GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DESIGN OF RISK ASSESSMENT MODEL FOR CLOUD COMPUTING

Saadia Drissi[*1], Siham Benhadou[2] and Hicham Medromi[3]
[*1, 2, 3] ENSEM, Casablanca

ABSTRACT

Cloud computing has recently emerged a new paradigm by introducing potential benefits in achieving rapid and scalable resource provisioning capabilities to Cloud consumers. Despite the fact that cloud computing offers many cost benefits for their cloud consumers, number of security risk are emerging in association with cloud usage that need to be assessed. This paper presents an intelligent, distributed and collaborative risk assessment model for cloud computing that will add a great help and assistance to both cloud consumers and cloud providers.

Keywords- *Cloud computing, an intelligent and distributed risk assessment model, cloud consumer.*

I. INTRODUCTION

Cloud computing has recently emerged a new paradigm by introducing potential benefits in achieving rapid and scalable resource provisioning capabilities to Cloud consumers. However, these benefits introduce 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 [1]. Therefore, assessment of security risks is essential [2].

The current risk assessment methods (EBIOS, OCTAVE, and MEHARI [3], [4], 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. The following sections analyze and discuss the risk assessment in cloud computing environment in literature and present the proposed risk assessment model. Finally, some concluding remarks are given at the end.

A) Related work

Several risk assessment approaches exist. However, none of them takes into account the characteristic and the complex nature of cloud computing.

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 [5], 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 [6], 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 [7]. In [8], 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, multitenant 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 [9].

B) Research methodology

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]:

Identification and study of the context (process 1): This study aims to define the scope of the approach by analyzing the environment of the target chosen for the process of risk management. The study is important in the context of risk management, as it allows obtaining information about all that revolves around the target and may possibly influence.

Threat Identification (process 2): 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 (process 3): 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 (process 4): In the third step, the purpose of risk determination is to assess the level of risk to the system.

In (Fig. 1), there are different kinds of agents in the architecture in each risk assessment process, each one with specific roles, capabilities and characteristic:

Agent mediator (communication agent): This agent is assigned to establish the link between the security objectives of each consumer and the agent AHP.

Agent AHP: 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 [11].

Agent organizer: this agent establishes the link between the agent AHP and the calculator agent.

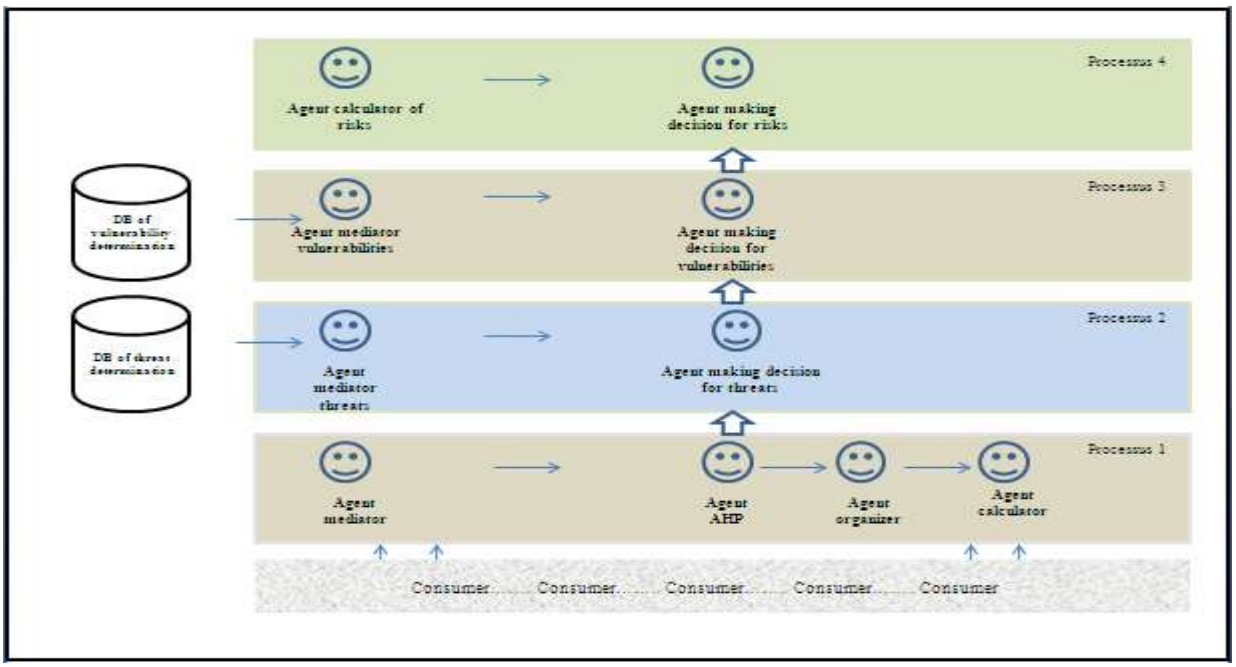

Fig 1: Architecture of risk assessment model based on SMA

Agent calculator: this agent is assigned to calculate the asset value of each consumer.

Agent mediator threats: This agent is assigned to establish the link between the knowledge base of threats and the agent Making Decision for threats.

Agent making decision for threats: this agent is responsible to define the potential of threats.

Agent mediator vulnerabilities: This agent is assigned to establish the link between the knowledge base of vulnerabilities and the agent Making Decision for vulnerabilities.

Agent making decision for vulnerabilities: this agent is responsible to define the severity of vulnerability.

Agent calculator of risk: this agent is assigned to calculate the risk.

Agent making decision for risks: the objective this agent is to define whether the risk is acceptable or not.
With such a collaborative 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.

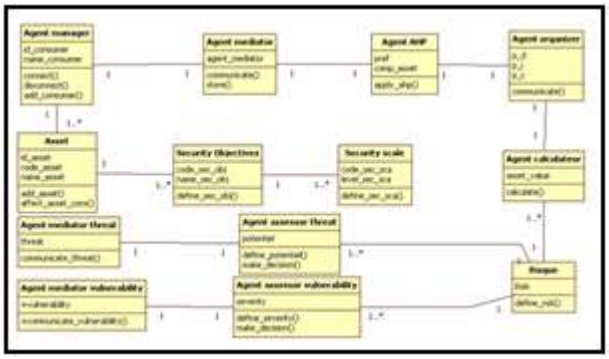

Fig 2: Class diagram of the proposed risk assessment model

The (Fig 2) shows the class diagram of the proposed risk assessment model for cloud computing.

II. CONCLUSION

In this paper, we have presented a new distributed, collaborative and intelligent risk assessment model for cloud computing that will add a great assistance and help to both cloud consumers and cloud providers. Therefore, with such an approach, the consumers can be guaranteed data security and the service providers can win the trust of their consumers.

REFERENCES

1. *Cloud Security Alliance (CSA): Top threats to cloud computing, version 1.0. http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf,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. *[3] EBIOS, Central Directorate for Information Systems Security, website. [Online]. Available: http://www.ssi.gouv.fr ,Version 2010.*
4. *[4] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.*
5. *[5] Prasad Saripalli and Ben 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.*
6. *[6] Liu Peiyu and Liu Dong . The New Risk Assessment Model for Information System in Cloud Computing Environment, Procedia Engineering, 2011.*
7. *Xuan and Wuwong . Information Security Risk Management Framework for the Cloud Computing Environments, in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), 2010.*
8. *Amit Sangroya, Saurabh Kumar, Jaideep Dhok and Vasudeva Varma. Towards Analyzing Data Security Risks in Cloud Computing Environments, International Conference on Information Systems, Technology, and Management (ICISTM), 2010.*
9. *Saadia Drissi , Hanane Houmani, Hicham Medromi. Survey: risk assessment for cloud computing, International Journal of Advanced Computer Science and Applications,2013*

10. *R. Farrell, Securing the cloud-governance, risk and compliance issues reign supreme," Information Security Journal: A Global Perspective, 2010.*
11. *Saadia Drissi, Siham Benhadou and Medromi H., Toward a risk assessment model based on multi-agent system for cloud computing, International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:6, 2014*