AN AUTONOMOUS RISK ASSESSMENT MODEL FOR CLOUD COMPUTING BASED ON MULTI-AGENT SYSTEM BEFORE AND AFTER THE CLOUD ADOPTION

S. Drissi, S. Benhadou, H. Medromi
National High School of Electricity and Mechanics, ENSEM,
University Hassan II, 8118, Casablanca, Morocco

ABSTRACT
Cloud computing is one of the most important technologies in modern IT world development. However, most of the research’s studies view the problem of security risks assessment for all cloud actors. Thus, the adoption of cloud solutions in a number of companies is stopped. To make a decision to adopt and to migrate to cloud services, there is a great need of new risk assessment model or method before and after the adoption of cloud services. Current risk assessment models and methods generally cannot be applied to cloud services because this paradigm changes its characteristics very rapidly. In this paper, a new, intelligent, shared, comprehensive, collaborative and transparent risk assessment model has been proposed for cloud computing as solution of this problem in which the cloud actor is an active entity. An experimental result will be showed at the end to demonstrate the effectiveness of this new risk assessment model.

Key word: Cloud Computing, security risk, and a new intelligent, shared, comprehensive, collaborative and transparent risk assessment model.

http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=8&IType=4

1. INTRODUCTION
The cloud presents several major advantages for its users. The cloud users can access their applications and cloud services wherever they are. However, they have many challenges posed by cloud computing regarding information security area that are: cloud computing governance, risk management, service level agreement and trust management, data privacy of the cloud users, virtualization management and identity management.
Since more than one cloud actors uses the cloud computer resources, its security becomes more important than normal IT resources that are used by one entity. In the other hand, each service model requires different computing resources; security measures which are used for each of these service models may be varied. Therefore, the risk assessment becomes more complex: cloud computing environment is multi-domain environment in which each domain can use different security and potentially employ various mechanisms.

The current risk assessment methods (EBIOS, OCTAVE, and MEHARI [16], [17], [18], have not been designed specifically for cloud computing environments. In current IT environments, everyone in the business has to flow the IT department to obtain IT related services.

In order to effectively carry out cloud computing security risk assessment, there is a need of a model of overall cloud computing security risk assessment, and move forward a specific risk assessment methodology [23]. Therefore, a new, collaborative, intelligent, shared and transparent risk assessment built to define all probable risks before and after the adoption for cloud computing.

ACRAM is an autonomous cloud risk assessment model based on intelligent experts’ agents. Major modules of ACRAM are (a) identification of assets [22], (b) determination of vulnerabilities, (c) determination of threats, (d) identification of risks and (e) identification of measures. ACRAM modules and their details will be explained in the third section.

Major objectives of design of ACRAM are:

- Have a collaborative model in which each cloud actor can be an active entity in risk assessment.
- Have a transparent model in which all the cloud computing operations are visible for cloud actors.
- Have a comprehensive model; very easy cloud computing tool for both cloud actors and cloud risk manager with the help of intelligent expert agents.
- Have an autonomous model based on multi-agent system.
- Have a shared model in which the risk assessment is shared between the cloud actor and the cloud risk manager in cloud computing environment.
- Solve all problems regarding the multi-domain.
- Assess the risks before the migration to cloud and after its adoption.
- Take into account all factors of risk assessment selection tools or methods.
- Satisfy all cloud actors in cloud computing environment.
- At the end the ACRAM will solve the major problems regarding cloud computing security.

The second section reviews related work, the third section gives an overview of the proposed risk assessment model, the fourth section presents the approach in detail, the fifth section presents a case study, and the last one provides a conclusion and perspectives.

2. RELATED WORK
In the next section, we will classify the risk assessment for cloud computing into various categories: risk assessment as service, quantitative, qualitative, semi-quantitative, hierarchic, risk assessment based on graphs and trust matrix.
2.1. Risk Assessment as Service

Security as a service solutions have been presented to provide and support security assessments in which a hosted cloud solution will make assessments and stores the resulting data. Actually, several tools for a number of security assessment areas have been implemented using the delivery model SecaaS [1], [2]. In the provision of SecaaS model, cloud consumers get the typical advantages of using cloud computing such as scalability and service on demand [3]. In [4], the risk assessment as a service is presented as a new paradigm for measuring real time risk by one or more entities in the cloud. A cloud provider can perform continuous self-assessments as a best practice by assessing its own execution environment. However, this work has not implemented such a service but rather offer it as a paradigm to be pursued. In [19], a new approach is proposed to deploy Risk-Assessment-as-a-Service (RAaaS) for both the cloud clients and the cloud provider. It focuses on providing the assessment service for every cloud client and cloud provider in the cloud environment, where everyone can assess a cloud service before adopting it. As a result, the party that deploys the assessment procedure can perform an informed decision to trust a specific or several cloud providers.

2.2. A Semi-quantitative Risk Assessment

In [6], a SEMI-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) prioritizes and categorizes cloud risks according to their impact on different Business Level objectives in a given organization. The approach is designed for a Cloud Service Provider (CSP) to improve the achievement of a BLO, i.e., profit maximization, by managing, assessing, and treating Cloud risks. In an exemplary experimentation, the risk assessment approach demonstrates that it enables a CSP to maximize its profit by transferring risks of provisioning its private Cloud to third party providers of cloud infrastructures. However, a simple method for qualitative or quantitative analysis will lead to the inaccuracy and one-sidedness of the evaluation results. Therefore, several studies used a composed method of qualitative and quantitative analysis to assess risk in cloud computing [7], [8], [9], [10].

2.3. Risk Assessment Based on Graphs

Graphs and mathematical models can be used to address and calculate security risk in clouds by simulating Graphs and mathematical models can be used to address and calculate security risk in clouds by simulating attacker possibilities. In [11], they presented a mathematical model for threats that considers communication inorder to identify security risk for individual entities, and then calculates it for a whole enterprise. The model is built by representing communications as a directed graph and then established a matrix to discover the risk. Furthermore, in [12], a hybrid risk-analysis method based on decision tree analysis (quantities) and risk matrix (qualitative) is proposed for risk assessment. In this method, risk factor from a user’s viewpoint is systematically extracted with the Risk Breakdown Structure (RBS) method then analysed and evaluated. Corresponding measures are produced on the basis of these results. The risk matrix method is used to classify risk into four kinds (Risk Avoidance, Risk Mitigation, Risk Acceptance, and Risk Transference) in accordance with the generation frequency and degree of incidence.

2.4. A Hierarchy Risk Assessment

In [13] a security risk assessment method has been introduced based on an Analytic Hierarchy Process (AHP) model. The assessment is carried out using the principles of: decomposition, pair wise comparison, and synthesis of weights. Thus, AHP has three layers of decomposition: formulating the problem of assessing cloud security risk in a hierarchical
structure is the first step in AHP. Then, in level two, 8 major factors were identified for assessing. In level three, 39 factors were identified corresponding to higher levels and specific local conditions. The evaluation module uses the constructed AHP tree to assess the system with the help of the judgment matrix that is filled by the cloud's experts. Finally calculating the weighted vectors and getting the final risk order. In [14], a hierarchical framework is built to analyze the risk and set the goal for the assessment. After that, an indicator system is built under each principle and sub indicators are introduced for assessment. For example, the first indicator could be risk of cloud computing platform, risk of cloud storage, risk of cloud security and soon. Secondary indicators of cloud platform risk could then be risk of operating system, risk of application software and risk of availability.

2.5. Risk Assessment Trust Matrix
In [15], Trust Matrix is used for security risk analysis in cloud environments. Two variables, namely “data cost” and “provider’s history” are considered. In “data cost” users can define a cost to data based on the data’ scriticality whereas “Provider’s history” includes the record of the past services provided by the provider to consumers. Additionally, Cloud Control Matrix (CCM) has been released by CSA, as a baseline security control framework designed to help enterprises assess the risks associated with a cloud provider. The CCM has included a risk management domain to ensure that formal risk assessments are aligned with the enterprise-wide framework, planned and scheduled at regular intervals determining the likelihood and impact of identified risks, using qualitative and quantitative methods. Thereby, it facilities transparency and increase trust level between the cloud customer and the cloud in order to make cloud a secure environment to the future of business [16].

2.6. A Quantitative Risk Assessment
In [5], a quantitative risk and impact assessment framework (QUIRC) is introduced to assess associated six key categories of security objectives (SO) (i.e., confidentiality, integrity, availability, multi-party trust, mutual audit ability and usability) in a cloud computing platform. The impact is determined by Subject Matter Experts, the knowledgeable about the impact of threats on their particular type of business.

2.7. A Qualitative Risk Assessment
The European Network and Information Security Agency (ENISA) [6] has published a guide that allow an informed assessment of the security risks and benefits of using cloud computing. For the purposes of the risk assessment, a medium-sized company was used as a use case and the aim was to expose all possible information security risks. The risks identified in the assessment are classified into three categories: technical, legal and policy and organizational issues. Each risk is presented in a table which includes probability level, impact level, reference to vulnerabilities, reference to affected assets and level of risk. The estimation of risk levels is based on ISO/IEC 27005.

2.8. Various Bodies
Various bodies such as the Cloud Security Alliance (CSA), the European Network and Information Security Agency (ENISA), and the US National Institute of Standards and Technology (NIST) have released documents assisting organizations and customers in the evaluation of the security issues related to cloud computing [21, 22, 23]. The Cloud Controls Matrix released by CSA provides an useful description of the security principles aiming to guide cloud vendors and help cloud clients in assessing overall security risks of a cloud service provider [22]. NIST Special Publication 800-144 provides an overview of the security
and privacy challenges for public cloud computing and give recommendations that organizations should consider when outsourcing data, applications, and infrastructure to a public cloud environment.

In an early study by ENISA [21], a cloud-specific, semi-qualitative risk assessment process was generally described using three use-cases: the SMEs’ perspective on cloud computing, the impact of cloud computing on service resilience, and a scenario on cloud-based e-Health applications. The ENISA study included a table showing the distribution of feared events’ probabilities and impacts having a scale of 0 to 8, and classifying low risk, medium risk and high risk. Feared events were classified into three categories: policy and organizational, technical, and legal. Within the first category, lock in, loss of governance, and compliance challenges were mentioned as having in some cases very high impact. Namely, lock in refers to the way tools, procedures and standard data formats or services interfaces are provided on the cloud; if portability is not guaranteed, the migration from one provider to another one may be extremely difficulty for a customer. This could be the cause for a business failure should the cloud provider go bankrupt or be acquired by another company. Loss of governance over data and services can have a potentially severe impact on any organization’s mission, leading to the impossibility of satisfying requirements about confidentiality, integrity and availability of data. Compliance problems may arise due to the migration of services to the cloud, since it is difficult for the cloud providers to provide evidence of meeting industry standards or regulatory requirements. Other feared events mentioned in the study include loss of business reputation due to co-tenant activities, and unwanted disclosure of information to co-tenants. The former event is linked to threats of malicious activities on the part of co-tenants that may affect the reputation of the other customers who are using the same cloud infrastructure. The latter event may be due to failure of mechanisms separating storage, memory and routing between different cloud actors of the shared infrastructure caused by different kind of threats, such as guest-hopping attacks, or SQL injection attacks exposing multiple customers’ data stored in the same table.

2.9. Risk Assessment in Whitepapers
A recent whitepaper [24] describes a qualitative risk assessment methodology specific for clouds. It starts by considering risk factors that change when an organization shifts from a traditional infrastructure to a cloud-based one. The analysis is based on the risk taxonomy presented by the Open Group [25]. The transition to a cloud infrastructure may change the probability of the occurrence of a harmful event, reducing the effort necessary to carry on an attack when a cloud specific vulnerability can be exploited. To denote a threat as cloud specific, four indicators are proposed. A first category collects all threats that are intrinsic to cloud computing, such as the possibility for an attacker to escape from the virtualized environment, the possibility to ride or hijack sessions in shared web applications, threats to the integrity and confidentiality of data caused by the insecure usage of cryptography or the selection of flawed implementation of cryptographic primitives. Other specific threats are the ones concerning problems with standard security controls, such as the difficulties to execute network security controls in virtualized environment, poor management or storage of the of encryption keys, the difficulty of establishing security metrics suitable to monitor the security status of cloud resources.

2.10. Synthesis
After reviewing the literature, several risk assessment methodologies and frameworks have been reviewed and suggested. The risk assessment methods have been classified into seven categories: assessment as a service, quantitative, qualitative, hierarchal, graph analysis, semi-
quantitative, and security matrix assessment. In addition to the risk assessment methods that have been reviewed, the CSA and ENISA lead a number of ongoing research initiatives (security guidance, CCM and STAR). Despite all these methodologies and initiatives, currently no complete and concise methodology exists for analyzing and evaluating security risks of cloud based solutions. A cloud-specific threats, vulnerabilities and risks have already been identified or assessed by numerous sources, but it still remains unclear how to assess risks basing on Information Risk Management frameworks or methods in the context of the Cloud. Thus, the adoption of cloud solutions in a number of industries is stopped. Most of the studies view the problem of assessing security risks either from cloud customer or cloud provider perspectives. The need for a comprehensive, shared, collaborative and intelligent risk assessment methodology that considers both customer and provider is recommended. Such as shared assessment enables the cloud provider to prove how the security risks have been managed and mitigated, as well as enabling the cloud consumer to determine the risk tolerance and define security requirements accordingly. The risk assessment in cloud computing environment will be more efficient and more autonomous by using the intelligent expert agents in our architecture makes.

3. DESIGN OF THE PROPOSED ARCHITECTURE

3.1. Description of the Proposed Architecture

This paper presents a new risk assessment model in cloud computing environments. The proposed model changes the generally current paradigm in research on cloud risk assessment, in which the CA entity is responsible for the specification of security requirements and analysis of these requirements in its own environment based on the multi-agent system (intelligent, collaborative and transparent risk assessment model). To make the risk assessment more transparent in cloud computing environment, the proposed model includes two major entities with active participation in risk assessment, the cloud actor and the risk manager.

3.2. Communication Layer

Agent Interface interacts with the all Cloud actors, the cloud manager, receiving configurations and also the Cloud Manager specification and the final results of risk analysis. The Agent interface gives the entries for each user and returns them to the coordinator agent.

3.3. Coordination Layer

Agent Coordinator: it is the agent responsible for the decomposition of tasks and planning. The coordinator agent maintains a set of beliefs about the capabilities of all the agents that make up the ACRAM method. It can decompose a given task into a number of sub-tasks and send them to the relevant agents to treat, in order to achieve the desired objectives.

3.4. Risk assessment Layer before the Cloud adoption

**Identifier assets MAS:** on the basis of inputs from each user interacts with the focal point for analyzing and defining the corresponding assets to each Cloud actor and suggested the resource value for each asset.

**Vulnerability Identifier MAS:** on the basis of inputs from each user interacts with the focal point for analyzing and defining the vulnerabilities for each Cloud actor, and suggests the value of each vulnerability based on old cases.

**Threat Identifier MAS:** based on the output of the resource identifier and the identifier of the vulnerabilities, the agent interacts with the focal point for analyzing and defining the corresponding associated threats, and suggests the value for each threat. The deciding officer
An Autonomous Risk Assessment Model for Cloud Computing Based on Multi-agent System before and after the Cloud Adoption

has two main functions: the function (1) is intended to provide a list of values for each resource; the function (2) is intended to provide a list of values for each vulnerability [26].

![Image](https://via.placeholder.com/150)

**Figure 1** The risk assessment architecture

\[
F(A) = \max (a_i) + 0.5 (m_{-1}) + 0.4 (m_{-1}) 0.3 (m_{-1}) + 0.2 (m_{-1}) + 0.1 (m_{-1}) \quad (1)
\]

\[
F(V) = \max (v_j) + 0.5 (h_{-1}) + 0.4 (h_{-1}) 0.3 (h_{-1}) + 0.2 (h_{-1}) + 0.1 (h_{-1}) \quad (2)
\]

*Risk Identifier MAS*: based on the output resource identifier, the identifier of the vulnerabilities and threats identifier interacts with the focal point for analyzing and defining the associated risks, and calculates the value of risk.

*Measures Identifier MAS*: based on the results of risk, this agent may propose appropriate measures for each player in the cloud environment Cloud Computing.

### 3.5. Risk assessment Layer after the Cloud Adoption

*Risk assessment checker*: on the basis of the data of each cloud actor, the risk assessment checker can verify whether the risk assessment is after or before the Cloud adoption.

*Risk assessment maker*: on the basis of the state of each cloud actor can define the need of risk assessment.

#### 3.5.1. Design of the proposed architecture

*The flowchart*

The approach is divided into two major stages as the risk assessment before and after the cloud computing adoption. A simple flowcharts of the approach is shown in Fig. 2, Fig.3 and Fig.4.
Figure 2 The simplified flowchart of risk assessment model for cloud risk manager before the cloud adoption

Figure 3 A simplified flowchart of Risk assessment model for Cloud actors before the cloud adoption

Figure 4 A simplified flowchart of Risk assessment model for Cloud risk manager after the cloud adoption
The use Case Diagram

On the website administrator, the risk manager on the website can define the overall cloud services and the possible users. The expert intelligent entity can define the corresponding security objectives, vulnerabilities and threats. More detail can be seen in Fig. 5.

![Figure 5](image1)

**Figure 5** Use case diagram application risk manager before cloud adoption

The main actors of the use case diagram the client application and the cloud provider. To access the content of cloud provider’s risk assessment must log in first. Content that can be accessed by cloud actors includes information about the initial security objectives, the corresponding vulnerabilities, the corresponding threats, the corresponding risks and the proposed measures. Then, cloud actor can be an active entity by proposing the adequate security objectives and the efficient measures. In this case, all the contents are defined by the expert intelligent agent Fig.6.

![Figure 6](image2)

**Figure 6** Use case diagram application cloud actor

4. EXPERIMENTATIONS

ACRAM is implemented as an autonomous system accessible through Web. Programming languages used for ACRAM are JAVA EE. The cloud actors can collaborate in the risk assessment using the Web interface. Input information is passed to the expert agent and results along with the explanation are returned back to the cloud actors.

A web interface is shown below in the Fig.7. This web interface can help the cloud organization to define their associated assets, vulnerabilities and threats.
Figure 7 A web interface of Risk assessment tool (in Cloud organization)

Figure 8 A web interface of Risk assessment tool (for cloud actors)

A web interface is shown below in the Fig.8. This web interface can help the cloud actors to collaborate and to be aware about their associated assets, vulnerabilities, threats, risks and measures.

5. ACRAM EVALUATION

Generally, risk assessment methods take a long time and processed slowly. Contrary to other methods, our method proposes a new intelligent, comprehensive, collaborative, transparent and shared risk assessment method based on expert agents which we can assess risk before and after the adoption of cloud computing. Also using the history of the risk assessment before the cloud adoption, can help the risk manager to determine which assets will be attacked and all the presents’ vulnerabilities in cloud environment. Our model ensures fast assessment with specific calculations as mentioned in equation (1) and (2).

<table>
<thead>
<tr>
<th>Features</th>
<th>Current solutions</th>
<th>Our solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support tool</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Automation efficiency</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Adaptability</td>
<td>Not all</td>
<td>Yes</td>
</tr>
<tr>
<td>Comprehensive</td>
<td>Not all</td>
<td>Yes</td>
</tr>
<tr>
<td>Shared with the</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
An Autonomous Risk Assessment Model for Cloud Computing Based on Multi-agent System before and after the Cloud Adoption

<table>
<thead>
<tr>
<th>Features</th>
<th>Current solutions</th>
<th>Our solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>different actors in CCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Before and after cloud adoption</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Collaboration</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

6. CONCLUSIONS

In this paper, a new approach have been performed in detail on the basis of the proposed web based solution, to demonstrate the effectiveness of this new comprehensive and shared risk assessment method for cloud computing that will add a great assistance and help to both cloud consumers and cloud providers. As consequence, with such an approach, the cloud consumers can be guaranteed data security and the cloud providers can win the trust of their consumers.

As future work, the authors are also working to implement as cloud web service and we will show experimental results to demonstrate the effectiveness of the new approach. In addition, the authors will give primordial improvements of the proposed risk assessment method.

REFERENCES


[22] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v2.1, 200

[23] NIST. Recommended security controls for federal information systems and organizations, 2009


