Revista de Sistemas de Informação da FSMA
n. 17 (2016) pp. 25-31

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

RACLOUDS - Model for Clouds Risk Analysis in the Information Assets Context

Paulo Fernando Silva, Carlos Becker Westphall, Carla Merkle Westphall

Networks and Management Laboratory
Post-Graduate Program in Computer Science
Federal University of Santa Catarina, Florianópolis, Brazil

***Abstract* – Cloud computing offers benefits in terms of availability and cost, but transfers the responsibility of information security management for the cloud service provider. Thus the consumer loses control over the security of their information and services. This factor has prevented the migration to cloud computing in many businesses. This paper proposes a model where the cloud consumer can perform risk analysis on providers before and after contracting the service. The proposed model establishes the responsibilities of three actors: Consumer, Provider and Security Labs. The inclusion of actor Security Labs provides more credibility to risk analysis making the results more consistent for the consumer.**

Keywords – cloud computing; risk analysis;

I. INTRODUCTION

Cloud computing is a paradigm that provides the possibility of access to applications and infrastructure software and hardware as a service. The cloud structure is provided to Cloud Consumers (CC) by a Cloud Service Provider (CSP) and is usually classified in Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) [1].

The cloud computing paradigm has changed the environment for technology companies. These companies are migrating from an isolated environment with few servers and applications to integrated environments with lots of different applications and servers. This new reality of information technology brings many security challenges for CSPs, and a lot of mistrust for CCs [2][3].

Adopting a cloud service generates for the CCs a huge challenge because unless cloud providers can readily disclose their security controls and the scope of their implementation to the client, so that he knows what controls are used to maintain the security of his information, there is huge potential for poor decisions and negative.

A new strategy for managing security challenges in cloud computing is risk analysis. Risk analysis is the identification of threats and vulnerabilities that can generate incidents, and the quantification of the impact that these incidents may have on the CC's information assets [4].

This paper proposes a collaborative risk analysis model in cloud computing. This new model combines the traditional actors CSP and CC, while also adding a new actor, the Information Security Laboratory – ISL. The ISL is responsible for acting collaboratively in specifying information security requirements for cloud computing. An ISL can be a laboratory or public, private or academic information security group with an interest in collaborating with information security in cloud computing which will then serve as a third party with no vested interests in the transaction, becoming able, then, to independently access all the flaws and qualities of whichever contract is defined.

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

II. RELATED WORK

Rot and Sobinska [5] discusses new information security threats specifically applied in cloud computing environments. The survey says that there are always new threats related to cloud computing and the constant evaluation of these threats is necessary to ensure the safety of information and services in the cloud.

Bleikertz and Mastelic [6] mentions that although there are several parties involved in providing cloud services, a cloud client still has a hard time assessing threats, vulnerabilities and risks of cloud environment that consumes. Hence, models are needed that allow for the systematic evaluation of the CSP by the CC. The authors also proposed a high-level model for CCs to evaluate the safety of CSPs. The model is based on the description of "what-if" scenarios and the systematic evaluation of these scenarios in the cloud environment.

Ristov and Gusev [7] presents a safety assessment of the main cloud environments open source. The study analyzed the

environments OpenStack, Eucalyptus, OpenNebula and CloudStack considering security aspects defined by ISO 27001 as: stability, implementation, operation, monitoring and review. The study shows that all evaluated environments are not fully compliant with most of the ISO 27001 requirements.

A cloud security assessment based on ISO 27001 is also presented by [8]. The paper presents some security controls ISO 27001 information applied to cloud computing, and security metrics for such controls. The paper concludes that many controls cited on ISO 27001 are also importants to cloud computing cenarious.

Alebrahim, Hatebur and Goeke [9] states that information security is a key issue for decision making on the acquisition of cloud computing services and the ISO 27001 provides a general standard for the treatment of this issue. The authors also said that risk analysis is an essential part of ISO 27001 and, therefore, proposes a structured approach to the identification of information assets, threats and vulnerabilities.

Cayirci, Garaga, Oliveira and Roudier [10] presents a model for cloud risk assessment in which the customer can carry out the assessment and analyze the risk of adopting a particular cloud provider. The author notes that this is an essential approach to the cloud customer to carry out the most appropriate decision-making in relation to its risk profile.

In [11] authors states that information security-related issues are among the top reasons for organizations to prevent the adoption of cloud computing services. The paper presents a model for CSP risk assessment considering the level of security provided for a particular application allocated in their environment, whose main benefit is a new model for risk assessment on CSP

Gupta, Mulero, Matthews, Dominiak, Omerovic, Aranda and Seycek [12] points out the amount of cloud service providers available in the market is increasing, all of them providing various types of services. This fact only complicates the decision on the adoption of a particular cloud provider by the customer. Therefore, there is an increasing amount of research that aims to provide the CC information to support his decision to choose his cloud provider. The author works in the approach of decision support systems for risk analysis of the particular cloud provider selection. Finally, as a proof of concept of goal, the paper presents a prototype of the proposed model.

The related works presented above discuss models and definitions of requirements for risk analysis in cloud computing, but they don't comment on the definition of the actors involved and their interactions during the execution of risk analysis. They also have no possibility of upgrading or evolving their security requirements, which are often described statically.

The risk analysis solutions for cloud computing identified in this section have different limitation levels in aspects of scope, adherence and independence of the risk analysis. The issue of scope relates to the definition of the scope of safety requirements applied to risk analysis. The adherence aspect is whether they consider the customer's business nature in the calculation of risk analysis. The independence aspect is on whether they carry out risk analysis so that its specification, implementation and results are not influenced by the interests of specific agents, such as CSP. These three aspects are the main focus of this paper.

III. THE RACLOUDS ARCHITECTURE

The risk analysis performed by RAClouds [13][14] is based on concepts defined by ISO 27001. In this context, threats exploit vulnerabilities that impact on information assets. The probability of an event occurring is calculated from the degree of exposure to a threat and the degree of disability of a vulnerability. The risk is calculated from the probability that an incident occurs and the impact of this incident.

In RACloud model the different existing resources in a cloud computing environment are grouped into RCs (Resource Category). Table 1 shows the 10 categories of cloud resources RACloud model.

RC	RL	Exemplos de Recursos
Hardware	0	CPU, memória, disco
SO System	1	Windows, linux
VM System	1	Vmware, HiperV
Communication System	1	IP, TCP, UDP, HTTP
Cloud System	1	Amazon S3, Rackspace Cloud Files
Database	2	Orable, MySQL, Amazon SimpleDB
Framework	2	Java, C#, etc
Application Server	2	Amazon AWS
Application System	3	Office 365
Information System	3	Sale force

Table 1. Resource Categories.

A particular threat is correlated with a certain vulnerability by RACloud model event correlation function when their resource categories are equal and at least one of its security properties is equal. This correlation between threat and vulnerability generates information security events, as shown in figure 5.

The RACloud model also organizes the different types of information assets allocated for CC in a cloud computing environment in four categories of assets (AC - Asset Category): (i) File, (ii) Database (iii) CC-Software and (iv) CSP-Software.

The category File consists of any files belonging to the CC and stored directly in the CSP file system. The second category, Database, consists of information pertaining to CC and stored in a database hosted on the CSP cloud environment. The "CC-Software" consists of developed and owned by CC systems, but running and available to users via the CSP environment. CSP-Software consists of information pertaining to CC and are stored in specific formats of the CSP and software are accessed through such software

For the generation of information security risk items RACloud the model performs the correlation between information security events and information assets. Table 2 shows the correlation between events (using resource categories) and information assets (using categories of information assets). The relationships marked with "X" means that the active information is always associated with the resource, whereas relationships marked "O" means that this relation is dependent on the context of information asset.

.

RL	Resource Category	Asset Category			
		File	Database	CC-Software	CSP-Software
0	Hardware	X	X	X	X
1	SO System	X	X	X	X
1	VM System	X	X	X	X
1	Communication System	X	X	X	X
1	Cloud System	X	X	X	X
2	Database		X	O	O
2	Framework			O	O
2	Application Server			O	O
3	Application System				O
3	Information System				O

Table 2. Correlation between events and information assets.

```
▼<RDL type="ISL" id="1299">
   <source>LRG-UFSC</source>
   <version>1.3</version>
   <description>...</description>
  ▼<vulnerabilities>
   ▼<item id="9593" propertyC="true" propertyI="true" propertyA="false">
    ▼<description>
        Apache CloudStack before 4.3.2 allow obtain private key
     </description>
     <category>Communication System</category>
     <wsra>http://localhost:8095/isl9593</wsra>
     <reference>CVE-2014-9593</reference>
    </item>
   ▼<item id="0140" propertyC="true" propertyI="true" propertyA="true">
     <description>Red Hat CloudForms 3.1 allow Unauthorised actions</description>
     <category>Cloud System</category>
     <wsra>http://localhost:8095/isl0140</wsra>
     <reference>CVE-2014-0140</reference>
    </item>
   ▶<item id="1609" propertyC="false" propertyI="false" propertyA="true">...</item>
   ▶<item id="3367" propertyC="true" propertyI="true" propertyA="true">...</item>
   ▶<item id="0640" propertyC="false" propertyI="false" propertyA="true">...</item>
   ▶<item id="0412" propertyC="true" propertyI="true" propertyA="true">...</item>
   ▶<item id="2576" propertyC="false" propertyI="true" propertyA="false">...</item>
   </vulnerabilities>
</RDL>
```

Figure 1. Example vulnerability RDL.

.

The RACloud model provides a language for risk specification, the RDL - Risk Definition Language. The RDL is specified in XML Schema (XSD) and contains information about threats, vulnerabilities and information assets. Figure 1 shows an example of vulnerability RDL, which describes all the information about the vulnerabilities used in a given risk analysis. There is the WSRA information (Web Service Risk Analysis), which defines the address for the Risk Analysis Web Service.

RAClouds' risk analysis is organized into two distinct phases, the risk specification phase and the risk assessment phase.

The RAClouds interacts with three main actors, which have well-defined roles in the implementation of risk analysis. The actors are: Cloud Consumer - CC, Cloud Service Provider - CSP and Information Security Labs – ISL. Now, let us explain how all these interactions take place in each phase.

Figure 2 illustrates the flow of interactions between the RAClouds components and the ISL, CSP and CC actors during the specification phase. Initially each of the actors must register in their respective registry component (Fig. 2a, b, c), and subsequently interact with the risk specification repositories.

In the risk specification phase, the ISL's role is to identify threats and vulnerabilities (RDLs) to the security requirements in cloud computing environments. From this identification, the ISL also has the responsibility of specifying the form of quantification of threats and vulnerabilities (WSRA), defining how threats and vulnerabilities will be quantified in a real cloud computing environment.

Besides specifying one or more RDLs for each security requirement, the ISL must also implement the form of quantification of each risk. In order to model RAClouds, risk quantification is implemented through a Web Service that runs in an environment under the responsibility of the ISL. After developing their RDLs and risk quantification Web Services (WSRAs), the ISL exports the RDL records to the RAClouds' RDLs repository (Fig.2-d, e).

.

The role of the CSP in the risk specification phase is to import the RDLs logged in the RAClouds and implement the risk quantification Web Services calls, as defined in the RDL specified by the ISL (Fig. 2-f, g). To meet the specific risk assessment needs, the CSP has the responsibility of correctly implementing and passing the data to the risk quantification Web Services.

The identification of threats and vulnerabilities is the responsibility of the ISL and the correct execution of the quantification of threats and vulnerability is the responsibility of the CSP, but identification of information assets and quantification of impact on these assets is the responsibility of the CC, as this is the actor best suited to express the size of a loss in the event of an incident. For this, the CC has a RDLs base of information assets (Fig. 2h).

This concludes the risk specification phase and the RAClouds is able to initiate the risk assessment of a CSP according to the requirements defined by the ISL and the impacts defined by the CC.

Figure 3 illustrates the flow of interactions between the RAClouds components and the ISL, the CSP and the CC during risk assessment. The implementation of risk analysis is distributed among components on all actors involved (CC, CSP, ISL and RAClouds).

The RAClouds has the Analysis Manager component that coordinates the interaction between external actors and other components inside RAClouds. The RDL Manager components store records of threats and vulnerabilities of ISLs and information assets of CCs, respectively.

WSRA Evaluator is a component that contains the Web Services assessment of threats and vulnerabilities identified by an ISL. WSRA Proxy is a component of the CSP deployed to handle the call of the Web Services responsible for the assessment of threats and vulnerabilities. Through this component the CSP invokes the threats and vulnerabilities Web Services of the ISL, passing their data about compliance to the security requirements or lack thereof.

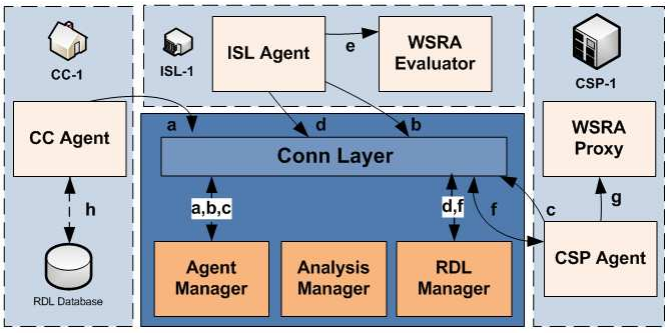

Figure 2. RAClouds specification phase.

.

The risk assessment begins with the CC accessing the RAClouds and selecting the CSP to be analyzed (Fig. 3a, b). Then the RAClouds accesses the RDL Manager (Fig.3c) and for each recorded risk passes to the WSRA Proxy its risk information (Fig.3d). The CSP then invokes the Web Service risk assessment from the ISL, according to information received from the RAClouds (Fig.3d). The Web Service risk assessment is performed by the ISL and returns the quantification of threat or vulnerability according to the parameters passed by the CSP (Fig.3d). The steps "c" and "d" in Figure 3 are executed for each record in RDL Repository.

.

After obtaining a quantification of all impacts (consulting information assets RDLs, Fig.3e), the RAClouds is able to perform the risk calculation. Therefore, all records of quantification of threats, vulnerabilities and impacts of information assets are correlated and returned to the CC as a result of risk RDL (Fig.3f), according to the example shown in figure 5.

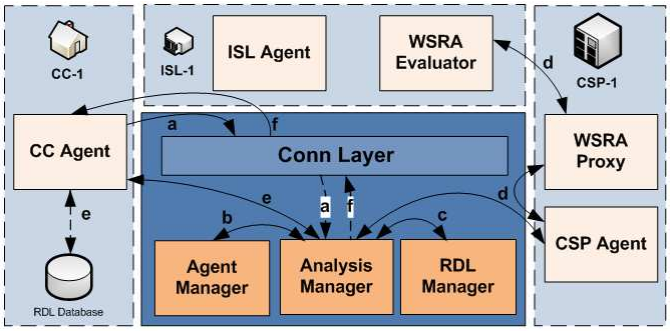

Figure 3. RAClouds assessment phase.

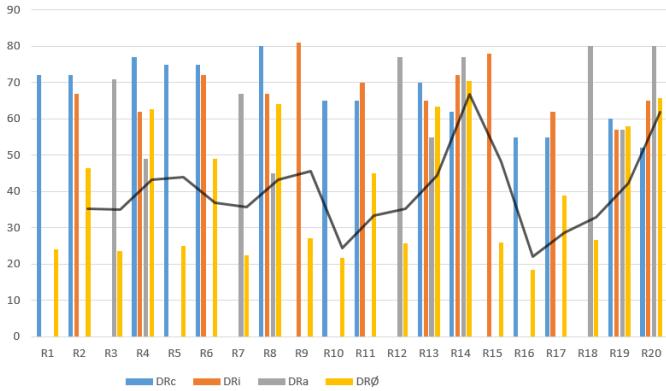

Figure 4. Evaluation of risk.

IV. RESULTS AND DISCUSSION

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

In the risk of specification phase, 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, the WSRAs Proxy and WSRAs were performed, quantifing each vulnerability and threat record. 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 4 shows the result of calculation of risk for the 20 risk scenarios (R1 to R20) specified in the prototype.

The lower risk identified was the R16 risk scenario, with risk of 18.33%. 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 R14,

with risk of 70.33%. This risk scenario specifies as information asset the e-mail service, as vulnerability the weak encryption protocol and as threat the DDoS.

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 of the deficiency in the adherence criterion 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 capable of defining the impacts and is also 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.

The RACloud model works to reduce the deficiency in the scope criterion 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 the deficiency in the independence of the results criretions comes from the fact that in 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 to 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 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.

The figure below shows the evaluation RDL to the risks discussed in this section .

```
▼<risk_item DRa="0" DRc="55" DRi="0" id="16">
   <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help desk</informationAsset>
  ▼<event Pa="0" Pc="70" Pi="0" id="9593@459">
    ▼<vulnerability DDa="30" DDc="70" DDi="50" id="9593">
       Apache CloudStack before 4.3.2 allow obtain private key
     </vulnerability>
     <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
   </event>
 </risk_item>
▼<risk_item DRa="77" DRc="62" DRi="72" id="14">
   <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de Pedidos</informationAsset>
  ▼<event Pa="75" Pc="65" Pi="60" id="0412@443">
    ▼<vulnerability DDa="90" DDc="40" DDi="30" id="0412">
       Oracle Java SE 6u85 vulnerability related to JAX-WS
     </vulnerability>
     <threat DEa="60" DEc="90" DEi="90" id="443">Spoofing of user</threat>
   </event>
 </risk item>
```

Figure 5. Result Risk RDL.

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 of confidence from the 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] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145 (draft), Jan. 2011, pp. 1–7.

[2] H. Yu et al., “Cloud computing and security challenges”. ACM-SE '12: Proceedings of the 50th Annual Southeast Regional Conference. March 2012.

[3] C. Wang et al., "Toward Secure and Dependable Storage Services in Cloud Computing," *Services Computing, IEEE Transactions on* , vol.5, no.2, pp.220,232, April-June 2012 doi: 10.1109/TSC.2011.24.

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

[5] 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.

[6] Bleikertz, S.; Mastelic, T.; Pape, S.; Pieters, W.; Dimkov, T., “Defining The Cloud Battlefield - Supporting Security Assessments By Cloud Customers”, Cloud Engineering (Ic2e), 2013 Ieee International Conference On, Digital Object Identifier: 10.1109/Ic2e.2013.31, Publication Year: 2013, Page(S): 78- 87.

[7] 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.

[8] O. Mirkovic, “Security Evaluation In Cloud”, Information & Communication Technology Electronics & Microelectronics (Mipro), 2013 36th International Convention On, Publication Year: 2013 , Page(S): 1088-1093.

[9] Alebrahim, A.; Hatebur, D.; Goeke, L., "Pattern-Based And Iso 27001 Compliant Risk Analysis For Cloud Systems," Evolving Security And Privacy Requirements Engineering (Espre), 2014 Ieee 1st Workshop On , Vol., No., Pp.42,47, 25-25 Aug. 2014.

[10] Cayirci, E.; Garaga, A.; Santana De Oliveira, A.; Roudier, Y., "A Cloud Adoption Risk Assessment Model," Utility And Cloud Computing (Ucc), 2014 Ieee/Acm 7th International Conference On , Vol., No., Pp.908,913, 8-11 Dec. 2014.

[11] M Madria, S.; Sen, A., "Offline Risk Assessment Of Cloud Service Providers," Cloud Computing, Ieee , Vol.2, No.3, Pp.50,57, May-June 2015. Doi: 10.1109/Mcc.2015.63.

[12] Gupta, S.; Muntes-Mulero, V.; Matthews, P.; Dominiak, J.; Omerovic, A.; Aranda, J.; Seycek, S., "Risk-Driven Framework For Decision Support In Cloud Service Selection," Cluster, Cloud And Grid Computing (Ccgrid), 2015 15th Ieee/Acm International Symposium On , Vol., No., Pp.545,554, 4-7 May 2015. Doi: 10.1109/Ccgrid.2015.111

[13] Silva, P. F.; Westphall, C. B.; Westphall, C. M.; Mattos, M. M. “An Architecture For Risk Analysis In Cloud”. The Tenth International Conference On Networking And Services. Infosys 2014. Icns 2014.Charmonix, France. 2014.

[14] Silva, P. F.; Westphall, C. B.; Westphall, C. M.; Mattos, M. M. “Model For Cloud Computing Risk Analysis”. The Fourteenth International Conference On Networks. Icn 2015. Barcelona, Espanha. 2015.