Model for Cloud Computing Risk Analysis

Paulo F. Silva, Carlos B. Westphall, Carla M. Westphall
Networks and Management Laboratory
Post-Graduate Program in Computer Science
Federal University of Santa Catarina, Florianópolis, Brazil
e-mail:paulofernando@furb.br; westphal@inf.ufsc.br, carlamw@inf.ufsc.br

Mauro M. Mattos
Development and Transfer Technology Laboratory
Regional University of Blumenau, Blumenau, Brazil
e-mail: mattos@furb.br

Abstract – **Several risk analysis solutions have been proposed for cloud computing environments. But these solutions are usually centered on the Cloud Service Provider, have limited scope and do not consider the business requirements of the Cloud Consumer. These features reduce the reliability of the results of a cloud computing risk analysis. This paper proposes a model for cloud computing risk analysis in which responsibilities are not centered in the Cloud Service Provider. The proposed model makes the Cloud Consumer an active entity in risk analysis and includes the Information Security Laboratory entity. A prototype developed from the proposed model demonstrates performing a risk analysis in the cloud with shared responsibilities between the Cloud Service Provider, Cloud Consumer and Information Security Laboratory entities.**

Keywords – ISO 27005; cloud computing; risk analysis;

I. INTRODUCTION

Some of the challenges posed by cloud computing in the information security area are: identity management, virtualization management, governance and regulatory compliance, Service Level Agreement (SLA) and trust management, data privacy of the users and protection against external and internal threats [1]-[4].

Risk analysis [5] has been a strategy used to address the information security challenges posed by cloud computing, often addressing specific technical vulnerabilities or threats identification.

However, recent approaches on cloud risk analysis [6]-[12] did not aim at providing a particular architecture model for cloud environments, considering the entities involved and their responsibilities. Thus, the current models have the following deficiencies in their way of analyzing the risk of cloud computing environments:

- The deficiency in the adherence Cloud Consumer (CC) occurs when the entity responsible for defining impacts unaware of the technological environment and the CC business environment. In this case, the impact of this specification can disregard relevant scenarios for the CC or overestimate not relevant scenarios, thereby generating an incorrect risk assessment;
- The deficiency in the scope occurs when the selection of security requirements are performed by the Cloud Service Provider (CSP) itself or one without sufficient knowledge entity. The CSP can specify addict's security requirements in their own environment, thus defrauding the risk analysis results. Having an unprepared authority may specify requirements or insufficient disregard some important requirement, thus generating an incorrect risk analysis;
- The deficiency in the independence of results arises when the quantification of probabilities and impacts are performed by an entity that has an interest in minimizing the risk analysis results. For example, if the analysis is performed solely by the CSP. It can soften the assessment of requirements and impacts, thus generating a satisfactory result for the CC, but incorrect.

This paper proposes a model for performing risk analyzes in cloud environments that:

- Consider the participation of the CC entity in the performance of risk analysis, that is, allows an adherent risk analysis to CC's information security;
- Enabling the development of a risk analysis scope that is impartial to the interests of the CSP and to be developed by an entity with deep knowledge in information security;
- Does not have the centralized performance of risk analysis for the CSP entity, or to generate more independent results risks analysis possible in relation to the CSP interest, thus acting on the independence of disability results.

Therefore, the proposed model organizes the risk analysis in two phases: risk specification phase and risk evaluation phase. It also defines the entities involved in each phase and their responsibilities. Finally, the proposed model also provides a language for defining risk and a protocol for

 ISBN: 978-1-61208-398-8

communication between the entities involved in risk analysis.

The rest of this paper is as follows organized. Section 2 discusses related works on. The Proposed model is presented in Section 3. Section 4 describes the results and discussions. We conclude the paper and present future works in Section 5.

II. RELATED WORKS

Hale and Gamble [7] present a framework called SecAgreement that allows management of security metrics between CSPs and CCs. An SLA for cloud risk management is presented by Morin, Aubert and Gateau [8]. Ristov, Gusev and Kostoska [9] discuss risk analysis in cloud computing environments based on ISO 27001 and offers a model for security assessment in cloud computing. Chen, Wang and Wang [10] present an architecture that defines security levels from the risk of each CC service in the CSP.

Zech, Felderer and Breu [11] introduce a model for security testing in cloud computing environments based on risk analysis of these environments. Wang, Lin and Kuo [12] discuss risk analysis in cloud computing using intrusion techniques based on attack-defense trees and graphs.

Rot and Sobinska [13] discuss new information security threats specifically applied in cloud computing environments. Ristov and Gusev [14] present a security assessment of the main cloud environments open source, while Mirkovic [15] presents some security controls from ISO 27001 applied to cloud computing.

Ullah, Ahmed and Ylitalo [16] describe the Cloud Security Alliance (CSA) effort to inform security evaluation of automation in cloud services providers, the Cloud Audit, while Khosravani et al. [17] present a study of risk analysis in case of cloud computing, focusing on the importance of data security requirements that will be migrated to the cloud. Lenkala, Shetty and Siong [18] build upon the National Vulnerability Database (NVD) to identify vulnerabilities in cloud environments. Liu, Wu, Lu and Xiong [19] propose a model for information security risk analysis in virtual machines cloud computing environments, based on the ISO 27001, 27002 and 27005.

The related works presented above discuss the risk analysis on requirements or specific scenarios in cloud computing. The model proposed in this paper is different from the related works because it addresses an architecture for different risk scenarios in cloud computing, including discussion of the agents involved, communication protocol and language for description of the risks.

III. THE RACLOUD MODEL

This section presents the model for risk analysis proposed in the cloud, called RACloud – Risk Analysis for Clouds.

A. Risk Definition Language

The model provides a language for specifying risk, Risk Definition Language (RDL). The RDL is specified in XML and contains information about threats, vulnerabilities and information assets. This information is the basis for performing risk analysis in RACloud model.

The RDL allows specification of three different types of records: threats, vulnerabilities and information assets. Figure 1 shows an example of specifying vulnerability records, which are two specified vulnerabilities from the Common Vulnerabilities and Exposures (CVE).

Each record contains information RDL header with Id, source and version of the XML file and registry information risk (threats, vulnerabilities or information asset) with Id, description, category and Web Service Risk Analysis (WSRA).

The WSRA is a web service responsible for evaluating the record of risk (threat, vulnerability and asset information). It is also responsible by quantifying the risk as shown in Section III-C.

```
<RDL type="ISL" id="1299">
    <source>LRG-UFSC</source>
    <version>4.5.1a</version>
    <description>...</description>
    <vulnerabilities>
        <item id="129">
            <description>Cipher protocol weak</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate129</wsra>
        </item>
        <item id="239">
            <description>Clear text password</description>
            <category>service</category>
            <wsra>http://lrg.ufsc.br:8095/evaluate239</wsra>
        </item>
    </vulnerabilities>
</RDL>
```

Figure 1. An RDL especification of vulnerabilities.

The RDL records are used by the components of the model RACloud (Section III-B) during phases of risk specification (Section III-D) and risk assessment (Section III-E).

B. Architectural Components

The RACloud model shares the responsibility of risk analysis between four distinct entities: RAH - Risk Analysis Host, ISL - Information Security Laboratory, CSP - Cloud Service Provider and CC - Cloud Consumer. These entities relate to different components at different times.

The RAH entity has responsibility for the host connection and core layers, formed by components Conn ISL, Conn CC, Conn CSP, Agent Manager, RDL Manager and Analysis Manager (Figure 2).

The components Conn ISL, Conn CC and Conn CSP are interfaces for communication with other components distributed respectively between the entities ISL, CC, CSP.

The Agent Manager component is responsible for managing the registration of CC, CSP and ISL entities in RACloud model. The RDL Manager component is responsible for managing and storing the records of defining risks. And Analysis Manager component is responsible for performing the risk assessment.

 ISBN: 978-1-61208-398-8

The ISL is a laboratory entity or group specializing in information security, its responsibility is to specify the RDLs vulnerabilities and threats, in addition to their WSRAs. This entity hosts the ISL Agent and WSRA Evaluator components. The component ISL Agent is responsible for registering the ISL in RACore and publish its RDLs. The WSRA Evaluator component is responsible for performing assessments of threats and vulnerabilities described in RDLs.

The CSP represents the entity's own cloud service provider aim of risk analysis. This entity hosting the CSP Agent and WSRA Proxy components. The CSP Agent component is responsible for registering the CSP in RACore and subscribe to RDLs, which the CSP aims to be analyzed. The WSRA Proxy component is responsible for collecting information from the CSP and make the call of WSRAs.

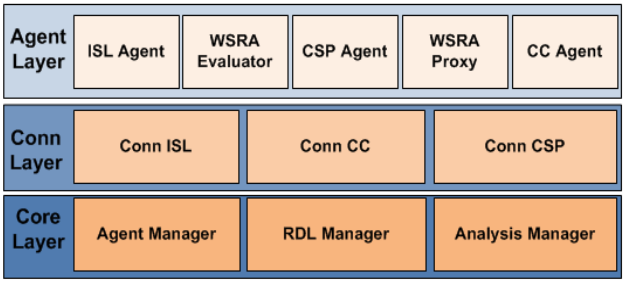

Figure 2. Model Layers RACloud.

The CC entity is the CSP's customer, hosting their information assets in the cloud and want to know which one is exposed to risk in relation to its CSP. This entity hosts the CC Agent component. This component is responsible for registering the CC in RACloud and initiate risk analysis.

C. *Risk Modeling*

Information assets, threats and vulnerabilities are the basic elements of a risk analysis of information security. RACloud in these model elements are defined by CC and ISL entities. Variables modeling of risk posed information assets, threats and vulnerabilities are shown in Table I.

TABLE I. BASIC ELEMENTS

Symbol	Description
T_x	Treat defined by ISL "x"
A_y	Information Asset defined by CC "y"
V_z	Vulnerability defined by ISL "z"

In the risk analysis, functions are applied to the information assets, threats and vulnerabilities, with the aim of analyzing their impact, exposure and disability, respectively. The functions for allocating degree of impact, degree of exposure and degree of disability are represented according to Table II.

TABLE II. FUNTIONS OF ANALYSIS

Symbol	Description
$eaf(T_x,w)$	Exposure analysis function of T_x on CSP "w"
$iaf(A_y)$	Impact analysis function of A_y
$daf(V_z,w)$	Deficiency analysis function of V_z on CSP "w"

The analysis functions represented in Table II result in the calculation of the degree of impact, degree of exposure and degree of disability. The three variables are represented in RACloud as described in Table III.

TABLE III. VIABLES OF ANALYSIS

Symbol	Description
$DE_{T,x,w}$	Degree of Exposure related with T_x and w. $eaf(T_x,w)=DE_{T,x,w}$
$DI_{A,y}$	Degree of Impact related with A_y. $iaf(A_y)=DI_{A,y}$
$DD_{V,z,w}$	Degree of Deficiency related with V_z and w. $daf(V_z,w)=DD_{V,z,w}$

A risk event is the relationship of a threat with a vulnerability. This relationship is established in RACloud through a correlation function of the event. From the risk events are calculated the probabilities of occurrence of the event, based on the degree of exposure and the degree of disability. The modeling related events and probabilities is presented by Table IV.

TABLE IV. PROBABILITY CALCULATION

Symbol	Description
$E_{T,V}$	Event relating T with V
$\alpha(T_x,V_z)$	Function correlating T and V $\alpha(T_x,V_z)=E_{T,V}$
$fp(E_{T,V})$	Function of probability of $E_{T,V}$ $fp(E)=(DE_{T,x,w}+DD_{V,z,w})/2$, or, $fp(E)=matrix(DE_{T,x,w},DD_{V,z,w})$
P_E	Probability of $E_{T,V}$ $fp(E_{T,V})=P_E$

From the probability of risk events and the degree of impact on information assets, it is possible to calculate the risk of a particular event on a particular information asset. The relationship between risk events and information assets are given by a function correlation risk. The modeling related to the correlation of risk and the final calculation of risk is presented by Table V.

TABLE V. RISK CALCULATION

Symbol	Description
$R_{E,A}$	Risk relating E and A
$\beta(E,A_y)$	Function correlating E and A_y $\beta(E,A_y)=R_{E,A}$
$raf(R_{E,A})$	Risk analysis function of $R_{E,A}$ $raf(R_{E,A})=(P_E+ DI_{A,y})/2$ or $raf(R_{E,A})=matrix(P_E,DI_{A,y})$
$DR_{E,A}$	Degree of risk related with $R_{E,A}$ $raf(R_{E,A})=GR_{E,A}$

D. *Specification Phase*

In the risk specification phase, RACloud model of the threats (T_x), vulnerabilities (V_z) and information assets (A_y) part of risk analysis is defined.

Figure 3 illustrates the flow of interactions between components of the model RACloud specification phase risk. Initially each agent must register with the Agent Manager component (Figure 3 -a, b, c). After it registed ISL has the responsibility to specify threats and vulnerabilities of cloud computing environments and develop RDLs and WSRAs to these threats and vulnerabilities. The vulnerabilities and threats WSRAs to match functions eaf(T_x,w) e daf(V_z,w) of the risk modeling, respectively.

After developing their RDLs and WSRAs ISL exports the records of RDLs for the RDL Manager (Figure 3 -d) component and publishes WSRAs (Figure 3 -e) so they can be called by the CSP in the evaluation phase.

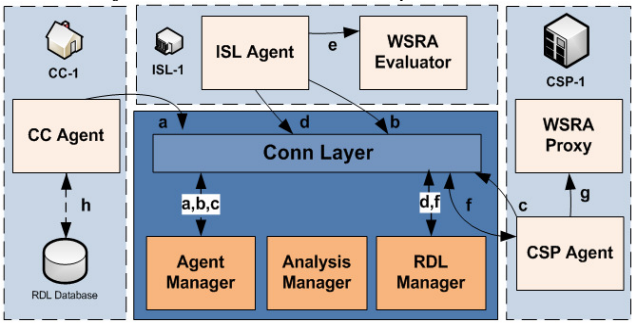

Figure 3. Specification time.

The performance of the CSP specification phase of risk is to import the RDLs recorded by ISL (Figure 3 -f.) and implement the Proxy WSRAs to call WSRAs of the evaluation phase (Figure 3 -g).

The identification of threats and vulnerabilities, is the responsibility of the ISL and the call of WSRAs, is the responsibility of the CSP, but the definition of information assets and quantification of impact on these assets is the responsibility of the CC. Because CC entity is most adequate for the express the potential loss in the event of an incident. Thus, the responsibility of CC Agent on phase specification risk is to build a database of information assets RDLs (Figure 3 -h).

E. Evaluation Phase

In the risk evaluation phase, it ocorrs the call of the functions eaf(T_x,w), daf(V_z,w) e iaf(A_y), and quantifying the variables $E_{T,V}$, P_E and $R_{E,A}$ defined in risk modeling.

The evaluation begins with the CC Agent informing the CSP to be analyzed (Figure 4 -a). From this component Analysis Manager obtains information from the CSP (Figure 4 -b) and queries the registered RDLs (Figure 4 -c).

Based on information obtained from CSP and RDL, Analysis Manager component starts and will evaluation threats and vulnerabilities. To do so, makes the invocation of CSP Agent. Then there is the collection of information about threats and vulnerabilities through WSRAs Proxy and the assessment of that information through WSRAs ISL. Then WSRAs ISL make quantification of the variables $DE_{T,x,w}$ and $DD_{V,z,w}$ (Table II) and return these values to Analysis Manager component (Figure 4 -d).

After quantifying all the threats and vulnerabilities associated with RDLs defined in CSP, begins to quantify the impacts defined by the CC. Therefore, the Analysis Manager component invokes the CC Agent for the degree of impact of their information assets (Figure 4 -e). With the return of CC Agent Analysis Manager component defines the value of the variables $DI_{A,y}$.

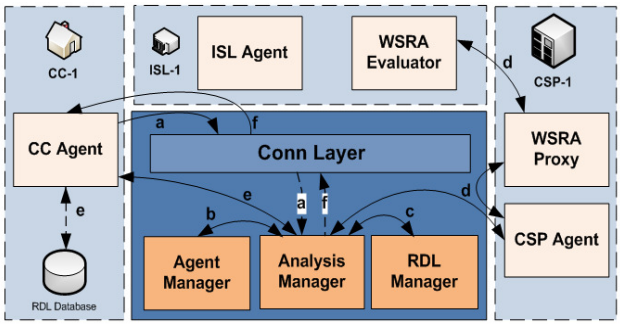

Figure 4. Evaluation time.

Once obtained the values of $DI_{A,y}$, $DE_{T,x,w}$ e $DD_{V,z,w}$ for all information assets, threats and vulnerabilities defined in RDLs, Analysis Manager component starts the calculation of the variables $E_{T,V}$ and P_E and through the functions $\alpha(T_x,V_z)$ and $fp(E_{T,V})$. This process results in a list of possible events, or which may threats and vulnerabilities which exploits, and the respective probability of each event.

Finally, the Analysis Manager component does the calculation of the variables $R_{E,A}$ and $DR_{E,A}$, through the functions $\beta(E,A_y)$ and $raf(R_{E,A})$ respectively. The result of this process is the ratio of risk items, ie valid relation between events and information.

After the calculation of all risk items ($R_{E,A}$) and their degrees of risk ($DR_{E,A}$) the result is returned to the CC Agent for it to take decisions on the acceptance or not of risk found in their CSP (Figure 4 -f).

IV. RESULTS AND DISCUSSION

For testing purposes and discussion, we developed a prototype RACloud model as presented in Section III. From the prototype were performed phases of risk specification and risk evaluation in a controlled environment for testing.

In the risk of specification phase (Section III-D), were specified 20 RDL records vulnerabilities and 20 RDL records threats and 10 RDL records of information assets. The RDL records of threats and vulnerabilities were specified as threats and vulnerabilities found in CVE -. Common Vulnerabilities, Exposures. Also WSRAs and WSRAs Proxy have been developed for the 40 records of threats and vulnerabilities specified.

In the risk evaluation phase (Section III-E), the WSRAs Proxy and WSRAs were performed, generating the DD and DE values for each vulnerability and threat record,

 ISBN: 978-1-61208-398-8

respectively. The records of vulnerabilities and threats were correlated by Analysis Manager component generates 20 events, which were correlated with the records of information assets, generating 20 risk scenarios.

Figure 5 shows the result of calculation of variables DE, DD, P, DI and DR for the 20 risk scenarios (R1 to R20) specified in the prototype.

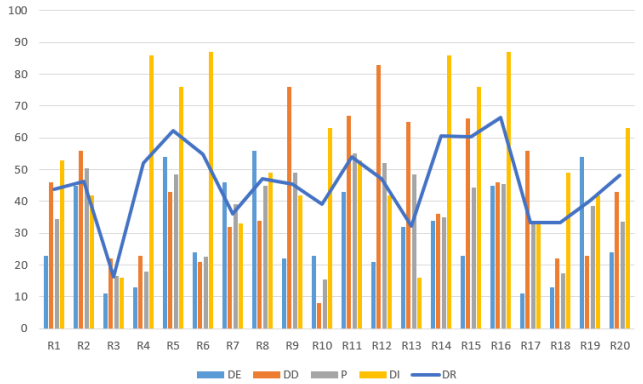

Figure 5. Evaluation of risk.

The lower risk identified was the R3 risk scenario, with risk of 16.25%. This scenario specifies as information asset the file transfer service, as vulnerability the unencrypted password and as threat the unauthorized access.

The greatest risk identified was the risk scenario R16, with risk of 66.25%. This risk scenario specifies as information asset the e-mail service, as vulnerability the weak encryption protocol and as threat the DDoS.

Figure 6 presents the results of the risk assessment generated by RACloud model prototype for the risk scenarios R3 and R16. For each risk scenario is possible to observe the results of probability and risk variables. You can also see a brief description of the items threats, vulnerabilities and information assets and the value of their respective variable degree of exposure, degree of deficiency and degree of impact.

With the risk analysis of the resulting information the CC may decide to allocate or not their information assets in a given CSP, or remove their systems of a CSP to present great risks.

The proposed model aims to reduce the three major deficiencies presented by current models of cloud risk analysis: deficiency in scope, deficiency in the adherence and deficiency in independence of results.

The reduction deficiency in the adherence occurs when the proposed model includes the CC as a key entity in the risk analysis process. In the model RACloud, the CC entity acts in active mode on risk analysis, defining information assets and quantifying impacts on these assets.

The CC is the entity most apt to define the impacts, it is the entity that best knows the relevance of each information asset within its area of operation. Therefore, it is CC's responsibility to say what the impact will be whether a system file or database has its integrity, confidentiality or availability impaired. The CSP and ISL entities have no automy to identify or quantify impacts on information assets, because they are not experts in CC business area.

```
<RDL Id="248" type="RISK">
   <source>RACloud-LRG</source>
   <version>5a</version>
   <description>...</description>
   <cc_id>consumerCC</cc_id>
   <csp_id>testCSP</csp_id>
   <risks>
      <item id="3">
         <probability>16.25</probability>
         <risk>42</risk>
         <informationasset DI="16">File transfer service</informationasset>
         <vulnerability DD="22">Clear text password</vulnerability>
         <treat DE="11">Unauthorized Access</treat>
      </item>
      <item id="16">
         <probability>45.5</probability>
         <risk>66.25</risk>
         <informationasset DI="87">Email service</informationasset>
         <vulnerability DD="46">Cipher protocol weak</vulnerability>
         <treat DE="45">DDos</treat>
      </item>
   </risks>
</RDL>
```

Figure 6. Result of risk.

The RACloud model works to reduce the deficiency in scope in that it introduces the ISL entity. As the ISL an entity specialized to information security is the entity best placed to define security requirements, threats and vulnerabilities (specification of RDLs) and set as the threats and vulnerabilities should be quantified (specification of WSRAs).

The reduction of deficiency in the independence of the results is the fact that the model RACloud the CSP has more restricted responsibilities than in the models traditionally presented by related work.

Traditionally, the CSP is responsible for defining security requirements and the tests that are applied to risk assessment of their own environment. In this scenario the risk assessment may be biased to the CSP. Including the ISL entity removes responsibilities traditionally assigned to the CSP, as identification and quantification of threats and vulnerabilities, thus making it more reliable the result of risk analysis.

The proposed model allows multiple ISLs act in the definition of RDLs and WSRAs together. Thus the risk definitions can come from different sources and can be constantly updated dynamic and collaborative way, forming a risk settings based on extensive and independent cloud.

The way WSRAs are specified is also a feature that impacts the improvement scope. The use of Web Services to specify security requirements allows them to be platform independent and can be ordered by any CSP. It also allows the use of a wide variety of techniques for quantification of threats and vulnerabilities, because the limit is defined only by the programming language chosen for implementation of WSRA.

The related works of cloud risk analysis did not consider the role of CC entity in the risk analysis. These works usually aim on the vulnerability assessment by the CSP itself, without considering the impact that the vulnerability will cause on the different CC information assets. By assigning the responsibility for identifying and quantifying

 ISBN: 978-1-61208-398-8

the impact of the CC are sharing the risk variables among different entities, so the responsibility for the quantification of risk analysis variables is not centralized in one specific entity.

The CSP is the entity that will be the analyzed then it doesn't have the autonomy to set any of the values of risk analysis, as this could make unreliable risk analysis. The role of CSP is only inform the data requested by ISL, so that ISL itself makes the quantification of security requirements.

With RACloud model CC can perform analyzes in several CSPs before deciding to purchase a cloud computing service. The CC can also carry out regular reviews of your current provider and compare them with other providers, opting for changing its CSP.

V. CONCLUSION

This paper presented a model for risk analysis in cloud computing environments.

The proposed model changes the generally current paradigm in research on cloud risk analysis, in which the CSP entity is responsible for the specification of security requirements and analysis of these requirements in its own environment, so the only entity responsible for the results risk analysis.

To reduce excess CSP responsibility for risk analysis, the proposed model includes two new entities with active participation in risk analysis, the CC entity and the ISL entity.

The model presented in this paper is an initiative of the CC itself can perform risk analysis on its current or future CSP. And that this risk analysis is adherent, comprehensive and independent of the CSP interests.

The characteristics presented in this paper are intended to generate a more reliable risk analysis for CC, so that it can choose its CSP based on more consistent information, specified and analyzed by an exempt entity interests, ISL.

Several papers on cloud computing indicate lack confidence CC in relation to the CSP as a great motivator for not acquiring cloud computing services. An independent risk analysis can act to reduce this mistrust and promote the acquisition of cloud computing services.

The prototype and the results show the specification and implementation of an adherent risk analysis, comprehensive and independent, because the analysis is not centered in the CSP. The identification and quantification of threats and vulnerabilities can be performed by many security laboratories and the impact on the information assets is defined by the CC itself.

Several future works can be developed from the RACloud model. There is a need to extend this work to suggest the controls or countermeasures for CSPs can mitigate its risks. Searches can be developed on the reliability of the data reported by the CSP to the ISL for risk analysis and the specification of risk definition language can be further explored in specific researches.

REFERENCES

[1] M. K. Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj, and P. Revathy, "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment". ICACCI '12: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, August 2012, pp. 470-476.

[2] H. Yu, N. Powell, D. Stembridge and, X. Yuan, "Cloud computing and security challenges". ACM-SE '12: Proceedings of the 50th Annual Southeast Regional Conference, March 2012, pp. 298-302.

[3] K. Ren, C. Wang and Q. Wang, "Security Challenges for the Public Cloud," Internet Computing, IEEE, vol.16, no.1, Jan.-Feb. 2012, pp. 69-73, doi: 10.1109/MIC.2012.14, retrieved: March, 2015.

[4] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE , vol.9, no.2, March-April 2011, pp. 50-57, doi: 10.1109/ MSP.2010.115.

[5] ISO/IEC 27005:2011, Information Security Risk Management. [Online]. Available: http://www.iso.org, retrieved: March, 2015.

[6] J. Zhang, D. Sun and D. 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., June 2012, pp.121,123, 15-18 doi: 10.1109/ ICQR2MSE. 2012.6246200.

[7] M. L. Hale, and R. Gamble, "SecAgreement: Advancing Security Risk Calculations in Cloud Services," Services (SERVICES), 2012 IEEE Eighth World Congress on , vol., no., June 2012, pp.133-140, 24-29, doi: 10.1109/SERVICES.2012.31.

[8] J. Morin, J. Aubert, and B. Gateau, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," System Science (HICSS), 2012 45th Hawaii International Conference on , vol., no., pp.5509-5514, 4-7 Jan. 2012 doi: 10.1109/HICSS.2012.602.

[9] S. Ristov, M. Gusev, and M. Kostoska, "A new methodology for security evaluation in cloud computing," MIPRO, 2012 Proceedings of the 35th International Convention , vol., no., May 2012, pp.1484-1489, 21-25.

[10] J. Chen, Y, Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, IEEE, vol.45, no.7, July 2012, pp.73,78, doi: 10.1109/MC.2012.120.

[11] P. Zech, M. Felderer, and R. Breu, "Towards a Model Based Security Testing Approach of Cloud Computing Environments," Software Security and Reliability Companion (SERE-C), 2012 IEEE Sixth International Conference on , vol., no., June 2012, pp.47,56, 20-22 doi: 10.1109/SERE-C.2012.11.

[12] P. Wang, W. Lin, P. Kuo, H. Lin and, T. Wang, "Threat risk analysis for cloud security based on Attack-Defense Trees," Computing Technology and Information Management (ICCM), 2012 8th International Conference on, vol.1, no., April 2012, pp.106-111, 24-26.

 ISBN: 978-1-61208-398-8

[13] A. Rot, and M. Sobinska, “IT security threats in cloud computing sourcing model”, Computer Science and Information Systems (FedCSIS), 2013, Federated Conference on, Publication Year: 2013, pp. 1153- 1156.

[14] S. Ristov, and M. Gusev. “Security evaluation of open source clouds”, EUROCON, 2013 IEEE, Digital Object Identifier: 10.1109/EUROCON. 2013.6624968, Publication Year: 2013, Page(s): 73- 80.

[15] O. Mirkovic, “Security evaluation in cloud”, Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on, Publication Year: 2013 , Page(s): 1088-1093.

[16] K. Ullah, A. Ahmed, and J. Ylitalo. “Towards Building an Automated Security Compliance Tool for the Cloud”. Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. Digital Object Identifier: 0.1109/TrustCom. 2013.195. Publication Year: 2013, Page(s): 1587- 1593.

[17] A. Khosravani, Nicholson, B., and Wood-Harper, T., “A case study analysis of risk, trust and control in cloud computing”, Science and Information Conference (SAI), 2013, Publication Year: 2013, Page(s): 879- 887.

[18] S. R. Lenkala, Shetty, S., and Kaiqi Xiong. “Security Risk Assessment of Cloud Carrier”. Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, Digital Object Identifier: 10.1109/CCGrid.2013.28, Publication Year: 2013, Page(s): 442- 449.

[19] S. Liu, J. Wu, Z. Lu, and H. Xiong, “VMRaS: A Novel Virtual Machine Risk Assessment Scheme in the Cloud Environment”, Services Computing (SCC), 2013 IEEE International Conference on, Digital Object Identifier: 10.1109/SCC.2013.12, Publication Year: 2013, Page(s): 384-391.

 ISBN: 978-1-61208-398-8