International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:6, 2014

Toward a Risk Assessment Model Based On Multi-Agent System for Cloud Consumer

Saadia Drissi, Siham Benhadou, Hicham Medromi

***Abstract*—**The cloud computing is an innovative paradigm that introduces several changes in technology that have resulted a new ways for cloud providers to deliver their services to cloud consumers mainly in term of security risk assessment, thus, adapting a current risk assessment tools to cloud computing is a very difficult task due to its several characteristics that challenge the effectiveness of risk assessment approaches. As consequence, there is a need of risk assessment model adapted to cloud computing. This paper requires a new risk assessment model based on multi-agent system and AHP model as fundamental steps towards the development of flexible risk assessment approach regarding cloud consumers**.**

***Keywords*—**Cloud computing, risk assessment model, multi-agent system, AHP model, cloud consumer.

I. Introduction

THERE are several changes that are likely emerged, among them is the sharing of resources by multi-consumers, the question of multi-tenancy that means the data may be located at several geographically distributed nodes in the cloud and the control over where the processes actually run and where the data reside. Consequently, these characteristics of cloud computing introduce a new issues that challenge the effectiveness of risk assessment approaches.

In spite of the advancement in cloud technologies, cloud computing being a novel technology introduces new security risks that need to be assessed and mitigated [1]. Therefore, assessment of security risks is essential [2], the traditional technical method of risk assessment should give way to the specific characteristics of cloud computing.

The current risk assessment methods (EBIOS, OCTAVE, and MEHARI [3]-[5], have not been designed specifically for cloud computing environments. In traditional IT environments, everyone in the business has to go to the IT department to obtain IT related services. However, for cloud computing, the risk assessment becomes more complex; cloud computing environment is multi-location environment in which each location can use different security and potentially employ various mechanisms.

Facing this complexity, this paper proposes a new risk assessment model which considering all relevant aspects of information security risk assessment, this new model is based on AHP model and multi-agent system, to ensure the effectiveness, the flexibility, fast model to use (real time) and the automation. The following section describes the main concept of risk assessment, cloud computing and multi-agent system (SMA). In Section III, we analyze and discuss the risk assessment in cloud computing environment in literature. In Section IV, we present our proposed risk assessment model as fundamental step toward the development of risk assessment model dedicated to cloud consumer. Finally, some concluding remarks are given at the end.

S.Drissi, S. Benhadou, and H. Medromi are with the National High School of Electricity and Mechanic, Hassan 2 University, Casablanca, CO 8118 Morocco (e-mail: saadia.drissi@gmail.com, benhadou.siham@gmail.com, hmedromi@yahoo.fr).

II. Fundamental Concept

The first part of this second section defines de main concept of cloud computing, the second part introduces the different process of risk assessment and third part presents the multi-agent system.

A. Cloud Computing

In literature, there are many different definitions for cloud. The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous [6], convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. European Community for Software and Software Services (ECSS) explains it as the delivery of computational resources from a location other than your current one [7].

Cloud can be categorized into three delivery models classified according to their uses; Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). Cloud Software as a Service (SaaS) which deliver software over the Internet (e.g. Salesforce CRM, Google Docs, etc), Cloud Platform as a Service which mainly offer virtualized execution environments to host Cloud services (e.g. Microsoft Azure, Force and Google App engine) and Cloud Infrastructure as a Service which provide virtualized computing resources as a service (e.g. Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydive and Rackspace Cloud).

Four deployment models have been identified for cloud architecture solutions: Private cloud: a cloud platform is operated for specific organization, Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns, Public cloud: a cloud platform available to public users to register and uses the available infrastructure. Hybrid cloud: a private cloud that can composite two or more clouds (private, community or public) [8].

B. Risk Assessment

Risk in itself is not bad, risk is essential to progress, and failure is often a key part of learning. But we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity [9].

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives. According to the introduction to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk [7]. Risk assessment is one step in the process of risk management.

Risk assessment is the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. The main objective of risk assessment is to define appropriate controls for reducing or eliminating those risks.

Generally there are four steps of risk assessment. The four steps are as follow [10]:

Threat Identification: This first step identifies all potential threats to the system. It allows identifying the potential threat sources and develops a list of a threat statement that is potential threat sources that are applicable to the system.

Vulnerability Identification: In the second step, the goal of vulnerability identification is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

Risk Determination: In the third step, the purpose of risk determination is to assess the level of risk to the system.

Control Recommendation: In the fourth step, the goal is to purpose some controls that could mitigate or eliminate the identified risks, as appropriate to the system organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the system.

C. Multi-Agent System

An agent is an autonomous real or abstract entity that is capable of acting on itself and its environment, which, in a multi-agent world, can communicate with other agents, and whose behavior is the result of observations, knowledge and interactions with other agents [11].

In this case, not only one agent is used but a set of agents witch interact among each other that are called Multi-agent system.

A multi-agent system is characterized by:

a. Every agent in the system has his own knowledge and way to resolve problems.
b. There is no global control of an multi-agent system,
c. The Data in multi-agent system is decentralized.

III. Related Work

Several risk assessment approaches exist. However, none of them takes into account the characteristic and the complex nature of cloud computing (e.g., sharing resources).

In recent years, the principles and practices of risk assessment were introduced into the world of utility computing such as Grid and Clouds either as a general methodology or a focus on a specific type of risk, such as SLA fulfillment. In [12], a quantitative risk and impact assessment framework based on NIST- FIPS-199 (QUIRC) is presented to assess the security risks associated six key categories of security objectives (SO) (i.e., confidentiality, integrity [13], availability, multi-trust, mutual audit ability and usability) in a Cloud computing. However, the challenge and difficulty of applying this approach is the meticulous collection of historical data for threat events probability calculation, which requires data input from those to be assessed Cloud computing platforms and their vendors. Similar efforts were carried out in [14]. In [15], a risk analysis approach from the perspective of a cloud user is presented to analyze the data security risks before putting his confidential data into a cloud computing environment. The main objectives of this work are to help service providers to ensure their customers about the data security and the approach can also be used by cloud service users to perform risk analysis before putting their critical data in a security sensitive cloud. However, there is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. In [2], a cloud-based risk assessment as a service is proposed as a promising alternative. Cloud computing introduces several characteristics that challenge the effectiveness of current assessment approaches. In particular, the on-demand, automated, multi-tenant nature of cloud computing is at odds with the static, human process-oriented nature of the systems for which typical assessments were designed. However, the autonomic risk assessment is far away from the light, because the risk assessment is hard task to do.

After survey the literature of risk assessment regarding cloud computing, most of the current works is for helping cloud consumers assessing their risk before putting their critical data in a security sensitive cloud. Therefore, the most obvious finding to emerge from this study is that, there is a need of specific risk assessment approach. At present, there is a lack of structured method that can be used for risk assessment regarding cloud consumers to assess their resources putting outside [16].

IV. Research Methodology

In the first part of this section, we explain why the current risk assessment tools are hard for cloud consumer. In the second part, we present the different steps of our proposed risk assessment model. In the third part of this section, we present the proposed architecture of asset assessment and explain the other process of risk assessment for cloud consumer.

A. Formalization of Risk Assessment

A formalized risk assessment mentioned in can be used for the conventional system [17]. However, in a cloud computing environment, when the resources are moved to cloud computing environment, an asset can have many locations and the security objectives can change depending on asset location in term of confidentiality, integrity and availability, because Cloud computing environment are multi-location environment

in which each location can have different security objectives. Therefore, each asset location can have its own asset value and not each asset can have its asset value like in conventional system. Thus, the methodology used to identify the asset value for conventional system is not valid for asset value in cloud computing environment or it will be difficult to carry out.

In conventional system, the organization can define the vulnerability level as mentioned in [17]. However, moving any organization to the cloud needs thinking critically about using multiple sources of identity with different attributes and different security. Additionally, each provider has their own established security system, thus, each one of them has their own vulnerability level. Therefore, each asset location can be exploited by different vulnerabilities depending on its locations.

After formalize risk assessment for conventional system, the shows that the risk assessment in cloud computing environment is harder than a conventional system. Consequently, there is a need of risk assessment model for cloud consumers [17].

Cloud computing environment are multi-location environment in which each location can use different security, privacy and trust requirement and potentially employ various mechanism. This is the reason why we use the archived asset assessment (before moving to cloud) and then define the weight of each asset per location in order to facilitate the risk assessment for cloud consumer.

B. Asset Assessment Model

When the resources are moved, we should critically think about using multiples sources of identity with different attributes (confidentiality, integrity and availability). As mentioned in [17], one asset can be located in different locations, thus, each asset can have its asset value. Facing this complexity, we will use an archived asset assessment for client to make easy the asset assessment in cloud computing environment.

To assess the risk for cloud consumers, below is the detailed procedure:

Step1. The risk assessor will define the priority of cloud providers (L1, L2, L3), where is located the cloud consumer's resources, the importance of asset and also the security objectives (Fig. 1).

Step2. Apply AHP model to define the weight of security objectives of each asset location, and then we can define the weight of each asset location basing on AHP model.

To define the weight of asset location, we require using AHP model. It also enables qualitative and quantitative analysis into the same decision making methodology by giving a basis for eliciting, discussing, recording, and evaluating the elements of a decision. It uses hierarchal way with goals, criteria, sub-criteria and alternatives. According to many researchers, AHP is an effective and flexible tool for structuring and solving complex group decision situations [18]-[20].

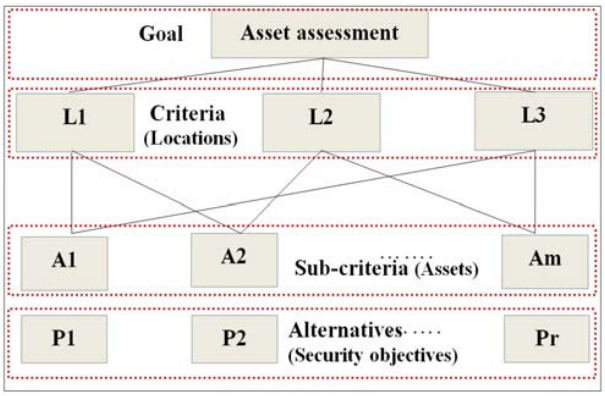

Fig. 1 Decision tree for asset assessment

Step3. After determine the weight of each asset location basing on the AHP model; we can define the asset value using the weighting process as mentioned below.

$$ai = \sum_{r=1}^{s} sir * wir / \sum_{r=1}^{s} wir \quad (1)$$

TABLE I
ASSET ASSESSMENT EXAMPLE

Asset	Security Necessity			Location	Weight of Security objectives			Asset value
				L1	*w11*	*w12*	*w13*	*a11*
A1	*s11*	*s12*	*s13*	L2	*w21*	*w22*	*w23*	*a12*
				L3	*w31*	*w33*	*w33*	*a13*

with C is the confidentiality, I is the integrity and A is the availability.

This methodology will help us to define the weights of each asset location, in order to define the asset value for each asset location.

C. Asset Assessment Architecture Based On Multi-Agent System

The proposed architecture dedicated to cloud consumer shows up two important paradigms:

a. AHP: Risk assessment is purely based on decision making. This is the reason why we show up AHP in our work. Thus, this paradigm can ensure the effectiveness, the flexibility and the automation to our risk assessment model.
b. SMA: One factor in the selection of risk assessment method is that it should be fast to use. The time taken to conduct a risk assessment requires resources which cost money. Furthermore, the risk assessment results may be required quickly. This is the reason why we show up the system multi-agent in our work.

In (Fig. 2), there are different kinds of agents in the architecture, each one with specific roles, capabilities and characteristic:

Communication agent CA1: This agent is assigned to establish the link between the risk manager and the knowledge base (DB1) and invokes the intelligent agent (IA1).

Communication agent CA2: This agent is a mediator, responsible to communicate the weight of each asset to intelligent agent (IA2)

Communication agent CA3: this agent is assigned to communicate the archived security objective of each asset from knowledge base (DB2).

Intelligent agent IA1: This agent is responsible to gear Analytic Hierarchy Process (AHP) by applying the multi-criteria decision making approach in which the factors are set in hierarchic composition.

Intelligent agent IA2: The objective of this agent is to carry out the weighting process using the equation mentioned above (1).

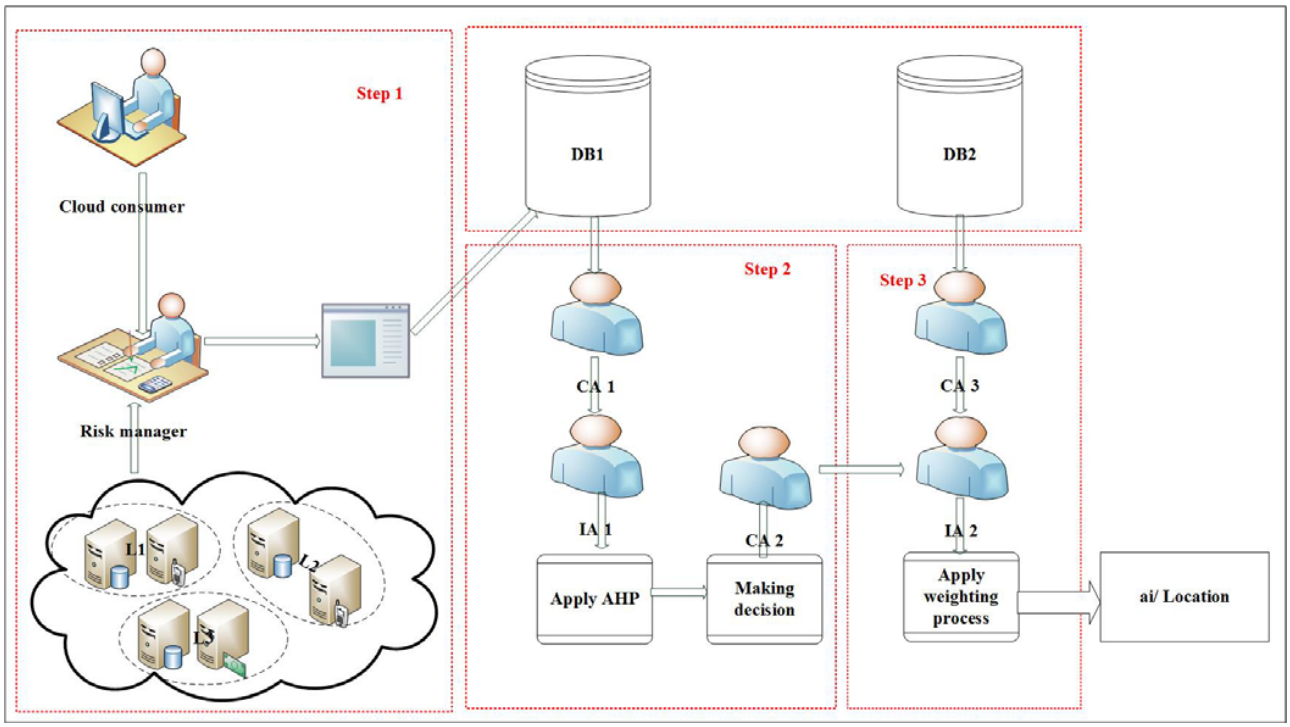

Fig. 2 Asset assessment model based on multi-agent system

Step4. Outsourcing services to cloud mean been exposed to new vulnerabilities, thus, resulting in a modified identification of vulnerabilities and also means that the methodology used for conventional systems will be hard to use for cloud consumers. Facing this complexity, we require defining the vulnerability per location in order to check which location is more critical. The flowing form depends on Asset location and vulnerability (Table II):

$$V = (vl,k) \quad (2)$$

TABLE II
VULNERABILITY IDENTIFICATION EXAMPLE

Vulnerabilities/cloud providers	Corresponding Assets CP1	Vulnerability value CP1	Corresponding Assets CP2	Vulnerability value CP2
V1	*A1, A2, A3*	*v11*	*A1, A2, A5*	*v21*
V2	*A2,A4,A5*	*v12*	*A2,A4,A6*	*v22*
V3	*A2, A3, A6*	*v13*	*A2, A3, A4*	*v23*
……	……..	……	……..	……..
Vh	*A3, A5, A6*	*v1h*	*A3, A5, A7*	*v2h*

Step5. The main reason that threats are important elements of the information security risk assessment is that they help to determine the scope of the vulnerabilities of the system being assessed. Thus, to assign threats for cloud consumer, we should define these threats by location in order to define which location or provider is critical (Table III).

$$T = (tl,j) \quad (3)$$

TABLE III
THREAT IDENTIFICATION EXAMPLE

Threat/ Cloud provider	Corresponding Assets CP1	threat value CP1	Owned Asset CP2	threat value CP2
T1	*A1, A2, A3*	*t11*	*A1, A2, A5*	*t21*
T2	*A2,A4,A5*	*t12*	*A2,A4,A6*	*t22*
T3	*A2, A3, A6*	*t13*	*A2, A3, A4*	*t23*
……..	……..	….	……..	……
Tn	*A3, A5, A6*	*t1n*	*A3, A5, A7*	*t2n*

With such an approach, the cloud consumers can check the effectiveness of the current security controls that protect an organization's assets and the service providers can maximize

and win the trust of their cloud consumers .Also the cloud consumers can perform the risk assessment to be aware of the risks and vulnerabilities present in the current cloud computing and check which asset location is more critical.

V. Conclusion

Cloud computing is a new way for delivering computing resources which introduce several benefits to its user. Despite its positive characteristics, cloud computing introduces several changes that have resulted a new ways for cloud providers to deliver their services to cloud consumers, thus, resulting a modified assessment for risk regarding cloud consumers. This paper proposes a new risk assessment model as fundamental steps towards the development of flexible risk assessment model regarding cloud consumers to provide a more reliable security in cloud computing. In the next work, a case study will be performed in detail to demonstrate the effectiveness of this new model for cloud consumers. With such an approach, the customers can be guaranteed data security and the service providers can win the trust of their customers.

References

[1] Cloud Security Alliance (CSA): Top threats to cloud computing, version 1.0. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.
[2] Burton S. Kaliski Jr. and Wayne Pauley,Toward Risk Assessment as a Service in Cloud Environment, *EMC Corporation, Hopkinton, MA*, USA, 2010.
[3] EBIOS, Central Directorate for Information Systems Security, Version 2010 website. [Online]. Available: http://www.ssi.gouv.fr.
[4] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute, (1999).
[5] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.
[6] Mell P, Grance T. Perspectives on cloud computing and standards. National Institute of Standards and Technology (NIST). Information Technology Laboratory; 2009.
[7] CSS, White paper on software and service architectures, Infrastructures and Engineering – Action Paper on the area for the future EU competitiveness Volume 2: Background information, Version 1.3, retrieved:15.08.2010,http://www.euecss.eu/contents/documentation/volume%20two_ECSS%20White%20Paper.pdf
[8] Miller, M. (2008). Cloud computing: Web-based applications that change the way you work and collaborate online. Indianapolis,
[9] Van Scoy, Roger L. Software Development Risk: Opportunity, Not Problem
[10] R. Farrell, “Securing the cloud-governance, risk and compliance issues reign supreme,” Information Security Journal: A Global Perspective, 2010.
[11] A. Sayouti, H. Medromi–“Les Systèmes Multi-Agents : Application au Contrôle sur Internet” Auteurs Éditions universitaires européennes, Août 2012.
[12] P. Saripalli and B. Walters, QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security , In the Proceedings of the IEEE 3rd International Conference on Cloud Computing, 2010, pp. 280-288.
[13] Peiyu L., Dong L.. “The New Risk Assessment Model for Information System in Cloud Computing Environment”, Procedia Engineering 15, 2011, pp. 3200 – 3204 .
[14] Z. Xuan, N. Wuwong , et al., “Information Security Risk Management Framework for the Cloud Computing Environments,” in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), 2010.
[15] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, “Towards Analyzing Data Security Risks in Cloud Computing Environments”, International Conference on Information Systems, Technology, and Management (ICISTM), Bangkok, Thailand, 2010.
[16] Drissi S., Houmani H., Medromi H., Survey: risk assessment for cloud computing, International Journal of Advanced Computer Science and Applications,2013, pp.143-148.
[17] S. Drissi and H. Medromi, “A new risk assessment approach for cloud consumer”, Journal of Communication and Computer (JCC), March 2014 (accepted).
[18] A. Altuzarra, J. M. Moreno-Jimnez and M. Salvador, A Bayesian prioritization procedure for AHP-group decision making, *European Journal of Operational Research*, vol.182, no.1 , 2007, pp.367-382.
[19] R. Ramanathan and L. S. Ganesh, Group preference aggregation methods employed in AHP: An evaluation and an intrinsic process for deriving members' weightages, *European Journal of Operational Research*, vol.79, no.2 , 1994, pp.249-265.
[20] R. F. Dyer and E. H. Forman, Group decision support with the analytic hierarchy process, *Decision Support Systems*, vol.8, no.2, pp.99-124, 1992.