CLOUD'S RISK ASSESSMENT MODEL – A COMPARATIVE STUDY

Bander M. Al-anazi[1], Ahmed E. Youssef[2]
Master of Information Systems, College of Computer & Information Sciences, King Saud University (KSU), Riyadh, KSA
Associate Professor, College of Computer & Information Sciences, King Saud University (KSU) Riyadh, KSA

ABSTRACT:

The field of Cloud computing security is considered a widespread research domain with a considerable quantity of attention, extending from protecting clouds data and source practice to preserving platform and hardware technologies. Considerably, the benefits of cloud computing are enormous, the privacy and security attention of cloud computing have constantly been the locus of infinite cloud clients and an obstruction to its broad adaptation by organizations and industries. The present article in the field of cloud computing offers a systematic literature review and comparative study with a focus on risk assessment. This would support research and cloud business/users organizations in the future to possess an overview of the risk circumstances in the environment of cloud computing. And to proactively outline their natural requirements with this technology.

KEYWORDS: *Risk assessment model, comparative study, cloud computing, threats, vulnerabilities.*

INTRODUCTION

Research Progress in cloud computing (CC) in recent years has ended in significant commercial benefit in employing cloud infrastructures to promote commercial employment and services. Yet, notable improvements in the fields of risk and dependability are essential formerly to widespread commercial adoption can convert to a certainty. Particularly, mechanisms of risk management require being combined within CC infrastructures, in order to advance beyond the best-effort way to maintain the terms that been followed by the current CC infrastructures [1].

The value of risk management in CC is an outcome of the demand to sustain multiple sections concerned in obtaining knowledgeable judgments concerning contractual agreements. The absence of sufficient confidence in a CC service in terms of the doubts correlated with its level of status may limit a CC service user from choosing CC technologies. Although the terms of a 0-risk service is not effective, if not impossible, an efficient and dynamic risk assessment (RA) of service consumption and terms, collectively with the similar reduction tools, can at least afford a technological guarantee that will guide to great confidence of CC service users on one side and a cost-effective and dependable productivity of the resources of cloud service providers (CSPs) on the other side.
In order to perform a task containing a service, Consider an end-user (a CSPs or a broker acting on their behalf) who is a member of the widespread public advancing the CC.

The end-user need shows the task and related conditions officially in a Service Level Agreement (SLA) form. According to this data, in order that the task is completed, the end-user requests to negotiate admittance with Infrastructure Providers (IPs) allowing those services. IPs grant admittance to services and resources through confirmed SLAs penalty, designating risk and price. Cooperation between end-users and IPs and can then be administered by a deal specifying the IP's responsibilities, the penalty the IP requires to pay in the event that it fails to meet its responsibilities and the price the end-user must pay.

The employment of SLAs to administer such cooperation in CC is obtaining momentum [1]. Furthermore, IPs require well-balanced infrastructures, then they can raise the Quality of Service (QoS) and decrease the quantity of SLA breaches. Such a way to increases the economic interest and motivation of end-users to outsource their IT tasks. A requirement to this is the IP's trustworthiness and their capability to successfully achieve an accepted SLA. In all stages of the service lifecycle for these stakeholders Risk assessment is regarded: IPsthroughout service access internal operations and control and end-users throughout service deployment. RA is regarded in the following context in service deployment:

1) What is the risk of dealing with before sending a request from the SLA to IPs, and which IP is less risky?;
2) Once the request reaches the IP from the SLA, regarding the end-user, what is the risk of dealing with it from where the request arrived from?;
3) The IP works in the admission control what is the risk of admitting the SLA request?; and
4) After the end-user receives an offer from the SLA, for using a service in an IP what is the risk connected with this i.e. enrolling an SLA by the IP?

The IP is enabled by the RA to selectively determine which SLA requests to admit (and which to fulfill and monitor consequently at service operation). Then again, end users need to get acquainted, risk-aware choices on the SLA quotes they receive from the IPs so that the choice is satisfactory and time stability risk and cost. They certainly profit of an assessment of the risk of an SLA breach, because it permits them to define the economic assumptions of corresponding to an appropriate SLA offer. In assessing the reliability of an IP's own RA, This is where RA can play a fundamental role. In service operation, RA assets to sustain the following:

1) What is the SLA risk of failure? from the end-user perspective,
2) Similarly what is the risk of failure of a particular SLA from the IP perspective? Of the CC infrastructure? Here, IPs work continuous RA at service operation, observing events of low-level from the infrastructure like the VMs security risk of failure.

Moreover, continuous monitoring service and RA has also performed by end-users level non-functional QoS metrics, for example, the reliability of VMs. as a general methodology, RA has been included into service computing like Grids [2], [3], [4] or concentrating on a particular sort of risk, like SLA achievement [5], [6].

The present article in the field of cloud computing offers a systematic literature review and comparative study with a focus on risk assessment. This would support research and cloud business/users organizations in the future to possess an overview of the risk circumstances in the environment of cloud computing. And to proactively map their indigenous needs with this technology.

LITERATURE REVIEW

2.1 Essential concepts

2.1.1 Cloud computing (CC)

In literature, for cloud computing, there are several definitions. The NIST [4] defines CC as ''a model for allowing ubiquitous, available, on-demand network access to a shared pool of configurable computing resources (such as. Networks, applications, storage, servers, and etc.) That can be immediately released and provisioned with minimum management effort or service provider interaction''. ECSS [5] describes it as the distribution of computational sources from a location other than your current one.

CC can be essentially classified into three main models classified based on to their uses; Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). SaaS which deliver software over the Internet (for instance. Google Docs), PaaS which mainly offer virtualized running environments to CC services (for instance. Force) and IaaS which provide virtualized computing resources as a service (for instance. Windows Live Skydive).

2.1.2 Risk assessment (RA)

"Risk is not totally wrong, as an opposite, it is required to development, and failure is regularly an essential element of learning. Still, we need learn to weigh the potential negative consequences of risk against the possible profits of its related opportunity" [9].

Risk management (RM) refers to a formed collection of methods and activities that are employed to regulate an organization and to manage the multiple risks that can influence its capability to accomplish objectives. According to ISO 31000 introduction, the RM as a term refers to the architecture that is employed to control risk [10]. RA in the process of RM is only a single step.

RA is the process of defining their probability of happening and recognizing the security risks to a system, their influence, and the safeguards that would decrease that influence. The central goal of RA is to define suitable controls for diminishing or removing those risks. In general, there are four steps of RA as follow [11]:

1) Identification of Threat.

All potential threats to the system are identified in this step. It permits identifying the possible threat causes and promotes a table of a threat report that is possible threat sources that are appropriate to the system.

2) Identification of Vulnerability.

To develop a list of system vulnerabilities is the goal of vulnerability identification step (flaws or weaknesses) that could be employed by the possible threat sources.

3) Determination of Risk.

The idea of risk determination in step three is to evaluate the level of risk to the system.

4) Recommendation of Control.

Fourth step represents the aim is to suggest some commands that could lessen or cancel the identified risks, as relevant to the system organization's procedures.to to diminish the level of risk to the system is the aim of the suggested commands.

2.2 Risk analysis techniques

Risk analysis techniques are commonly classified into the qualitative or quantitative analysis:

1.2.1 Quantitative Risk Analysis (QtRA)

Quantitative risk is employed in many well-developed industries but still it is not ordinarily employed in IT. However, risk methodologies can include qualitative and quantitative as partially. It is the authors' view, however, to classify all of the primary methodologies as primarily qualitative since none of them can provide ALEs that can credibly be employed to estimate precise costs versus profits as QtRA should. They preferably afford a more general sense of benefit versus cost despite sometimes holding features that are predominantly quantitative, such as conflict statistics [12].

1.2.2 Qualitative Risk Assessments (QlRA):

It is a method that defines in detail the likelihood of consequences. This method is employed in situations where it is hard to display a numerical measure of risk. It is, for instance, the existence without sufficient data and numerical data. Such analysis can be employed as an original evaluation to identify risk [13]. The following are some of the influential RA methodologies possible today: OCTAVE [14], and MEHARI [15].

Some are openly accessible (e.g. OCTAVE), while others are limited to members of groups that are co-operating to form and updated them (e.g. SPRINT). The following are concise descriptions of each of these methodologies. OCTAVE [14] is a process of evaluation on the basis of the operating assets

of the company for threats and vulnerabilities. MEHARI [15] in the context of the security of ISs is a RA system; this system is composed to fit the requirements of every company.
These mechanisms have not been produced especially for CC environments. In common IT environments, to obtain IT related services, everybody in the business should go to the IT department. However, the RA become more complicated for CC, there are various problems that are possible appeared? Amongst them is the question of multi-tenancy that indicates the data can be placed at different geographically assigned nodes in the CC and the authority over where the processes really operated and where the data remain.

Current RA processes and standards (such as ISO/IEC 27005) are regularly concentrated on forming the various activities and steps to be conducted. Their attached value also relies on the information foundation of risks [16], [17], [18] and CC security requirements [16], [18] they demand. They are the data to the activities conducted. The methodological features are therefore commonly accurate since they form on a well-defined process and construction to be followed.

1.3 CC systems and cyber security challenges

As a new technology CC that has facilitated innovation for an increasing quantity of organizations. as part of their innovation process, It permits developing CC skills, for their services and products distribution, and diversification, also their entire organizational extension and evolution CC is an emerging paradigm of computing that substitutes computing as a private line by computing as a common benefit. It can be described as the delivery over the Internet of on-demand computing sources on a basis of pay-for-use. The resources (such as processing resources and data storage) are provisioned across the internet in a dynamic way and its subscribers are billed based on the utilization of computing resources. CC grants all the benefits of a common service system, in terms of economy of convenience flexibility, and scale but it proposes substantial problems such as the need of authority and loss of security.

However as more and more data on companies and individuals are located in the cloud, obstacles are starting to develop mainly about security. In fact, data users' externalization gets difficult to sustain data privacy and integrity as well as availability which creates serious outcomes. Security is the influential difficulty in CC systems [19], [20], [21], [22], [23], and [24]. In fact, According to a survey carried by IDG enterprise in 2014 [25] for CC, security is strongly the prime concern. In fact, up from 61% in 2014, and higher between finance groups (78%), 67% of groups have concerns regarding the security of CC clarifications. The further difficulties for decision-makers are not yet on the equivalent playing field; only 43% are regarded with integration, accompanied by the ability of CC solutions to fit enterprise standards (35%) [25]. Presented their high-security concerns, groups are integrating tools and strategies (like CC security control and its tools) to reduce these difficulties over the next months.

RELATED WORKS

1.3.1 RA for conventional system

RA has been under discussion in a different area by many types of research. In [26], Smartphone has been the main topic to be discussed in a RA method; this method represents an RA as a method is tailored for Smartphone. This kind of device is not treated by the method as a single entity. Alternatively, it recognizes Smartphone assets and affords a comprehensive list of distinctly applicable threats.

The triplet's assets that are associated with permission and threats combinations. Then, the risk is estimated as a combination of threat likelihood and asset influence. The method employs user data, with regard to influence estimate, joined with statistics calculation of threat likelihood. In [27], the present paper offers a method for a probabilistic model run conditions of RA on security. The normal relations of security conditions are described employing MEBN logic that forms a specific and clear formal RA model that carries evidence-driven arguments.

There are a number of methods for QtRA exist. In [28], they offer a cost-benefit analysis process as a kind of SAEM method which is for interpreting security design determinations based on the observation of a "threat index". Nevertheless, it is an theoretical opinions. In [29] they offer security ontology for coordinating information on assets and threats. This activity generates a method for QtRA and forms classification for every one of these groups, employing its own framework. The work does not employ recognized guidelines or standards as an input for its evaluation model, so wanted tools and countermeasures have to be determined in the process of risk analysis. QtRA conditions are reflecting in [30] uses PACT as a "filter" organized in series to discover a proportion of the impact of the risk factor or likelihood. Still, it lacks the capability to express the consequences of various risk factors. The SSRAM framework in [31] affords a prioritization that assists in defining how the risks recognized will be discussed in various stages of software improvement. Anyway, it lacks a baseline for systematically recognizing possible reasoning and risks about their interactions and relationships in a true operational situation.

In [32], a new method is suggested, in which AHP that stands for (Analytic Hierarchy Process) can be merged with some varieties, is shown. The method involves; firstly, the analytic structure of the RA is formed and the method of PSO broad judgment is adjusted according to the exact provision of the data security. Secondly, the risk level placed ahead is PSO view of the risk possibility, the risk consequence cruelty, and risk uncontrollability. Finally, it contributes examples to confirm that this method Multi MOPM can be suitably utilized to security RA and for establishing the risk control strategy of the IS security it presents thoughtful data.

2.4.2 RA for CC

The practices and principles of risk assessment In recent years were included into the field of utility computing like Clouds either as a focus on a particular sort of risk, like security problems [33] or as a general methodology [34][35][36][37][38][39].

RA reports of CC was released by ENISA, it pointed out the security risks and benefits in CC, afforded some possible suggestions and outlined a collection of assurance standards to evaluate the risk of choosing CC services [40] [41]. In [42], a QtRA model based on NIST [33] (QUIRC) is given to evaluate the associated 6-keyss security risks sections of security goals in a CC (i.e., availability, mutual audit ability, multi- party trust, usability, integrity, and confidentiality). The quantitative definition of risk is introduced as an output of the possibility of a security agreement, i.e., an occurring threat situation, and its possible consequence or influence. for the assigned application The entire platform security risk is under a provided security purposes category can be the average across the cumulative, the sum of n threats that map to that security purposes category. In addition, a weight that outlines the significance of a provided security purposes to a distinct organization vertical is similarly required and their sum continually adds up to 1.

This model uses an extended band Delphi technique [43], employing rankings built upon expert opinion regarding the consequence and the likelihood of threats, as scientific ways to assemble the data needed for evaluating security risks. The benefit of this QtRA is that it permits CC and CSPs consumers as well as the regulation agencies the capability to comparatively assess the corresponding robustness of several CC vendor contributions and suggestions in a defensible way. However, the difficulty and challenge of applying this approach is the accurate set of historical data for threat events probability calculation, to be evaluated CC platforms and their vendors it demands data input from those. The same efforts were done in [44].

In [45], from the perspective of a CC in a risk analysis approach, the user is offered to analyze the risks of data security before placing into a CC environment his confidential data. The central goals of this work are to assist CSPs to guarantee their customers about the approach and data security can also be employed by users of cloud service to conduct a risk analysis before placing their significant data in a security sensitive CC. trust matrix is the base for this approach. There is a need for approaches to structured analysis that can be employed for risk analysis in CC.

In [46], an SEBCRA method that is knowledgeable of the Business-Level Objectives (BLO) of a presented CC group is given. The method is designed for a CSP to promote the fulfillment of a BLO, i.e., advantage maximization, by maintaining, treating CC risks and evaluating. The center idea on which this method is based is that "Risk Level Evaluation for each BLO is equivalent to the possibility of a presented risk also its influence on the BLO in question". as soon as risk has been estimated, the Risk Treatment sub-process determines possible risk-aware procedures, policies and controls to carry an suitable risk reduction procedures, such as, bypass the risk, by removing its cause(s), decrease the risk by holding measures to cut down its possibility, its influence, or both, accept the risk and its associated outcomes or delegate or transfer the risk to outside groups. In a worthy experimentation, the RA method confirms that it permits a CSP to maximize its advantage by carrying risks of provisioning its individual Cloud to 3rd party providers of CC infrastructure. This RA method can be enlarged and promoted to serve as an autonomic risk-aware program also to tackle situations where various BLOs are determined by a CSP, which will be based on heuristics and business-driven management that assist the CSP in developing its reliability.

In [47], RA as a service based on a cloud is suggested as an encouraging alternative. CC offers various features that challenge the effectiveness of modern evaluation approaches. In particular, the multi-tenant nature and on-demand, automated, of CC is at differences with the static, individual process-oriented character of the systems for which representative evaluations were composed. Still, the autonomic RA is in distant from the light, since the RA is a difficult task to accomplish. In [48], a framework described and named as SecAgreement (SecAg) is shown, that enlarges the negotiation of the current SLA, WS-Agreement, to enable security metrics to be displayed in service classification service level objectives and terms. CSPs is enabled by the framework to incorporate security in their SLA contributions, raising the likelihood that their services will be employed. We represent and illustrate a CC service matchmaking algorithm to rank and assess SecAg improved WS-Agreements by their risk, enabling groups to quantify risk, recognize any gaps of policy agreement that might exist, and as a conclusion choose the CC services that best satisfy their security demands.

In [49], they offer a methodology for conducting security RA for CC architectures in deferent degrees basing on commands of Bayesian dependencies. The central purpose of the present paper is to demonstrate how to estimate the relative risk (RR).

In [50], for the security policies and lists the similar circumstances the present paper sums up eight sorts of threats. Searching with virtualization and collaborative of CC technology and so on, using AHP theory and presenting the correlation coefficient to analyze the various objective decisions, the paper proposes a new information security RA model based on AHP in CC. Therefore, the purpose of this paper is to prepare the security RA procedures of the data system in the CC.

INFORMATION SECURITY RA MODELS

In this section, we present for CC system the fundamental security RA models. Actually, these models quantify the security of a computing system by a stochastic variable that describes for every stakeholder, the quantity of loss that occurs from system vulnerabilities and security threats. We offer forward five models for CC system. To quantify security violations.

3.1 Sec Agreement

In [18], Hale et al. showed a model under the name (SecAgreement) to allow CSPs to involve growing the possibility that their services will be employed. The method determines a cloud service matchmaking algorithm to estimate and value SecAg heightened SLA by their risk, enabling groups to quantify risk, recognize any policy agreement gaps that possibly exist, and consequently pick the cloud services that best fit their security requirements.

3.2 The Mean Failure Cost (MFC)

A security metric called MFC introduced by Ben Aissa et al., in [17], its purpose is to quantify the security of a CC system by the statistical tools of the stochastic variable that outlines for each stakeholder, the quantity of loss that occurs from system vulnerabilities and threats of security. The MFC changes by stakeholder and considers the variety of the stakes that a stakeholder has in fitting each security condition. The infrastructure in question reveals the advantages that stakeholders possess in every security provision, the dependency of security conditions on the development of architectural elements and the influence that security threats possess on these elements.

This matrix defines which threats change which elements and evaluate the possibility of success of every threat in light of perpetrator performance and potential counter-measures. Generation of the threat vector: it describes the possibility that a threat grows during the unitary time of operation.

3.3 MFCext and MFCint

A new model for quantifying security threats risks was proposed by Jouini et al. in [7] by viewing an order of the recognized threats: the MFCext and MFCint. In fact, in order to know the source of threats, threats are classified using their sources shared data systems and particularly the CC systems to evolve suitable strategies to stop or lessen their influences. Using threat sources dimensions as a base in order to manage threats sources. According to a model of two dimensions named External and Internal, the security threat for the model is interference is partitioned into subspaces.

3.4 The MFC Extension model (MFCE)

A new security metric for IS and for CC environment especially is suggested by Jouini et al, in [5], the MFCE. The model has relied on an order model named as the Hybrid threat Classification (HTC) and introduced in [9]. The HTC is the generic model that attaches criteria of several characteristics or threats or like intent, threat source, motives, threat perpetrators and threats consequences.

The focus of The MFCE model is on perfecting the evaluation of the influence matrix IM and the vector PT of the (MFC) proposed before. This model permits investigating the influence of an entire class of threats rather than an insignificant threat. In fact, in terms of time, threats are variable and security clarifications vary over time.For the IM, it was produced two new matrices: the IM and the CM.

3.5 Multi-dimensional Mean Failure Cost Model (M2FC)

Jouini et al. suggest, in [10], select the approach of multi-dimensional to evaluating security threats. They suggest a novel model for evaluating the failure cost of an IS security that regard threats dimensions to adequately evaluate threats risks. The model named M2FC and reflected that the threat world is split into various threats views each possessing different orthogonal dimensions. In fact, every security threat shows various features, described as perspectives, which raise the risk level faced by a system. These perspectives are able to divide this space into many parts named as dimensions.

For decomposition object, the model holds a head dimension in the threat world to permit concentrating more on one dimension than the rest of the dimensions. For instance, to evaluate failure cost of the dimensions per architectural elements regards we determine the elements dimension as the leading one. In other circumstances, we would like to concentrate not on elements only on deployment position of the enterprise, next we will surely have the mean failure cost per area. Its considerable takes into account in the M2FC model the stakeholders' evaluation of the cost associated with their demands with regard to the components of two dimensions.

COMPARATIVE ANALYSIS

To compare in larger detail the three distinct methods is the purpose of the study of the four QtRA models for CC systems also to present advantages and limits for every model. The model of SecAgreement is a quantitative approach that is employed to distinguish between CSPs to choose the best one depending on the estimate of the risk factor of every one plus do not assess risks according to security violations for the environment of CC.

Several advantages are arising from The MFC. Additionally, in financial terms, it quantifies the system security, particularly, in a case of how much every stakeholder in the system stands to lose as a consequence of security system vulnerabilities and threats. Indeed, this metric alters in relation to the stakes that every stakeholder has in fitting every security demand. However, it displays certain deficiencies. After investigating and analyzing the MFC metric and security threats, we noticed the following MFC limits:

- Security threats over time are variable and evaluative and have various features, and there is the hierarchical structure or no logical in PT vector among the several cataloged threats as they are not based on a distinct characteristic to distinguish them.
- Underestimation of the MFC: the term employed to describe the ambiguous threat in the PT, this can drive to a projection between the different threats i.e. each threat may refer to different sources at once and therefore it is counted multiple times, so we have an underestimation of the mean failure cost.
- This method when used by users to derive threats may have totally different outcomes.
- The source of threats risks cannot identify by the Managers in order to recommend suitable countermeasures.
- Toward the structure of security threats, The MFC is considered blind. It supposes that any failure because of a threat is a failure with regard to the entire specification. Yet stakeholders can possess several stakes in various security threats perspectives and dimensions which are not indicated in the MFC.

The MFCint and The MFCext present the crucial threats range to support managers to select the proper countermeasures. They promote the analysis of the system vulnerability. They define the sort of solution to decrease the normal value of failure. In fact, employing the threat analysis source dimension, they enable classifying the origin of the threats range to let managers focus on the intervention range producing the larger mean failure costs. Nevertheless, it does not take into account all threats features and just count one standard which does not correctly report a threat (like the source), therefore in security failure, they do not present true measure on the cost. In addition, the estimated criteria (source) are based on a binary order while threat sources may involve 3 subclasses.

On the basis of a threats classification model, The MFCE considers threat classification and enables providing a threat clarification by section, the present model does not express the cost depending on the dimensions of security threats. Moreover, we showed out that the adopted threats model of classification is not full model in the manner of size. Furthermore, if managers desire to identify critical measures or dimension that affects the cost consequences of security failure, they cannot define them employing these models. Therefore we need to generate a metric that correctly evaluates security violations and provides significant dimension to adequately control security policies in groups. Accordingly, if the decisions makers require possessing critical criteria or dimensions that affect procedures of the cost of security failure, they are unable to determinate them utilizing these models.

Eventually, this M2FC is an enhancement of the MFC 17. This model alters by stakeholder and takes into account the variance of the stakes that a stakeholder has in fitting every security demand still it does not take into account threat dimensions and perspectives. Furthermore, this it views as a multi-dimensional presence as a threat includes many dimensions, to reduce the security it takes into account threats perspectives risk to every system and it considers variations in systems like differences in the deployment, elements, and variations in user admittance policies. Therefore, it takes into account threats dimensions features and enables recognizing significant dimensions that cause the highest costs.

CONCLUSION

Regarding risk assessment, Cloud computing poses new challenges. These involve the estimation of a dynamic environment, in accordance with loose edges, as well as an unfamiliar risk profile that is influenced by different threats and opponents and arises from varied locations (e.g., co-tenants, the provider, the technology itself, etc.). Such estimates include a level of confidence on the concept that different, alternating third parties will present secure services.

Risk evaluation is a fundamental tool in the wheel of Data Management of Security. It is necessary for enterprises to utilize a well-structured and systematic process for evaluating data security risks to its assets. The foremost goal of the study is to compare, review and quantitative model of a security risk for Cloud Computing systems because these systems serve a possibility technology for firms that improve organizations' brand also decrease cost. The outcomes will end with a comparison that benefits decisions makers to choose the proper models to evaluate security risks for CC situation and indeed for other data systems. In fact, it serves to assess the models' applicability to a group and their precise needs.

REFERENCES

[1] A. J. Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, A. Ali Eldin, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S. K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C. Sheridan, "Optimis: A holistic approach to cloud service provisioning," Future Generation Computer Systems, vol. 28, no. 1, pp. 66 – 77, 2012.

[2] K. Djemame, I. Gourlay, J. Padgett, K. Voss, and O. Kao, Market-Oriented Grid Computing, R. Buyya and K. Bubendorfer (Eds.). Wiley, 2009, ch. Risk Management in Grids.

[3] X. Zhang, N.Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology, ser. CIT '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 1328–1334.

[4] J. O. Fit ´o and J. Guitart, "Business-driven management of infrastructure-level risks in cloud providers," Future Generation Computer Systems, vol. 32, pp. 41–53, Mar. 2014.

[5] P. Saripalli and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, ser. CLOUD '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 280–288.

[6] K. Djemame, J. Padgett, I. Gourlay, and D. Armstrong, "Brokering of risk-aware service level agreements in grids," Concurrency and Computation: Practice and Experience, vol. 23, no. 7, 2011.

[7] Mell P, Grance T. Perspectives on cloud computing and standards. National Institute of Standards and Technology (NIST). Information Technology Laboratory; 2009.

[8] CSS, White paper on software and service architectures, Infrastructures and Engineering – Action Paper on the area for the future EU competitiveness Volume 2.

[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, vol. 19, pp. 310–319, 2010.

[11] ISO 31000:2009, Risk management—Principles and guidelines

[12] Vishal Visintine, "An Introduction to Information Risk Assessment", GSEC Practical, Version 1.4b, August 8, 2003

[13] Harms-Ringdahl, L. (2001) Safety analysis: Principles and practice in occupational safety. CRC Press.

[14] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute, Juin 1999.

[15] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.

[16] DCSSI (2004). EBIOS – Expression of Needs and Identification of Security Objectives. http://www.ssi.gouv.fr/en/condence/ebiospresentation.html, France.

[17] ISO/IEC 27005 (2008). Information technology -Security techniques - Information security risk management. International Organization for Standardization, Geneva.

[18] ISO/IEC 27001 (2005). Information technology -Security techniques - Information security management systems - Requirements. International Organization for Standardization, Geneva.

[19] Jouini M, Ben Arfa Rabai L, A Security Risk Management Metric For Cloud Computing Systems, International Journal of Organizational and Collective Intelligence (IJOCI) 2014;4(3): 1-21.

[20] Jouini M, Ben Arfa Rabai L. Surveying and Analyzing Security Problems in Cloud Computing Environments, The 10th International Conference on Computational Intelligence and Security (CIS 2014); 2014. p. 689-493.

[21] Jouini M, Ben Arfa Rabai L. Mean Failure Cost Extension Model Towards A Security Threats Assessment: A Cloud Computing Case Study, Journal of Computers (JCP) 2015;10(3):184-194.

[22] Saripalli, P., & Walters, B. QUIRC: A quantitative impact and risk assessment framework for cloud security. Proceedings of the IEEE 3rd International Conference on Cloud Computing 2009, 280–288.

[23] Jouini M, Ben Arfa Rabai L, Ben Aissa A, Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2012;1(3):265-279.

[24] Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A. A cybersecurity model in cloud computing environments, Journal of King Saud University - Computer and Information Sciences; 2013.

[25] IDG Cloud Computing Survey, Cloud Continues to Transform Business Landscape as CIOs Explore New Areas for Hosting, http://www.idgenterprise.com/news/press-release/cloud-continues-to-transform-business-landscape-as-cios-explore-new-areas-for-hosting, 2014.

[26] Theoharidou, M., Mylonas, A., Gritzalis, D.: A risk assessment method for smartphones. In: Proc. of 27th IFIP Information Security and Privacy Conference, pp. 428-440 (2012)

[27] 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, pp. 1328-1334.

[28] Butler, S.A., Security Attribute Evaluation Method: A Cost-Benefit Approach, (2002), 232.

[29] Ekelhart, Fenz, Klemen and Weippl, Security Ontologies: Improving Quantitative Risk Analysis, (2007), 156a.

[30] Feather, M. and Cornford, S. Quantitative risk-based requirements reasoning. Requirements Engineering, 8 (4),pp. 248-265.

[31] Mkpong-Ruffin, I., Umphress, D., Hamilton, J. and Gilbert, J. Quantitative software security risk assessment model , ACM workshop on Quality of protection, Alexandria, Virginia, USA, 2007.

[32] Gamal A. Awad, Elrasheed I. Sultan Noraziah Ahmad, N. Ithnan, "Multi-objectives model to process security risk assessment based on AHP-PSO" ,Modern Applied Science Vol. 5, No. 3; June 2011

[33] J. A. Zachman, A Framework for information systems architecture,IBM Systems Journal, Vol 26. No 3, 1987

[34] A. Morali and R. J. Wieringa, Risk-based confidentiality requirements specification for outsourced IT systems, pp. 199-208, Proceedings of the 18th IEEE International Requirements Engineering Conference, 2010, DOI 10.1109/RE.2010.30 148 | P a g e www.ijacsa.thesai.org

[35] C. S. Yeo and R. Buyya, Integrated risk analysis for a commercial computing service in utility Computing, Journal of Grid Computing, Vol 7,No.1,pp.1-24,ISSN:1570-7873,Springer,Germany,March 2009

[36] Min Luo, Liang-Jie Zhang and Fengyun Lei, An Insurance Model for Guaranteeing Service Assurance, Integrity and QoS in Cloud Computing, pp. 584-591, Proceedings of 2010 IEEE International Conference on Web Services, DOI 10.1109/ICWS.2010.113

[37] J. Oriol Fitó, Mario Ma_as and Jordi Guitart, Towards Business driven Risk Management for Cloud Computing, pp. 238-241, Proceedings of 2010 Int. Conf. on Network and Service Management

[38] A. Juan Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R.M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S.K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C. Sheridan, OPTIMIS: a Holistic

Approach to Cloud Service Provisioning, Future Generation Computer Systems, 2011,DOI: 10.1016/j.future.2011.05.022

[39] G. Tucker, and C. Li, "Cloud Computing Risks," Proceedings on the International Conference on Internet Computing, 2012.

[40] Catteddu, D., Hogben, G.: ENISA Cloud Computing Risk Assessment. ENISA (2009)

[41] Catteddu, D., Hogben, G.: Cloud Computing Information Assurance Framework. ENISA (2009)

[42] 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, pp. 280-288, 2010

[43] H. A. Linstone, The Delphi Method: Techniques and Applications. Addison-Wesley, 1975.

[44] W. Hsu, "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective," IEEE Technology and Engineering Education, 2012.

[45] 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 2010), Bangkok, Thailand

[46] J. Oriol Fitó, Mario Ma_as and Jordi Guitart, Towards Business driven Risk Management for Cloud Computing, pp. 238-241, Proceedings of 2010 Int. Conf. on Network and Service Management

[47] Burton S. Kaliski Jr. and Wayne Pauley "Toward Risk Assessment as a Service in Cloud Environments," EMC Corporation, Hopkinton, MA, USA 2010

[48] M. Hale, and R. Gamble, "SecAgreement: Advancing Security Risk Calculations in Cloud Services," 8th IEEE World Congress on Services, 2012.

[49] Afnan Ullah K, Manuel O, Mariam K, Ming J, Karim D."Security risks and their management in Cloud Computing". 2012 IEEE 4th International Conference on Cloud Computing Technology and Science

[50] Peiyu L., Dong L., 2011. "The New risk assessment model for information system in Cloud Computing environment", Procedia Engineering 15, pp. 3200 – 3204

[51] Hale, M., & Gamble, R. SecAgreement: Advancing security risk calculations in cloud services. Proceedings of 8th IEEE World Congress on Services, 2012.

[52] Ben Aissa A, Abercrombie RK, Sheldon FT, and Mili A. Quantifying security threats and their potential impact: a case study. Innovation in systems and software engineering 2010;6 (1):269–281.

[53] Jouini M, Ben Arfa Rabai L, Ben Aissa A, Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2012;1(3):265-279.

[54] Jouini M, Ben Arfa Rabai L. Mean Failure Cost Extension Model Towards A Security Threats Assessment: A Cloud Computing Case Study, Journal of Computers (JCP) 2015;10 (3):184-194.

[55] Jouini M, Ben Arfa Rabai L, Ben Aissa A. Classification of security threats in information systems, ANT/SEIT 2014 2014:(32)489-496.

[56] Jouini M, Ben Arfa Rabai L, Khedri R. A Multidimensional Approach Towards a Quantitative Assessment of Security Threats, ANT/SEIT 2015 2015, 507-514.