Cloud Computing: A Risk Assessment Model

Alireza Shameli-Sendi and Mohamed Cheriet
Synchromedia Laboratory for Cloud Computing
École de technologie supérieure
Montreal, Canada
alireza.shameli@synchromedia.ca, mohamed.cheriet@etsmtl.ca

***Abstract*—Cloud computing has recently emerged compelling paradigm by introducing several characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Despite the fact that cloud computing offers huge cost benefits for companies, the unique security challenges have been introduced in a cloud environment that make risk assessment challenging. Cloud consumers need a protection to their cloud applications against cyber attacks. Although some security controls and policies are devised for each element of cloud computing, we need a framework with overall quantitative risk assessment model.**

The aim of this paper is to propose a framework for assessing the security risks associated with cloud computing platforms. The fully quantitative, iterative, and incremental approach enables cloud customer/provider to assess and manage cloud security risks. A proper result of risk assessment leads to have appropriate risk management mechanism for mitigating risks and reach to an acceptance security level.

***Keywords*-Cloud computing; Risk assessment; Risk management;**

I. Introduction

Cloud computing has critical role in today's mission-critical business requirements. The cloud provides convenient and on-demand network access to a shared pool of computing resources with great efficiency and minimal management overhead [1]. This infrastructure encouraged companies, that were involving with purchasing software or new hardware, start relying on cloud-services. On the other hand, we are surrendering all company's sensitive information to a third-party cloud service provider. Thus, security is one of the major issues in cloud computing and a critical requirement of the cloud provider (CP) and cloud customer. With these points in mind, the organizations have to have right comprehensive about important risks in cloud computing environment [3]. This requires proper security Risk Assessment (RA) and then security Risk Management (RM) in cloud. Thus, we need an integrated framework for managing security risks in all levels in cloud [2].

There are some standards available for risk assessment such as ISO/IEC 27002:2005 [4], NIST risk management guide for information technology systems [5], and "best practice" documents that are developed by security organizations, such as CERT's OCTAVE [6] method. In this sense, cloud security (risk assessment and management) looks unsuitable [7] with current (Manual) information security risk assessment approaches (In spite of difficulty to automate risk assessment in cloud, there are some efforts in this area like Cloud Audit (A6) [8]). If we apply these standards to cloud not only there are no details on how to implement it in cloud computing but also they left some questions unanswered: 1) how to segregate security roles and responsibilities? 2) which activities have to be done by each role?, 3) which artifacts have to be generated by each activity. The main contribution of this work is to focus on addressing these questions and find an appropriate solution for risk assessment as a service (RAaaS) in cloud computing. The paper is organized as follows: first, we will discuss about the proposed model. Then experimental results are given in Section III. Finally, Section IV concludes the paper.

II. Proposed Model

The proposed framework is an iterative and incremental approach that can help design, implement, monitor, and manage information security management system in Cloud Computing. This approach provides any cloud consumer with a predictable life-cycle security process for the development, adoption, and continual improvement of the Information Security solution. In our model, iterations are planned in number, duration, and objective. A proper assessment of objectives enables the move to the next iteration successfully.

As seen in Figure 1, the proposed model includes two dimensions: static, which are disciplines, and dynamic, which are phases. In this architecture, the static dimension comprises six disciplines that are represented by business modeling, asset, security policy, implementation, configuration and change management, and project management. The dynamic dimension contains four life-cycle phases that are illustrated by inception, analysis and design, construction, and monitoring. Also, each phase can iterate. The area under the curve that is associated with each discipline shows the relative amount of effort and activity required to perform it over time. Along the vertical axis are the disciplines, which are a collection of workflows related to a major area of concern within the overall project. From a security management perspective, each phase is concluded by a major milestone. In each milestone, there are some major criteria that must be evaluated to determine whether the objectives

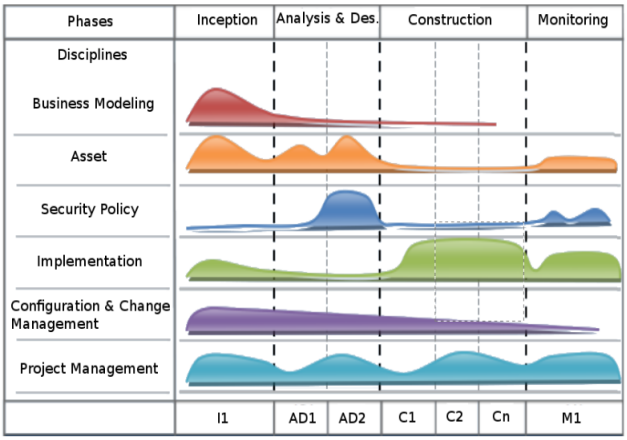

Figure 1: Architecture (Phases: dynamic dimension; Disciplines: static dimension)

of the phase have been met or not. These criteria are the phases' objectives that must be reached.

A workflow consists of some activities that produce a result of observable value. Figure 2 presents, identifies and analyzes risk workflow from asset discipline. As seen in Figure 2, in each workflow, we have some roles, activities, and artifacts that are integrated to provide the goal of workflow. As mentioned, role segregation has not been considered in risk assessment standards and other security models properly. Our model proposes appropriate role segregation and makes sure that we establish a framework where we can easy segregate security roles and responsibilities. As mentioned, Figure 2 illustrates one of the model workflow that are relevant to the asset discipline. Roles segregation is clearly shown in this workflow that includes eight roles: *Asset Evaluator, Vulnerability Evaluator, Threat Evaluator, Risk Evaluator, SaaS Security Specialist, PaaS Security Specialist, IaaS Security Specialist,* and *Data Security Specialist*. Seven activities have been specified and in fact, each role is responsible to perform the related sub-activities. Also, all the artifacts (output of activities) should be updated and each role has to keep updated the related sections of each artifact.

A. Risk Assessment

In the proposed model, we use the fuzzy multi-criteria decision making technique for risk assessment in Cloud Computing. First, the important coefficients for the basic goals of information security, which are confidentiality, integrity, and availability (CIA) are determined [12]. Second, the basic goals of information security are used to calculate the value of each asset. Then, vulnerability indices are created for each asset separately. In this model, linguistic variables are used to obtain expert opinions for weighting criteria and for rating alternatives as shown in Table I and Table II.

CIA Triad Evaluation: This step is key to calculating

Table I: Linguistic variables and fuzzy equivalents for the importance weighting of each criterion

Linguistic variables	Fuzzy triangular
Very Low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium Low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium High (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1.0)
Very High (VH)	(0.9, 1.0, 1.0)

Table II: Linguistic variables and fuzzy numbers for the criterion ratings

Linguistic variables	Fuzzy triangular
Very Poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium Poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium Good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very Good (VG)	(9, 10, 10)

the CP's risks, and we can determine which of these three complimentary goals is more important to a CP. The weight of confidentiality (*C*), integrity (*I*), and availability (*A*) are denoted as w_C, w_I, and w_A respectively. We use *n* experts (*e*) to evaluate the CIA triad. $\tilde{x}_i^{e_k}$ illustrates the expert opinion *e* in domain *i*. Finally, the base of the *CIA* triad can be calculated using the following formula:

$$
\begin{aligned}
& i \in [1,2,3] \\
& k \in [E_1, E_2, ..., E_n] \\
& \tilde{x}_i^{e_k} = (a,b,c) \\
& \tilde{w}_C = \tfrac{1}{n}[\tilde{x}_1^{e_1}(+)\tilde{x}_1^{e_2}(+)...(+)\tilde{x}_1^{e_n}] \\
& \tilde{w}_I = \tfrac{1}{n}[\tilde{x}_2^{e_1}(+)\tilde{x}_2^{e_2}(+)...(+)\tilde{x}_2^{e_n}] \\
& \tilde{w}_A = \tfrac{1}{n}[\tilde{x}_3^{e_1}(+)\tilde{x}_3^{e_2}(+)...(+)\tilde{x}_3^{e_n}] \\
& \tilde{W} = [\tilde{w}_C, \tilde{w}_I, \tilde{w}_A]
\end{aligned}
\tag{1}
$$

Asset Value: The *CIA* triad should be used to calculate the value of each asset. We use *n* experts to evaluate each asset. Every expert assigns a value from the list of linguistic variables to each part of the *CIA* triad. For example, a large number of important linguistic variables for confidentiality means that this asset's privacy level is very high, and fewer linguistic variables for availability means that the availability of the asset is not as important. The asset value could be calculated as follows:

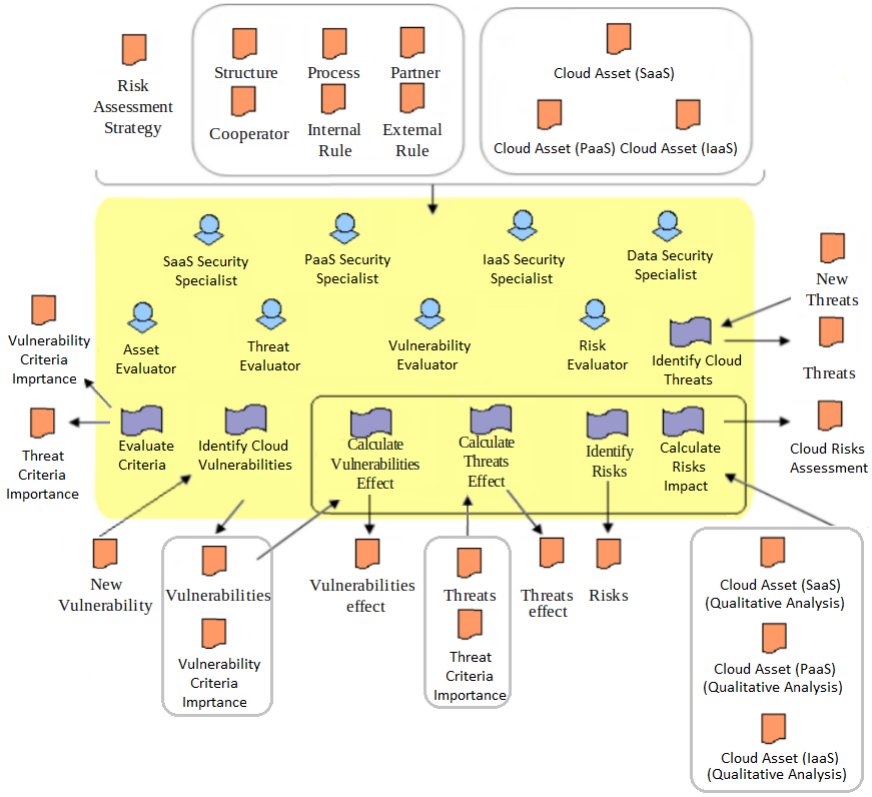

Figure 2: Identify and Analyze Risk Workflow

$$
\begin{aligned}
&i \in [1,2,3] \\
&j \in [A_1, A_2, ..., A_n] \\
&k \in [E_1, E_2, ..., E_n] \\
&\tilde{x}_{ij}^{e_k} = (a,b,c) \\
&\tilde{x}_{ij} = \tfrac{1}{n}[\tilde{x}_{ij}^{e_1}(+)\tilde{x}_{ij}^{e_2}(+)...(+)\tilde{x}_{ij}^{e_n}] \\
&\tilde{A} = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_n \end{array} \begin{array}{c} \begin{array}{ccc} C & I & A \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \tilde{x}_{13} \\ \tilde{x}_{21} & \tilde{x}_{22} & \tilde{x}_{23} \\ \vdots & \vdots & \vdots \\ \tilde{x}_{n1} & \tilde{x}_{n2} & \tilde{x}_{n3} \end{bmatrix} \end{array}
\end{aligned} \tag{2}
$$

The next step is to linearly normalize the consolidated matrix through the following relationship (category B is related to the benefit criteria and category C is related to the cost criteria) [10] [11]:

$$
\tilde{r}_{ij} = \begin{cases} \frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} & \text{if } j \in B \\ \frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}} & \text{if } j \in C \end{cases} \tag{3}
$$

$$
\begin{aligned}
c_j^* &= max \quad c_{ij} \quad if \quad j \in B \\
a_j^- &= min \quad a_{ij} \quad if \quad j \in C
\end{aligned}
$$

Then, the combined weights are defuzzified, using the Signed Distance method $(w_C.def, w_I.def, w_A.def)$, and normalized using the following formula:

$$
\begin{aligned}
&i \in [1,2,3] \\
&w_i.def = \frac{w_i.def}{\sum_i w_i.def}
\end{aligned} \tag{4}
$$

After defuzzification of each criterion, we calculate the weight matrix:

$$
\begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & \cdots & \tilde{x}_{2n} \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \cdots & \tilde{x}_{mn} \end{bmatrix} * \begin{bmatrix} w_C.def \\ w_I.def \\ w_A.def \end{bmatrix} \tag{5}
$$

The final step is to establish the asset value matrix by combining the criteria and the defuzzification of fuzzy values by the Signed Distance method for each asset. AV_i illustrates the calculation of an asset value based on the CIA triad.

$$\tilde{C}, \tilde{I}, \tilde{A} = (a, b, c)$$
$$\tilde{AV}_i = \tilde{C} + \tilde{I} + \tilde{A}$$
$$AV_i.def = \frac{a+2b+c}{4}$$

$$A = \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{matrix} \begin{bmatrix} AV_1.def \\ AV_2.def \\ \vdots \\ AV_n.def \end{bmatrix} \tag{6}$$

Vulnerability Effect: A vulnerability is a flaw or weak point in the design or implementation of a system security procedure. It could be exploited by an attacker or may affect the security goals of the CIA triad. We represent the vulnerability effects with a percentage, and, for better accuracy, we obtain help from *n* experts. We define two criteria: 1) *Threat Capability (TC)*, which illustrates the extent to which the attacker is capable of compromising an asset. Expert opinion in evaluating this factor for each asset is based on the recent history of threats against the asset respect to the vulnerabilities; and 2) *Control Strength (CS)*, which indicates the extent to which each asset is resistant to all relevant threats. A low linguistic variable for the *CS* factor means that there is poor security control to this vulnerability and related threats have a high probability of occurring [13]. The vulnerability effect could be calculated as an asset value, but the final step in this case is different. In the final step, we first defuzzify the fuzzy values using the Signed Distance method for the *TC* and *CS* attributes. Then, we establish the asset vulnerability matrix. This matrix represents *n* vulnerabilities with two attributes. Finally, we calculate the vulnerability effect using the division function:

$$\tilde{TC}, \tilde{CS} = (a, b, c)$$
$$TC_i.def, CS_i.def = \frac{a+2b+c}{4}$$

$$\boldsymbol{V} = \begin{matrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{matrix} \begin{bmatrix} TC_1.def & CS_1.def \\ TC_2.def & CS_2.def \\ \vdots & \vdots \\ TC_n.def & CS_n.def \end{bmatrix} \tag{7}$$

$$V_i = TC_i.def / CS_i.def$$

Threat Effect (TE): We used the *CIA* triad to calculate threat effects. We use *n* experts to calculate those effects. For each threat, we should get help from relevant experts to get better results. The calculation method of threats is similar to the one for assets.

Risk Identification and Impact: The objective of risk identification is to identify all possible risks to the assets. In the previous steps, we exposed all the vulnerabilities of each asset. We also exposed all threats to the SaaS software. In this step, we determine which threats are related to which vulnerability. The relationship between each vulnerability and threat is a risk. The risk impact is modeled using three parameters: *Asset value* (A), *Vulnerability effect* (V), and *Threat effect* (T). Below, we show how the risk impact can be calculated with the fuzzy model.

$$R = \begin{matrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{matrix} \begin{bmatrix} A[i_1] * V[j_1] * T[k_3] \\ A[i_1] * V[j_2] * T[k_4] \\ \vdots \\ A[i_n] * V[j_m] * T[k_l] \end{bmatrix} \tag{8}$$

Finally, we have an ordered list of risk impact in SaaS layer of cloud computing. In the risk management process, the customer provider has to chose appropriate solution to deal with them.

III. Experiment Results

A. Environment

To better illustrate our approach, we present a case study about an Industrial Car Company. This company decides to manage the Enterprise Resource Planning (ERP) systems in a Cloud Computing environment. ERP integration can be very complex and time consuming considering the manufacturing process, inventory, shipping, supply-chain management, and accounting. Cloud based ERP provides managers and engineers with better performance, resource scalability, and integration. The company simple uses secure web browser to login to cloud.

B. Results

We used three cloud Decision Makers (DM) in our case study: DM1, DM2, and DM3. The first step in our model is to indicate the importance of asset, vulnerability, and threat criteria (Tables III and VII).

Table VII presents the decision makers' opinion about the importance of vulnerability criteria. They all believe that the history of cloud threats is not very important (C1: Threat Capability). They accentuate preparation to tackle threats by applying secure controls or configurations in all assets in cloud (C2: Control Strength). Of course, they could have a different opinion such that the history of threats against the assets is important than how much each asset is resistant to all relevant threats. The literature shows that experts accentuate preparation to tackle threats by applying secure controls or configurations in all layers of cloud (C2: Control Strength). In other hands, they connive at the history of cloud threats (C1: Threat Capability). Table IV illustrates cloud assets in our case study that consists of four assets. A1 is Cloud Customer database that has interact with company web application (A2) and ERP software (A3). Cloud Provider exposes a software interface or API (A4). Industrial Car Company uses this interface to manage and interact with cloud services.

Table III: Importance weightings of the criteria for Cloud Customer

	DM1	DM2	DM3
C1: Confidentiality	VH	H	VH
C2: Integrity	VH	H	VH
C3: Availability	VH	VH	H

Table IV: Cloud Assets

	Asset
A1	Database
A2	Company Website
A3	ERP Software
A4	Cloud Interfaces and APIs

Table VIII illustrates unique vulnerabilities in the cloud respect to the cloud assets [9]. Each vulnerability is mapped to an asset. As Table VIII shows company web site and ERP software has two vulnerabilities while company database and cloud interface has one. As Tables V, IX, and XI illustrate, the experts use the linguistic rating variables to evaluate assets, their related vulnerabilities, and threats with respect to their criteria. Table IX column "Control Strength" represents that all experts believe that there is not enough security control for all vulnerabilities respect to the cloud assets. For the threat capability they assigned appropriate linguistic variables based on threat history in the Internet. Table XI shows a list of threats with relative values reflecting their potential impact on confidentiality, availability, and integrity in our case study. The next steps involve constructing the fuzzy decision matrix and the fuzzy weighted normalized decision matrix. Tables VI, X, and XII present the final results after the defuzzification step. As Table V illustrates, based on expert opinion, company data is more important compare to other assets. Table X shows that vulnerability V5 (Weak Encryption or Authentication Mechanism) has the biggest effect because not only it has good threat history but also there is not very strong implemented security control about it in our cloud computing. It looks threat T3 (Cross-site scripting), can bypass access controls, will be very dangerous for our cloud and has high impact on CIA triad. The final step is risk assessment involves a process to compute the residual risk arising from each combination of assets with the related vulnerabilities and threats. Table XIII illustrates the identified risks in our case study, the impact, and relative rank from the most serious to the least.

Table V: Ratings of all assets by decision makers under criteria

	Asset	Confidentiality			Integrity			Availability		
		DM1	DM2	DM3	DM1	DM2	DM3	DM1	DM2	DM3
A1	Database	G	VG	G	G	VG	G	VG	VG	VG
A2	Company Website	MG	MG	G	G	MG	G	F	F	G
A3	ERP Software	G	G	VG	G	G	G	VG	VG	G
A4	Cloud Interfaces and APIs	VP	P	MP	F	F	MG	VG	VG	VG

Table VI: Asset Values

	Confidentiality	Integrity	Availability	Fuzzification Value	Defuzzification Value	Normal
A1	(0.26,0.32,0.33)	(0.26,0.31,0.33)	(0.30,0.33,0.33)	(0.811, 0.956, 1)	0.931	93
A2	(0.19,0.26,0.31)	(0.21,0.28,0.32)	(0.14,0.21,0.27)	(0.544,0.744,0.900)	0.733	73
A3	(0.26,0.31,0.33)	(0.23,0.30,0.33)	(0.28,0.32,0.33)	(0.767,0.933,1)	0.908	91
A4	(0.01,0.04,0.10)	(0.12,0.19,0.26)	(0.30,0.33,0.33)	(0.433,0.567,0.689)	0.564	56

Table VII: Importance weightings of the vulnerability criteria

	DM1	DM2	DM3
C1: Threat Capability	M	MH	ML
C2: Control Strength	VH	VH	VH

Table VIII: Vulnerabilities

Id	Name	Asset
V1	Poor Integrity or Backup Control	A1
V2	Insertion of unchecked data in restricted system locations	A2
V3	Lack of hashes to protect the cookie	A2
V4	Flaw in the security design of software	A3
V5	Weak Encryption or Authentication Mechanism	A3
V6	Insecure Interfaces and APIs	A4

Table IX: Ratings of all asset vulnerabilities by decision makers under criteria

	Threat Capability			Control Strength		
	DM1	DM2	DM3	DM1	DM2	DM3
V1	MP	MP	MP	G	G	MG
V2	G	MG	P	MG	G	G
V3	MP	MP	F	F	F	F
V4	MG	MP	G	MG	F	MP
V5	VG	G	G	MG	F	MG
V6	F	F	P	MG	F	F

Table X: Asset vulnerability Effect

	Threat Capability	Control Strength	Defuzzification TC Value	Defuzzification CS Value	Vulnerability Effect	Normal
V1	(0.02,0.05,0.09)	(0.23,0.30,0.35)	0.053	0.292	0.182	18
V2	(0.07,0.10,0.13)	(0.23,0.30,0.35)	0.1	0.292	0.344	34
V3	(0.06,0.06,0.10)	(0.18,0.18,0.25)	0.074	0.196	0.376	38
V4	(0.08,0.11,0.14)	(0.11,0.18,0.25)	0.111	0.179	0.620	62
V5	(0.14,0.17,0.18)	(0.15,0.23,0.30)	0.161	0.226	0.711	71
V6	(0.04,0.06,0.10)	(0.13,0.20,0.27)	0.066	0.202	0.328	33

Table XI: Ratings of all threats by decision makers under criteria

	Asset	Confidentiality			Integrity			Availability		
		DM1	DM2	DM3	DM1	DM2	DM3	DM1	DM2	DM3
T1	Data theft	MP	F	P	MP	F	P	VP	VP	VP
T2	Unauthorized access	VG	VG	VG	VG	VG	VG	F	F	F
T3	Cross-site scripting	VG	G	G	VG	G	G	MG	F	MG
T4	Cookie manipulation	MG	MG	G	VG	VG	G	P	MP	MP
T5	Data loss/manipulation	VG	VG	VG	VG	VG	VG	P	VP	MP

Table XII: Threat Effect

	Confidentiality	Integrity	Availability	Fuzzification Value	Defuzzification Value	Normal
T1	(0.04,0.10,0.17)	(0.04,0.10,0.17)	(0.00,0.00,0.04)	(0.09,0.20,0.37)	0.216	22
T2	(0.30,0.33,0.33)	(0.30,0.33,0.33)	(0.15,0.20,0.28)	(0.75,0.87,0.95)	0.857	86
T3	(0.26,0.31,0.33)	(0.26,0.31,0.33)	(0.17,0.25,0.33)	(0.68,0.88,1.00)	0.859	86
T4	(0.19,0.26,0.31)	(0.28,0.32,0.33)	(0.03,0.09,0.17)	(0.49,0.67,0.82)	0.663	66
T5	(0.30,0.33,0.33)	(0.30,0.33,0.33)	(0.01,0.05,0.12)	(0.61,0.72,0.79)	0.710	71

Table XIII: Risks

Risk Id	Threat Id	Vulnerability Id	Asset Id	Risk Effect	Rank
R1	T1	V6	A4	40,656	9
R2	T2	V6	A4	158,928	7
R3	T2	V4	A4	298,592	3
R4	T2	V2	A4	163,744	6
R5	T3	V2	A2	213,452	4
R6	T4	V3	A2	183,084	5
R7	T5	V5	A3	458,731	1
R8	T4	V5	A3	426,426	2
R9	T5	V1	A1	118,854	8

Table XIV: Risk Level

Risk Level	Score	Number of outcomes
Very Low	1-800	0
Low	801-64000	0
Medium	64001-216000	6 (R1,R2,R4,R5,R6,R9)
High	216001-512000	3 (R3,R7,R8)
Very High	512001-1000000	0

C. Risk Level and Risk Management

To understand risk result, we group similar results in graduated levels ranging from Very Low to Very High as Table XIV illustrates. Six risks are in *Medium* level and three risks are in *High* level. This result is very important for risk management. The first step in risk management is to define "acceptance risk level". In our case study, acceptance risk level is Low. It means if all risks fall in *Low* level, there is no concern in our cloud. All risks in our case study pass our threshold and are identified as unacceptable risks. The next step in RA is to identify appropriate security designs or safeguards that could mitigate unacceptable risks and reduce them to below acceptable level. The main question here is that how much the safeguards cost to mitigate a risk. If the cost is very high and the risk reduction is very low, it is obvious that it is not acceptable by cloud customer. The next question is that how much is the risk reduction amount by implementing safeguards. To answer these questions, we ask cloud expert to verify vulnerabilities list (Table IX) and reevaluate linguistic variables. Our framework automatically updates all processes and shows the next level of risk. Then we can decide based on implantation cost and risk reduction amount.

IV. Conclusion

In this paper, we first discussed the main cloud computing characteristics and how these characteristics make hard applying traditional security approaches. Then, we focused on the main issues in manual security standards for implementing risk assessment/management in cloud computing. Since cloud computing is growing rapidly, providing an efficient and reliable solution for security risk assessment is needed. Although having an automated solution is critical and ideal for Risk Assessment as a Service (RAaaS) in cloud, it needs too much effort respect to the cloud computing characteristics. In this paper, we proposed a framework for risk assessment/management in cloud computing environment. Our main contribution consists of proposing a fuzzy multi-criteria decision making technique for analyzing public cloud risks. One major benefit of the proposed model is its ability to keep security management continuously within the cloud computing by an iterative and incremental approach. The limitation of the model is that it is not fully automated in cloud but it is trying to solve the inefficiency of current traditional risk assessment models that have to be used in cloud. As future work, we intend to make use of more sophisticated cloud computing and have some solutions for fully automated risk assessment.

Acknowledgment

This work is partly funded by MSERC RDC to GSTC project and by CRC on Sustainable Smart Eco-Cloud.

References

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011.

[3] S. Ramgovind, M. M. Eloff, and E. Smith, "The Management of Security in Cloud Computing," Proceedings of IEEE International Conference on Information Security for South Africa, 2010.

[4] ISO/IEC 27002:2005. Information technology Security techniques Code of practice for information security management. http://www.iso.org/iso/catalogue_detail?csnumber=50297

[5] National Institute of Standards and Technology, Gary Stoneburner, Alice Goguen, and Alexis Feringa, "NIST SP 800-30 Risk Management Guide for Information Technology Systems," pp. 8-26.

[6] C. Alberts and A. Dorofee, "Managing information security risks," The OCTAVE approach, Addison Wesley, ISBN 0-321-11886-3, 2002.

[7] B. S. Kaliski Jr. and W. Pauley, "Toward risk assessment as a service in cloud environments," Proceedings of the 2nd USENIX conference on Hot topics in cloud computing (HotCloud'10), USENIX Association, Berkeley, CA, USA, 2010.

[8] Cloud Audit. The Automated Audit, Assertion, Assessment, and Assurance API. http://www.cloudaudit.org/

[9] M. Theoharidou, N. Tsalis, and D. Gritzalis, "In Cloud We Trust: Risk-Assessment-as-a-Service," Proceedings of the 7th IFIP WG 11.11 International Conference, pp 100-110, 2013.

[10] C. T. Chen, "A fuzzy approach to select the location of the distribution center," Fuzzy Sets and System, vol. 118, pp. 65-73, 2001.

[11] S. Y. Chou, Y. H. Chang, and C. Y. Shen, "A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes," Operational Research, vol. 189, pp. 232-145, 2008.

[12] A. Shameli-Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: Fuzzy expert model for risk assessment," Proceedings of the Fifth International Conference on Internet Monitoring and Protection, pp. 48-53, Barcelona, Spain, 2010.

[13] J. Jones, "An introduction to factor analysis of information risk (FAIR)," Norwich Journal of Information Assurance, vol. 2, no. 1, pp. 1-76, 2006.