An Architecture for Risk Analysis in Cloud

Paulo F. Silva[1,2], Carlos B. Westphall[1], Carla M. Westphall[1], Mauro M. Mattos[2], Daniel Ricardo dos Santos[1]

[1]Networks and Management Laboratory
Post-Graduate Program in Computer Science
Federal University of Santa Catarina, Florianópolis, Brazil
{westphal, carlamw, danielricardo.santos}@inf.ufsc.br,

[2]Development and Transfer Technology Laboratory
Regional University of Blumenau, Blumenau, Brazil
{paulofernando, mattos}@furb.br

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; information security; risk analysis;

I. INTRODUCTION

Cloud computing brings several challenges for the scientific community of information security. Major challenges cited are [1] [2] [3] [4]: data privacy of users, protection against external and internal threats, identity management, virtualization management, governance and regulatory compliance, Service Level Agreement (SLA) management and trust gaps.

A strategy to meet the challenges of information security in cloud computing is the risk analysis [5]. Several papers have worked on risk analysis on cloud computing [6] [7] [8] [9] [10] [11] [12], focusing on specific techniques for identifying and assessing risks.

Current solutions for risk analysis in cloud computing does not specify the agents involved and their responsibilities during the implementation of risk analysis. This uncertainty creates deficiencies in risk analysis, as:

- Deficiency in scope: occurs when the selection of security requirements is performed by the Cloud Service Provider (CSP) or an agent without sufficient knowledge. The CSP can specify security requirements vicious in their own environment, thus defrauding the results of the risk analysis. An agent unprepared may specify wrong or insufficient requirements, thus creating an incorrect risk analysis;
- Deficiency in adhesion to Cloud Consumer (CC): occurs when the agent responsible for defining impacts ignores the technological environment and business nature of the CC. In this case, the specification can disregard the impact scenarios relevant to the CC or overestimate scenarios that are not relevant, thus creating an incorrect risk assessment;
- Deficiency of reliable results: occurs when the quantification of the probabilities and impacts is performed by an agent who is interested in minimizing the results of the risk analysis. For example, if the analysis is performed solely by CSP, he can soften the requirements and evaluation of impacts, thus generating a satisfactory result for the CC. However, such results are incorrect.

The deficiencies outlined above can generate a lack of trust on the part of CCs in relation to risk assessments, as in current models where CSPs are performing their own risk analysis, without the participation of CCs or any other external agent.

This paper proposes a model of shared responsibilities for risk analysis in cloud computing environments. The proposed model aims to define the agents involved in the risk analysis, their responsibilities, language for specifying risks and a protocol for communication among agents.

The rest of this paper is organised as follows. Section 2 discusses related works. The proposed model is presented in Section 3. Section 4 discusses the results. The conclusion and future works are presented on Section 5.

II. RELATED WORK

Architectures for risk analysis in cloud computing are presented in [7][8][9][10][11][12].

Paper [7] shows an architecture called SecAgreement which enables the management of security metrics between CSPs and CCs. A SLA for risk management in the cloud is presented by [8]. Reference [9] discusses the analysis of risk in cloud computing environments based on ISO 27001 and proposes a model for assessing security in cloud computing.

Paper [10] presents an architecture that defines levels of security from the risk of each service offered by CSP.

Reference [11] portrays a model for security testing in cloud computing environments based on a risk analysis of these environments. Paper [12] explores the risk analysis in the cloud using techniques based on intrusion attack-defense trees and graphs.

The related works presented above discuss risk analysis of requirements or specific scenarios on cloud computing, but they don't address the definition of the agents involved and their interactions during the risk analysis.

III. THE PROPOSED ARCHITECTURE

The proposed architecture defines the sharing of responsibilities between three agents during the risk analysis. Information Security Labs (ISL) is an agent that represents a public or private entity which specializes on information security, eg an academic or private laboratory. The CC is an agent that represents the entity that is hosting their information assets in the cloud. The CSP is an agent that represents the entity being analyzed.

The three agents defined by the proposed architecture divide the responsibilities of running a risk analysis, according to the concepts defined by ISO 27005. In this context threats exploit vulnerabilities to generate impacts on information assets [5].

A risk analysis works with many variables. The variables used on proposed architecture are: (i) DE – Degree of Exposure, defines how the cloud environment is exposed to certain external or internal threat, (ii) DD – Degree of Disability, defines the extent to which the cloud environment is vulnerable to a particular security requirement, (iii) P – Probability, defines the probability of an incident occurrence, ie, a threat exploiting a vulnerability (iv) I – Impact, defines the potential loss in the event of a security incident, (v) DR – Degree of Risk, defines the degree of risk for a given scenario of a security incident.

The risk analysis of the proposed model is organized on two well-defined phases: risk specification and risk assessment.

The risk specification phase defines threats, vulnerabilities and information assets that will compose the risk analysis. At this stage it is also defined how to quantify the threats, vulnerabilities and assets specified.

The risk assessment stage comprises the quantification of the variables DE, DD and I, for threats, vulnerabilities and information assets, respectively. In this phase the quantification of variables of P and DR for each incident scenario is also performed (a combination of threat, vulnerability and asset information).

Figure 1 illustrates the flow of interactions between components of the architecture and the ISL, CSP and CC agents in the risk specification phase. Initially each agent must register on their respective registry component (Fig. 1 a, b, c). After their registration the ISL is responsible for identifying threats and vulnerabilities in cloud computing environments. Then the ISL specifies how to quantify threats and vulnerabilities.

The architecture provides a language for the specification of risk, the RDL – Risk Definition Language. This language is used by ISL to specify threats and vulnerabilities. The RDL is specified in XML and contains information such as: risk ID; ISL ID; threat and \ or vulnerability ID and reference to a WSRA – Web Service Risk Analyzer. The WSRA is a Web Service specified by ISL to perform the quantify the Degree of Disability (DD) and Degree of Exposure (DE).

After developing its RDLs and WSRAs the ISL exports the records for the RDLs repository (Fig.1-d) and publishes WSRAs.

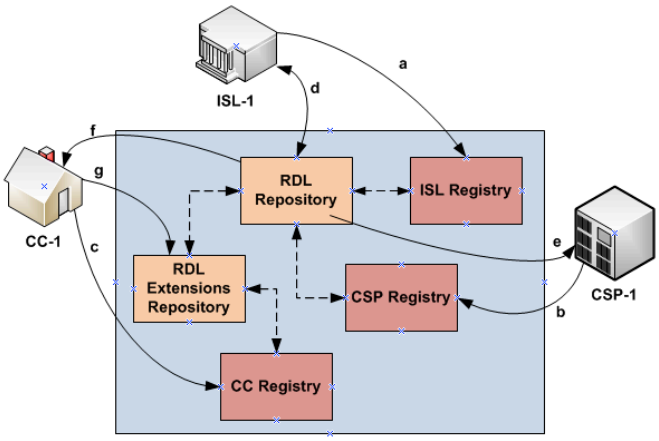

Figure 1. Risk specification phase.

The responsibility of the CSP on the specification phase of risk consists in importing RDLs and implementation of calls to WSRAs (Fig.1-e).

ISL is responsible for the correct identification of threats and vulnerabilities. CSP is responsible for the correct execution of the quantification of threats and vulnerability. The CC agent is responsible for the identification of information assets and the quantification of impact, as this is the most fitting agent to express the cost of an information security incident.

In order to perform the identification of an information asset and quantifying an impact on this asset a CC must import the RDLs (Fig.1f) and extend them including information on information assets and their impacts.

The method of quantification of impacts may be static or dynamic. In the static method the CC determines a fixed value for the impact and in the dynamic method the CC specifies a Web Service to quantify the impact. After specifying their information assets and their impacts the CC exports the extension to the RDL Extensions Repository (Fig.1g).

Figure 2 illustrates the flow of interactions between the components of the proposed architecture and the ISL, CSP and CC agents during risk assessment.

The Risk Analysis component coordinates the interaction between external agents and other internal components of the proposed architecture. The RDL Repository and RDL Extensions Repository components store records of threats and vulnerabilities of ISLs and information assets of the CC, respectively. The RA Processor component is responsible for establishing the relationships between information assets,

threats and vulnerabilities, as well as performing the calculation of risk.

The CC, ISL and CSP agents present the components Impacts Evaluation, Evaluation WSRA and CSP Proxy respectively. Impacts Evaluation is a component that contains the Web Services for dynamic definition of impacts or tables for static impacts. Evaluation WSRA is a component that contains the Web Services assessment of threats or vulnerabilities identified by an ISL. CSP is a proxy component deployed in CSP to perform the call of the WSRAs.

The risk assessment begins with the CC informing the CSP to be analyzed (Fig.2a). Then the Risk Analysis component queries the RDL repository (Fig.2b) and performs a call of the CSP Proxy component passing the information about each risk (Fig.2c).

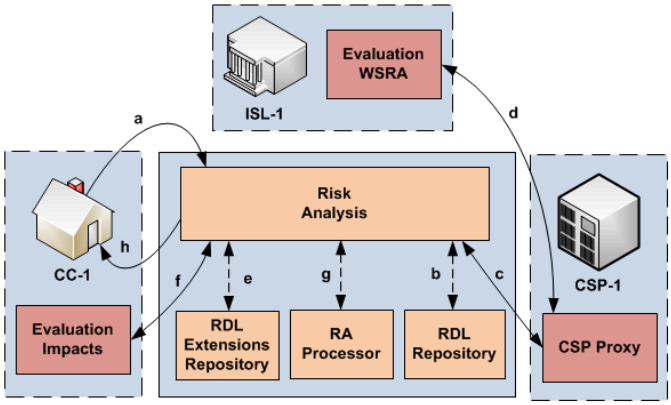

Figure 2. Risk assessment phase.

Based on each RDL received the CSP performs a call of the WSRA (Fig.2d). The WSRA is run by ISL and returns the quantification of the threat (DE - Degree of Exposure) or vulnerability (DD - Degree of Disability). Then the quantification of the threat or vulnerability is returned to the Risk Analysis component (Fig.2c) and stored. The steps "b", "c" and "d" in Figure 2 are executed for each RDL in RDL Repository.

The quantification of impacts as defined by the CC starts after the quantification of all threats and vulnerabilities. The Risk Analysis component queries the RDL Extensions Repository (Fig.2e) performs a call of the Evaluation Impacts component for the quantification of the impact (I - Impact) (Fig.2f).

After obtaining the quantification of all impacts the Risk Analysis component is able to perform the calculation of the probability and risk. Therefore, all records showing the quantification of threats, vulnerabilities and impacts are sent to the RA Processor component (Fig.2g).

The RA Processor component sets the valid relationships between information assets, threats and vulnerabilities, and performs the calculation of the probability (P - Probability) and of the risk (DR – Degree of Risk) through the variables DD, DE and I previously quantified.

After calculation of risk analysis the result is returned in XML for Risk Analysis component (Fig.2g), and transferred to CC (Fig.2h).

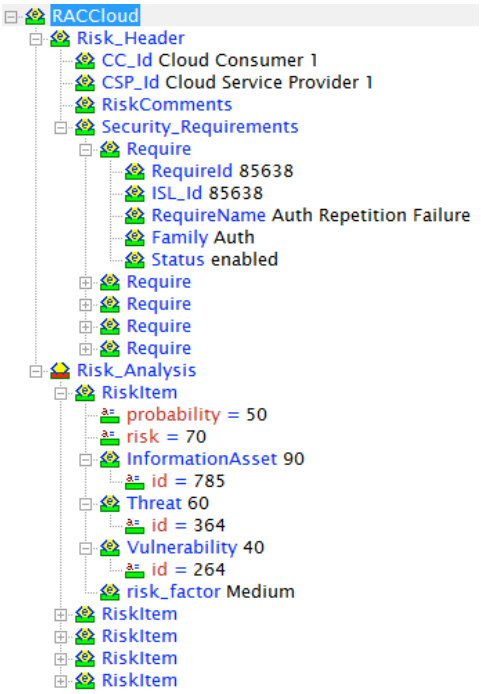

Figure 3. Risk Analysis result.

The XML resulting of the risk analysis (Fig. 3) contains the ID of the CC and CSP agents, and a list of security requirements that were defined by ISLs. Each requirement contains its ID and the ID of the ISL that created it. The XML resulting still contains the probability (P) and the degree of risk (DR) which was calculated for each requirement and the results of variables, DE, DD and I.

IV. Results and Discussion

With the information from the risk analysis the CC may decide to allocate or not their information assets in a particular CSP.

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

The reduction in adhesion deficiency occurs when the proposed model includes the CC as a key agent in the process of risk analysis. The CC agent has an important role in risk analysis, defining information assets and quantifying impacts on these assets.

The CC is the most suitable agent for the definition of impacts. It is the agent which best understands the relevance of each information asset within its area of expertise. CSP and ISL agents are not able to identify or quantify the impacts on information assets. They are not experts in the business of CC.

The proposed model acts to reduce the deficiency in scope by adding the ISL agent. ISL is an agent specializing in information security. It is the entity best suited to define

security requirements, threats and vulnerabilities (specification of the RDLs), as well as to define how to qualify such threats and vulnerabilities (specification of the WSRAs).

The proposed model acts on the deficiency of reliable results because in our model the CSP has more restricted responsibilities than in models traditionally presented by related works.

Traditionally, the CSP is responsible for defining security requirements and the tests that are applied to evaluate the risk of their own environment. In this scenario, the risk assessment can be smoothed by CSP. The inclusion of the ISL agent removes responsibilities which are traditionally assigned to the CSP, such as the identification and quantification of threats and vulnerabilities, thus the result of the risk analysis more reliable.

The proposed model allows multiple ISLs defining RDLs and WSRAs jointly (Fig. 1). Thus, the definitions of risk can come from different sources and can be constantly updated in a dynamic and collaborative way, forming a large and independent base of risk definition for cloud.

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

Related works of risk analysis in the cloud do not consider the role of the CC agent on risk analysis. These works usually focus on the vulnerability assessment by the CSP, without considering the impact it will have on the vulnerability of the different information assets of the CC. The proposed model assigns the responsibilities of the identification and quantification of impact to the CC. Thus, the performing of risk analysis is shared among different agents, so the responsibility for quantifying the variables of risk analysis is not centered on a specific agent.

The CSP is the agent that will be analyzed; therefore it is not able to set any of the variables of the risk analysis, as this could make the results of risk analysis incorrect. The role of CSP is only to inform the data requested by ISL, so to the own ISL performs the quantification of each information security requirement.

A CC can perform analysis on multiple CSPs before deciding to purchase a cloud service. It is also possible to perform periodic reviews of its current provider and compare them with other providers in the market, choosing to change CSP or not.

V. CONCLUSION

This paper presented a model of shared responsibilities for risk analysis in cloud computing environments. In addition to the traditional CC and CSP agents the model adds the ISL agent, which is responsible for identifying and specifying the security requirements.

The model presented in this paper is an initiative to allow the CC can perform the risk analysis on its current or future CSP, and this risk analysis is broad, current, unbiased and reliable.

The characteristics presented in this article aim at generating a more reliable risk analysis for CC, so that it can choose its CSP based on more solid information.

Several papers on cloud computing indicate the lack of trust from CC to CSP as a relevant factor in avoiding the purchase of cloud computing services. A risk analysis can act to reduce or eliminate this suspicion and boost the acquisition of cloud computing services.

The presented model performs a free and reliable risk analysis, because the analysis is not centered in the CSP. The identification and quantification of threats and vulnerabilities are carried out collaboratively by several laboratories. Safety and impact on information assets are quantified by the CC.

The risk analysis of the proposed model is broad, because the security requirements are defined by specialized laboratories and the CC itself defines and quantifies their information assets. It is dynamic, because the various ISLs can modify their security requirements for considering new vulnerabilities in future risk analyzes.

This work opens possibilities for the development of future research. There is a need for research on the reliability of the data reported between CSP and ISL during risk analysis. The RDL - Risk Definition Language can be further explored in specific jobs. Further research should be done on the inferences on the results of risk analysis. These inferences can help all stakeholders in understanding the causes of incidents and their solutions. Finally, there is the need to extend this work in order that the proposed model can also suggest the controls or countermeasures to the CSPs.

REFERENCES

[1] M. K. Srinivasan et al., “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.

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

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

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

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

[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.,

pp.121,123, 15-18 June 2012 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., pp.133-140, 24-29 June 2012 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., pp.1484-1489, 21-25 May 2012.

[10] J. Chen, Y, Wang and X. Wang, "On-Demand Security Architecture for Cloud Computing," *Computer*, IEEE, vol.45, no.7, pp.73,78, July 2012 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., pp.47,56, 20-22 June 2012 doi: 10.1109/SERE-C.2012.11.

[12] P. Wang et al., "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., pp.106-111, 24-26 April 2012.