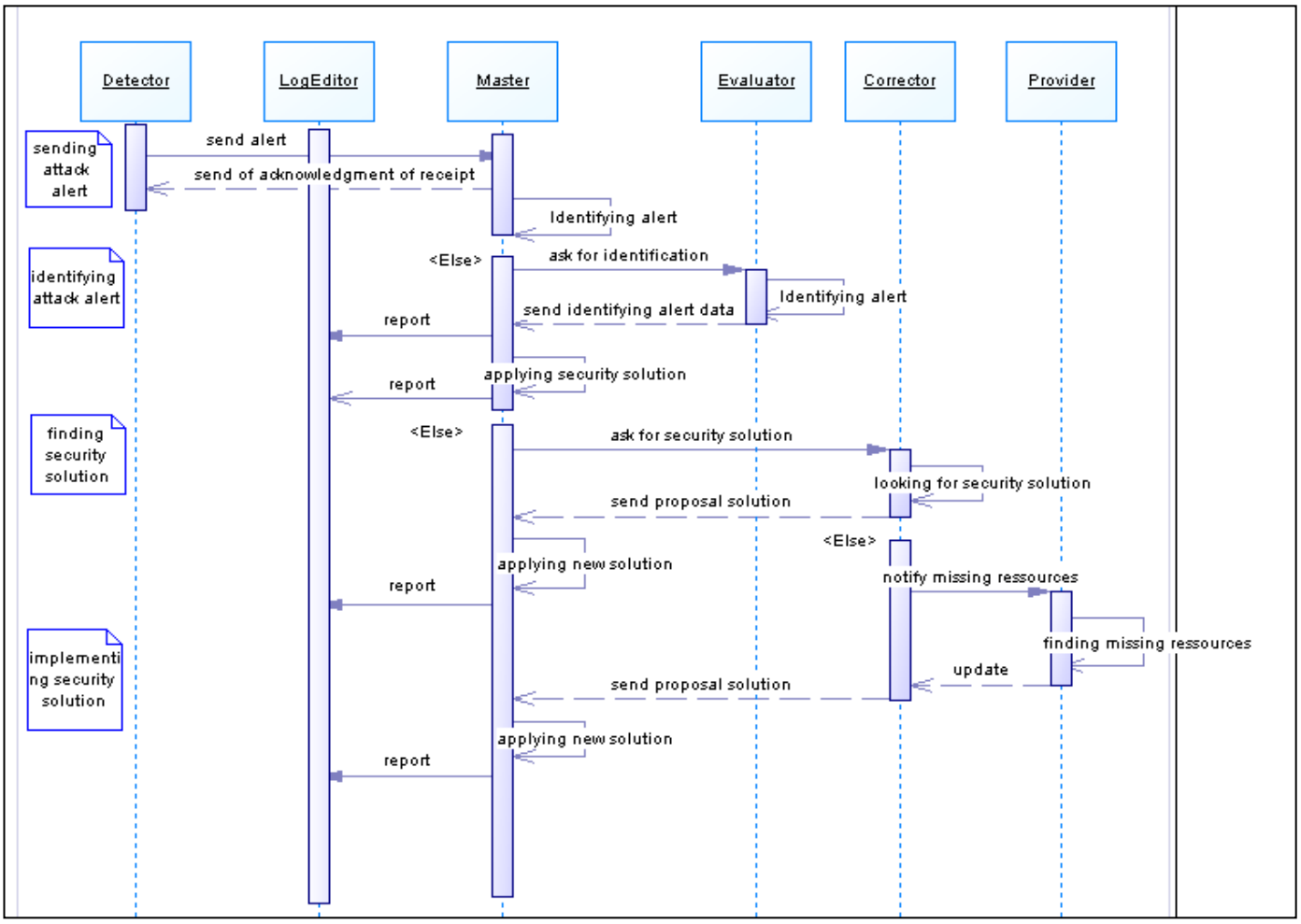

Fig.4: interactions diagram of a proposed framework for detection and response case

8 DISCUSSION:

Risk assessment is the most complicated task in the CC environment. According to Canavan work [21], security is a trinity consisting of three elements: Prevention, Detection and Response. In the prevention phase, the system is in the calm state if we see it from the outside; however, detection agents and the master agent perform all the time a risk computing based on one of the security assessment approach to be vigilant and wary to happen any surprised harm.

As For the detection and response phase, all defense mechanisms (agents) intervene to face up to the intrusion as shown in the figure 4.

This model allows us to automate the response and monitor, in real time, the cloud system taking into account the recommended user requirements of security user (RSE) and being up to date on all emerged news of threats or discovered vulnerabilities by being connected with external databases (the role of the EA). We do not forget the role of the agent (CA) to approach solutions to the system and ensure the upgrading when needed. Then, the reactivity, autonomy, flexibility, cooperation and communicability between entities, intelligent learning ability, all these assets give us a powerful system and a robust immunity to the new appeared threats. Therefore, this model has several advantages, for this reason it can be considered as an effective solution for the management risk.

9 CONCLUSION

There is a tremendous need for secure cloud environment for reassure and amply satisfy customer expectations. Among the security issues that breaks the back, is the management of risk in real time. Then, in this paper an intelligent model was proposed, based on the collaboration of different agents as MA, PA, EA, CA, HAD, OSDA, and LEA, to meet this challenge by providing robust immune system troubles ahead.

REFERRENCES:

[1] CSI/FBI (2007, 12, 03). *The 12th Annual Computer Crime and Security Survey.*

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

[3] M. Cherghi H. Medroumi and A. Souti, " Inter – organizational workflow for Intelligent Audit of Information Technologiesin terms of Entreprise Business Processes" *International Journal of Advanced Computer Science and Aplication,* 5(5), 2014

[4] R. Latif, H. Abbas, S. Assar, Q. Ali, Cloud computing risk assessment: a systematic literature review, in: *Future Information Technology*, Springer,Berlin, Heidelberg, 2014, pp. 285–295.

[5] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti & S.K. Sadhukhan. (2006, 01, 07). e-Risk Management with Insurance : A framework using Copula aided Bayesian Belief Networks, Proceedings of the 39th Hawaii *International Conference on System Sciences.*

[6] F. Foroughi, « Information Security Risk Assessment by Using Bayesian Learning Technique", *Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008*, July 2 - 4, 2008, London, U.K.

[7] E. Loukis, D. Spinellis, "Information Systems Security in the Greek Public Sector*". Information Management and Computer Security* 9(1), pp. 21–31, 2001.

[8] M. Myerson, "Risk Management Processes for Software Engineering Models". *Boston: Artech House,* 1997.

[9] D. Spinellis, S. Kokolakis, S. Gritzalis, "Security requirements, risks and recommendations for small enterprise and home office environments". *Information Management & Computer Security* 7(3), pp. 121-128, 1999.

[10] T. Tsiakis, "Information Security Expenditures: a Techno-Economic Analysis", *IJCSNS International Journal of Computer Science and Network Security*, VOL.10 No.4, April 2010

[11] W. Böhmer, "Evaluation of the Quality of an Information Security Management System (ISMS) or how secure is secure?". *Guest lecture at the Gjovik University College,* 2006.

[12] B. Berger. (2003, 08, 20). *Data-Centric Quantitative Computer Security Risk Assessment,* [Online]. Available: http://www.sans.org/reading_room/whitepapers/auditin g/1209.php.

[13] L.B.A. Rabai , M. Jouini, A. Ben Aissa, A. Mili, « A cybersecurity model in cloud computing environments", *Journal of King Saud University – Computer and Information Sciences* (2013) 25, 63–75

[14] A. Ben Aissa, R.K. Abercrombie, F.T. Sheldon, A. Mili, "Quantifying security threats and their potential impacts: a case study". *Innovation in Systems and Software Engineering: A NASA Journal* 6, 269–281.2010

[15] X. Zhang, N. Wuwong, H. Li, "Information security risk management framework for the cloud computing environments". In: *10th International Conference on Computer and Information Technology (CIT),* pp. 1328–1334. 2010

[16] 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.

[17] 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

[18] 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.

[19] 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.

[20] 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

[21] J. Canavan, "*The Fundamentals of Network Security*". Boston: Artech House, 2001.