Cloud Computing Security Risk Assessment: A Survey

Ishraga Khogali,

Sudan University of Science and Technology,

Khartoum, Sudan

Eshragakhogali@yahoo.com

Abstract

Cloud computing is a new computing technology which has attracted much attention. Unfortunately, it is a risk prone technology since users are sharing remote computing resources, data is held remotely, and clients lack of control over data. Therefore, assessing security risk of cloud is important to establish trust and to increase the level of confidence of cloud service consumers and provide cost effective and reliable service and infrastructure of cloud providers. This paper provides a survey on the state of the art research on risk assessment in the cloud environment.

Keywords — cloud computing security, risk assessment, impact, and likelihood

1. Introduction

Cloud computing is a new technology that provide real promise to business with real advantages in term of cost and computational power. The National Institute of Standards and Technology(NIST) defines cloud computing as ‘‘a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction’’[1].

In general, the idea of handing over important data to another company is worrisome such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment [6]. However, it's important to consider security and data protection when it comes to widespread cloud adoption [7] because cloud computing raises severe security concerns that existing in traditional system as well as issues that appear to be specific to that domain. Although most of these concerns are not new, already exist in traditional IT environment, they need more consideration because of the dynamic nature of cloud computing platform. Therefore, before utilizing cloud-services, organizations should ensure that they understand the security and privacy risks in the cloud environment and their security and privacy requirements based on their business requirements are satisfied [8]. So, in spite of the advancement in cloud technologies and increasing number of cloud users, Cloud computing encompasses new technologies such as virtualization and there are both new risks to be determined and old risks to be re-evaluated and mitigated [14].

The process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact called Security risk assessment [1]. It is aimed at examining possible threats, vulnerabilities, the likelihood and impact of them [12] to define appropriate controls for reducing or eliminating the risks [1]. Moreover, there are Dynamic risk assessment where frequent updates of risk evaluation information are used to evaluate risk exposure, as close as possible to real-time [13].

Risk assessments provide significant value in increasing trust and thus appear particularly beneficial to the adoption of cloud computing [17]. Furthermore

Therefore, the traditional assessments developed for conventional IT environments do not readily fit the dynamic nature of clouds. Hence, the introduction of cloud specific security assessment methodology has significant importance and scope. Recently, several studies have been conducted to improve traditional security assessment techniques and present new paradigms for analyzing and evaluating security risks in cloud environment. However, security assessment in cloud is still challenging domain and a growing area of research [12].

In general, there are three categories for risk assessment methods: quantitative, qualitative and semi-quantitative (or hybrid). Quantitative risk assessments, which provide accurate measurements of impacts' magnitude but involve calculations that are

tedious and include a strong element of arbitrariness, moreover these quantitative impacts may be unclear, thus requiring to be interpretd in a qualitative way. In another hand, the qualitative assessments that do not provide enough quantifiable measurements concerning probabilities and impacts of risks but prioritize risks and identify the most important areas for improvement. As a result, semi-quantitative risk assessments replace very well tedious quantitative approaches, and incomplete qualitative methods [14].

This paper organized as follows: section 1 is the introduction; Section 2 is a literature review, Section 3 open issues and section 4 a conclusion.

2. Literature Review

In this review, we introduce in section 2.1 the related work, section 2.2. A classification of cloud-based security risk assessment methods and tools and section 2.3 discusses the open issues directions.

2.1 Related work

2.1.1 Towards Analyzing Data Security Risks in Cloud Computing Environments

In [16] Amit Sangroya et al. (2010) present the advantages and disadvantages (in the context of data security) of using a cloud environment. They also investigate the security mechanisms that are used by major service providers. Their study supports that in the context of data security trust is a major element, which is missing in the currently existing computing models. In order to build a better trust mechanism between the cloud service provider and users, they present a risk analysis approach that can be primarily used by the perspective cloud users before putting their confidential data into a cloud. Their approach is based on the idea of trust model, principally used in distributed information systems. They extend the general idea of trust management and present its use in analyzing the data security risks in cloud computing. They build a trust matrix to analyze the data risk. To build the trust matrix, a number of heuristics can be used for selecting the security parameters. They select data cost and provider's history as trust variables to build the trust matrix. However, other variables can also be used for building the trust matrix such as Service Cost, Monitoring support etc.

Along with trust variables, few parameters used in measuring trust can be applied to fine-tune these trust variables. The parameter, which they choose in this category, are

Data Location such that data located at the sites, which are geographically or politically sensitive, would likely to have lower trust than other locations.

Fig.3 represents an example trust matrix with area representing the Low Risk/High Trust zone and, High Risk/Low Trust zone where x-axis represents the data cost, y-axis represents the service provider's history and z-axis represents the data location.

The variables have been defined in this method can be used where there are some past statistics about the service provider. The method has been used to measure the trust and will be used for all future transactions. Based on this method, we were able to define the trust actions, for all future transactions with the service provider.

The most obvious finding to emerge from this study is that, there is a need of better trust management framework and there is a lack of structured analysis approaches that can be used for risk analysis in cloud computing environments. The approach suggested in [16] is a first step towards analyzing data security risks it is easily adaptable for automation of risk analysis.

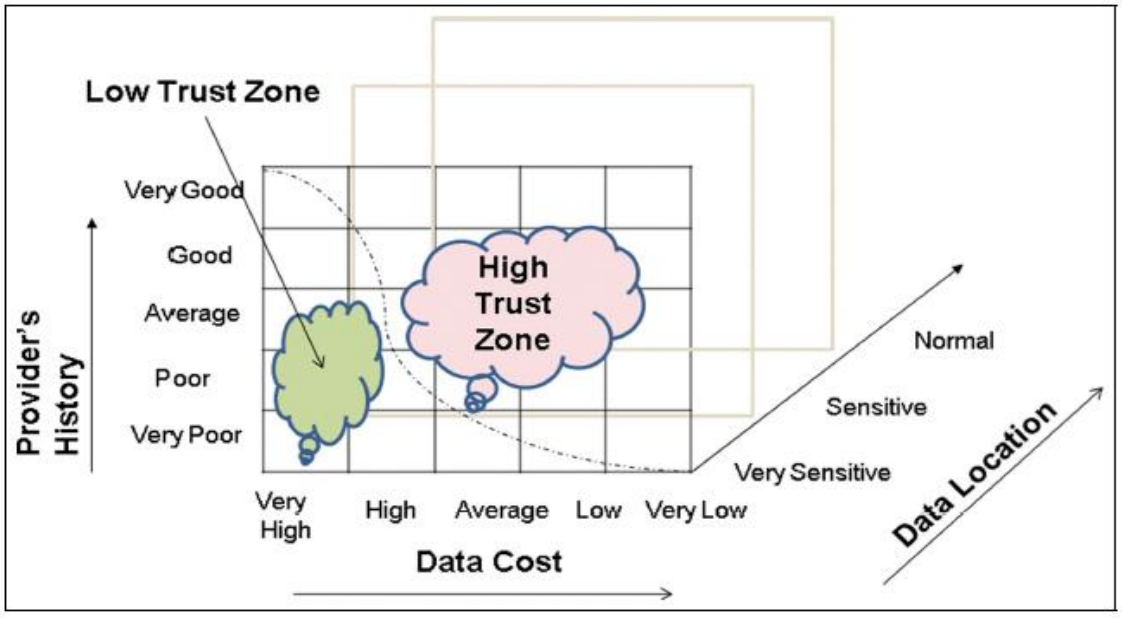

Fig. 3. A Trust Matrix for Risk Analysis [16]

2.1.2 Information Security Risk Management Framework for the Cloud Computing Environments

Xuan Zhang et al. (2010) in [18] present information risk management framework that provide better understanding for critical areas of focus in cloud computing environment, to identifying a threat and identifying vulnerability. It is covering all of cloud service models and cloud deployment models. Cloud provider can be applied this

framework to organizations to do risk mitigation. This framework was developed in a standard quality management (or Plan, Do, Check, Act) cycle of continuous improvement. The framework was to describe critical areas of focus in cloud computing that should be protect and designed to protect the confidentiality, integrity and availability of information assets. The framework have seven processes, including: processes-selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. Where Risk assessment is the determination of quantitative or qualitative an output from risk analysis process. This step have four major processes:

- Likelihood Determination: To derive an overall likelihood rating that indicates the probability vulnerability may be exercised within the construct of the associated threat environment. The likelihood that a potential vulnerability could be exercised by a given threat-source can be describe as high, medium, low. The output from likelihood determination step is likelihood rating.
- Impact Analysis: The step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or combination of any, of the following three security goals: integrity, availability, and confidentiality that can be describes qualitative categories as high, medium, low [18].
- Risk Determination: The purpose of this step is to find the risks and opportunities that impact of critical area's risk that selected in Selecting Critical Area step. They use sample matrix to shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level [18].

This risk scale, with its rating of High, Medium, and Low, represents the degree of level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level. Output from this step is risk level (High, Medium, or Low).

- Control Recommendations. - During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operation

provided. The goal of the recommend controls is to reduce the level of risk to cloud computing environment and its data to an acceptable level [18].

However, the risk assessment in this paper is not quantitative.

2.1.3 QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security

Prasad Saripalli et al. (2010) in [19] present a Quantitative risk and impact assessment framework (QUIRC), to assess the security risks associated with cloud computing platforms. This come in response to the U. S. Federal Information Security Management Act (FISMA) of 2002, where the Federal Information Processing Standards (FIPS) proposed confidentiality, integrity, availability, authenticity and accountability as the key principles of information security.

They propose six Security Objectives: three security objectives for information and information systems (Confidentiality, Integrity and Availability), three requirements unique to cloud platforms (multi-party trust considerations, mutual auditability and Usability). These six Security Objectives for the cloud platforms may be referred to as the CIAMAU framework [19].

STRIDE may be considered an alternative to the Security Objectives based CIAMAU categorization. For the purposes of QUIRC analysis, any categorization is sufficient. QUIRC methodology would work with any framework, by assigning relative weights of importance to each SO category [19].

They define a risk as a product of the Probability (*Pe*) of a security compromise, i.e. a threat event, *e*, occurring and its potential Impact or Consequence (*Ie*) [19]:

$$R_e = P_e I_e$$

Pe typically is a fraction less than one, whereas *Ie* may be assigned a value on a numerical scale. They propose these ranges for Impact (*Ie*): LOW (1-5); MODERATE (6-10); HIGH (11-15). These values are relative, and may be amplified depending on the required granularity for the visualization of risk metrics [19].

Security risk under each CIAMAU category is assessed, and the overall platform security risk for the given application under a given category (*Rs*) would be average over the cumulative, weighted sum of *n* threats that map to that SO category [19]:

$$R_s = \frac{1}{n} \sum_{i=1}^{n} P_e I_e$$

It is also necessary to assign a weight for each of the SO categories, such that their sum always adds up to 1. This weight, *ws*, represents the relative importance of a given SO to a particular organization and/or business vertical. Then, Net Security Risk (R) to the application integrated over the six CIAMAU objectives is a weighted average:

$$R = \sum_{s=1}^{6} w_s R_s$$

where ws is the relative weight assigned to an SO category s. Evaluation of the probabilities of several threat events currently is difficult, due to a lack of historic data.

Advantages of the QUIRC methodology are as follows. A quantitative approach gives vendors, customers and regulation agencies the ability to comparatively assess the relative robustness of different cloud vendor offerings and approaches in a defensible manner. It also can be helpful in alleviating the considerable FUD (Fear, Uncertainty and Doubt) associated with cloud platform security issues and helping that they are dealing in an effective way [19].

However, Limitations of the approach include that it requires the meticulous collection of input data for Probabilities of events, which requires collective industry SME inputs [19]. Moreover, this framework does not cover risks during all the stages of the lifecycle of the service when it exists on the cloud [4]. A fully quantitative risk assessment framework would further improve this methodology. In general, there is lack of structured analysis approaches that can be uses for risk analysis in cloud computing environments [1].

2.1.4 Security Risks and their Management in Cloud Computing

Afnan Ullah et al. (2012) in [20] propose a methodology for performing security risk assessment for cloud computing architectures presenting some of the initial results. They consider the deployment and operation stages in the cloud lifecycle. Deployment stage where the initial placement of services on cloud providers, and the service operation stage where cloud resources and data managed by the cloud provider to fulfill the Service Level Objectives.

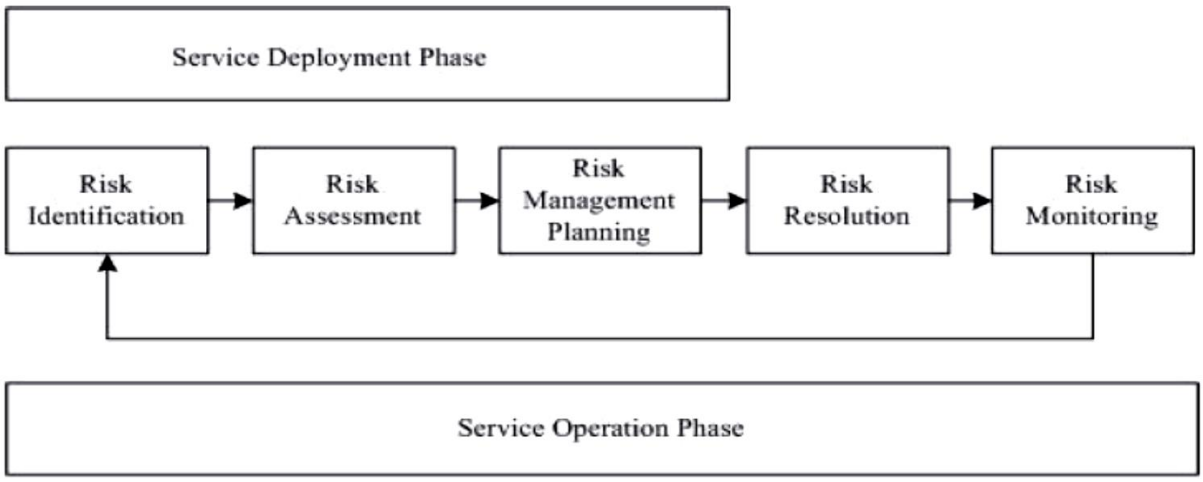

Fig. 4 Risk assessment lifecycle during service deployment/operation [20]

A number of stages have identified for performing a complete risk assessment on clouds by considering core risk assessment approaches as explained below [20]:

A. High level analysis of the system

An initial high-level analysis of the deployment scenarios helps identifying the actions and assets involved at the different stages in the cloud [20].

B. Identifying the assets involved

There are various assets involved either at the deployment or operation stage such as the SLA or customer data. These can be monitor in relation to the specific threats in the environment [20].

C. Identify the threats in each cloud deployment scenario

In which threats and vulnerabilities of a system can be identified. To do this they coupled information risk analysis methodology with the threat and vulnerability assessment tool (T&VA) which provides a standard list of threats relating to IT systems, then adopting the threats relevant to the cloud deployment scenarios being investigated. In addition to other threats that have been added to introduce the differences between cloud computing and other forms of distributed computing [20].

D. High-level analysis of each threat

Each of the threats can be further analyzed in terms of who causes them and the incidents leading up to them, which can then prioritized depending on this information [20].

E. Risk Evaluation

Depending on the priority of the assets and likelihoods of the threats occurring, the threat items can be plotted into an evaluation matrix to document their occurrences [20].

F. Risk Treatment

Once evaluated, the risk mitigation strategies can be generated in terms of the actions taken to resolve them. These can be to accept, treat or outsource the risk.

At the deployment stage, the risk assessment tool will read inputs from the risk inventory, which documents all the threats, the vulnerabilities, assets affected and their likelihoods. Based on rules of Bayesian dependencies, the probability of each threat affecting the particular assets can be calculate before making the decision to accept the service by the IP [20].

However, at the operation stage, along with the calculated security risk for this stage, the risk assessment tool will be interacting with the monitoring database and additional tools like the network and historical database to monitor if certain threats are becoming live [20].

However, Afnan Ullah et al. [20] consider the three security requirement for information systems (Confidentiality, Integrity and Availability), but they do not consider other security requirements that unique to cloud platforms such as (multi-party trust considerations, mutual auditability and Usability).

Further future work includes testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur. This will then be extended to work on determine threats which may be eventually seen based on the data being collected and difficult to determine directly from the events [20].

2.1.5 Toward Risk Assessment as a Service in Cloud Environments

Burton S. Kaliski et al. (2010) in [17] introducing risk assessment as a service. Risk assessment as a service is a new paradigm for measuring risk as an autonomic method that follows the on-demand, automated, multi-tenant architecture of the cloud – a way to get a continuous "risk score" of the cloud environment with respect to a given tenant, a specific application, or more generally, for use by new tenants and applications [17].

They proposed a cloud-based *assessment as a service* paradigm as a promising alternative. However, they didn't implement such a service but rather offer it as a paradigm to be followed [17]. As well as they don't suggest method to calculate risk score.

Table 10: Summary of the related works.

Lit. Ref	Context of Research	Technique Used	Problems	Model/ Tool/ Proposed
16	Risk analysis approach that can be primarily used by the perspective cloud users.	Build a trust matrix to analyze the data risk.	The variables have been defined in this method can be used where there are some past statistics about the service provider. A lack of structured analysis approaches that can be used for risk analysis in cloud computing environments.	Better trust management framework.
18	Information risk management framework	The Risk assessment step have four major processes (Likelihood Determination, Impact Analysis, Risk Determination according to Risk Scale, and Control Recommendations).	Risk assessment in this paper is not quantitative.	-
19	Quantitative risk and impact assessment framework (QUIRC)	Security risk under each Security Objective category would be average over the cumulative, weighted sum of n threats that map to that SO category and assign a weight for each of the SO categories. Then, Net Security Risk (R) to the application integrated over the SO is a weighted average.	This framework requires the careful collection of input data for Probabilities of events [19]. Moreover, it does not cover risks during all the stages of the cloud lifecycle [4].	A fully quantitative risk assessment framework would further improve this methodology [1].

20	Methodology for performing security risk assessment for cloud computing architectures.	A number of stages have identified for performing a complete risk assessment (High level analysis of the system, Identifying the assets involved, Identify the threats in each cloud deployment scenario, High-level analysis of each threat, Risk Evaluation using evaluation matrix, and Risk Treatment).	They consider the three security requirement for information systems but they do not consider other security requirements that unique to cloud platforms.	Testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur.
17	Risk assessment as a service	It is a paradigm to be followed.	No implementation as well as there are no method suggested to calculate risk score.	The dynamic assessment service

2.2 A Classification of Cloud-based Security Risk Assessment Methods and Tools

Fatimah M. Alturkistani et al. [12] present a classification of cloud-based security risk assessment methods and tools as follow:

1) **Risk assessment as a service**: It is available in real-time by one or more of the entities in the cloud [21].

2) **Qualitative and quantitative assessment:** Risk assessment have analyzed security risk by using qualitative or/and quantitative approach. In the research article by Peiyu, et al. [22] an integrated method of qualitative and quantitative analysis used to build the assessment model in cloud.

3) **Graphs analysis assessment**: Graphs and mathematical models can be used to address and calculate security risk in clouds by simulating attacker possibilities. Leitold, et al. [23] have presented a mathematical model for threats that considers communication in order to identify security risk for individual entities, and then calculates it for a whole enterprise. The model built by representing communications as a directed graph and then established a matrix to discover the risk before finally making a simulation. Furthermore, in another study, Tanimoto, Hiramoto, Iwashita, Sato and Kanai [24] have used a hybrid risk-analysis method based on decision tree analysis (quantities) and risk matrix (qualitative).

4) **Hierarchal assessment:** Jijun, et al. [25] built a hierarchical framework to analyze the risk and set the goal for the assessment. In addition, another assessment method has been introduced based on an Analytic Hierarchy Process (AHP) model [20].

5) **Security matrix assessment:** Trust Matrix is a method used for security risk analysis in cloud environments.

Fatimah M. Alturkistani et al. [12] suggests to have a collaborative security risk assessment method where the assessment be collaboration between customers and providers that will add great assistance to both service providers and consumers.

3. Open Issues

There are many open issues need research to make cloud computing more trustworthy and reliable like the following:

(1) Building distributed, collaborative and intelligent risk assessor that guide customer to evaluate the security level of cloud provider and identify the associated risk before the decision of cloud adoption has been taken.

(2) Designing a mechanism that will allow the cloud provider to prove the confidentiality and integrity of the data and computation without disclosure of sensitive cloud topology information.

(3) Security standards for cloud risk assessment. Security assessment can give little information unless there is a standard to compare it with [12].

(4) Risk assessment approach for cloud consumers to check the effectiveness of the current security controls that protect an organization's assets. At present, there is a lack of risk assessment approaches for cloud consumers where the cloud consumers can perform the risk assessment to be aware of the risks and vulnerabilities present in the current cloud computing [1].

4. Conclusion

It is important to analyse the potential security challenges and risks cloud applications may face. Therefore, security risks assessment play a major role in the cloud computing environment where it may uncover some of the key risks, prioritize those risks and formulate a plan of action [27].

However, for cloud computing, risk assessment becomes more complex, there are several issues that are likely to emerge [1]. Therefore, the traditional assessments developed for conventional IT environments do not readily fit to the dynamic nature of clouds where Cloud computing provides opportunity to dynamically scale the computing resources for applications and end-users can arrive and leave the cloud at any time. Hence, the introduction of cloud specific security assessment methodology has significant importance and scope.

This paper introduces many security risk assessment methods addressed particularly for cloud computing environments and according to Fatimah M. Alturkistani et al. [12] the security risk assessment methods in cloud computing are classified into five classes: Risk assessment as a service; Qualitative and quantitative assessment; Graphs analysis assessment; Hierarchal assessment; and Security matrix assessment.

At the end, security risk assessment in clouds is still a challenging domain and a growing area of research and there are significant shortcomings in this area [3].

References:

[1] Drissi S., Houmani H. and Medromi H., Survey: Risk Assessment for Cloud Computing, University Hassan II Aïn Chock. ENSEM Casablanca, Morocco, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 12, 2013

[2]http://www.tutorialspoint.com/cloud_computing/cloud_computing_architecture.htm

[3] S. Subashini n, V.Kavitha Anna," Review A survey on security issues in service delivery models of cloud computing ",University Tirunelveli, Journal of Network and Computer Applications 34,India, 2011.

[4] Jaydip Sen,"Security and Privacy Issues in Cloud Computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[5] Lionel Bernard, Dr. Monica Bolesta, Dr. James Gelatte, Dr. Michael Evanchik," A Risk Assessment Framework for Evaluating Software-as-a-Service (SaaS) Cloud Services Before Adoption", Faculty of University of Maryland University College, January 21, 2011.

[6] Kuyoro S. O., Ibikunle F. & Awodele O.," Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3): Issue (5): 2011

[7] http://blogs.datadirect.com/2013/07/banking-security-cloud.html

[8] CSA, The Notorious Nine: Cloud Computing Top Threats in 2013, Top Threats Working Group, CSA, 2013, https://cloudsecurityalliance.org/download/the-notorious-nine-cloudcomputing- top-threats-in-2013/.

[9] Katerina Lourida1, Antonis Mouhtaropoulos2, Alex Vakaloudis, "Assessing Database and Network Threats in Traditional and Cloud Computing", International Journal of Cyber-Security and Digital Forensics (IJCSDF).

[10] Prof. Chitra Baggar, Prof. Richa Sinha," Identification And Analysis Of Risks For Cloud Computing In IAAS, PAAS And SAAS",International Journal of Computer & Organization Trends –Volume 3 Issue 9, Gujarat, Oct 2013,

[11] David López, Oscar Pastor, Luis Javier García Villalba1," DYNAMIC RISK ASSESSMENT IN INFORMATION SYSTEMS: STATE-OF-THE-ART", 6th International Conference on Information Technology May 8, 2013

[12] Fatimah M. Alturkistani, Ahmed Z. Emam, "A Review of Security Risk Assessment Methods in Cloud Computing", New Perspectives in Information Systems and Technologies, Volume 1 , Springer International Publishing, 2014.

[13] David Lopez,Oscar Pastor, Luis Javier Garcia Villalba," Data model extension for security event notification with dynamic risk assessment purpose",Science China Information Sciences, Volume 56, Issue 11, pp 1-9, November 2013.

[14] J. Oriol Fit´o, Mario Mac´ıas and Jordi Guitart, Toward Business-driven Risk Management for Cloud Computing, Barcelona Supercomputing Center and Technical University of Catalonia, 978-1-4244-8909-1/$26.00 _c 2010 IEEE.

[15] Federal communications commission, Cyber Security Planning Guide

[16] 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)

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

[18] Xuan Zhang, Nattapong Wuwong, Hao Li ,Xuejie Zhang,"Information Security Risk Management Framework for the Cloud Computing Environments",10th IEEE International Conference on Computer and Information Technology (CIT 2010), China.

[19] 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.

[20] Afnan Ullah, Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, Karim Djemame ,Security Risks and their Management in Cloud Computing, 4th International Conference on Cloud Computing Technology and Science ,UK,University of York, Switzerland ,Barcelona, Spain, 2012 IEEE.

[21] Onwudebelu, U.; Chukuka, B., "Will adoption of cloud computing put the enterprise at risk?," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.82,85, 25-27 Oct. 2012

[22] Peiyu, L. I. U., and L. I. U. Dong. "The new risk assessment model for information system in cloud computing environment." Procedia Engineering 15 (2011): 3200 3204

[23] Leitold, F.; Hadarics, K., "Measuring security risk in the cloud-enabled enterprise," Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on, vol., no., pp.62, 66, 16-18 Oct. 2012

[24] Tanimoto, S.; Hiramoto, M.; Iwashita, M.; Sato, H.; Kanai, A., "Risk Management on the Security Problem in Cloud Computing," Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on, vol., no., pp.147,152, 23-25 May 2011

[25] Jijun Zhang; Dejian Sun; Donghang Zhai, "A research on the indicator system of Cloud Computing Security Risk Assessment," Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012 International Conference on, vol., no., pp.121,123, 15-18 June 2012

[26] Cloud Security Alliance, Cloud Control Matrix. September 26, 2013

[27] Cloud Computing Risk Assessment A Case Study, ISACA Journal volume 4, 2011