A Trust Model for Cloud Computing environment

Teófilo Teixeira Branco and Henrique Santos
University of Minho, Guimarães, Portugal
teofilotb@hotmail.com
hsantos@dsi.uminho.pt

Abstract: This paper presents a proposal for a management model based on reliability requirements concerning Cloud Computing (CC). The proposal was based on a literature review focused on the problems, challenges and underway studies related to the safety and reliability of Information Systems (IS) in this technological environment. This literature review examined the existing obstacles and challenges from the point of view of respected authors on the subject. The main issues are addressed and structured as a model, called "Trust Model for Cloud Computing environment". This is a proactive proposal that purposes to organize and discuss management solutions for the CC environment, aiming improved reliability of the IS applications operation, for both providers and their customers. On the other hand and central to trust, one of the CC challenges is the development of models for mutual audit management agreements, so that a formal relationship can be established involving the relevant legal responsibilities. To establish and control the appropriate contractual requirements, it is necessary to adopt technologies that can collect the data needed to inform risk decisions, such as access usage, security controls, location and other references related to the use of the service. In this process, the cloud service providers and consumers themselves must have metrics and controls to support cloud-use management in compliance with the SLAs agreed between the parties. The organization of these studies and its dissemination in the market as a conceptual model that is able to establish parameters to regulate a reliable relation between provider and user of IT services in CC environment is an interesting instrument to guide providers, developers and users in order to provide services and secure and reliable applications.

Keywords: Cloud computing, information systems, information security, trust model, service level agreement (sla), audit management

1. Introduction

This work aims to organize, by the use of a literature review and discussion of controversial points on the existing obstacles to the full use of information systems Cloud Computing environment, from the viewpoint of reliability.

The new technology of Cloud Computing (CC) causes doubts and misgivings about the advisability of the adoption of this technology, particularly with respect to information security. Although promising, this technology still needs to resolve several points of vulnerability (Grobauer, Walloschek, & Stocker, 2011). From the perception of uncertainty hovering over the CC environment about the safety in the operation of applications and store data, the author saw an opportunity to treating

these issues, starting initially by a literature review to elucidate the main controversial points and in discussion currently.

From this literature review, we propose a model of CC environmental management that aims to organize and check the requirements for the information systems operate reliably and with safety on a CC environment. These factors are essential for this technology to produce good results for the operation of information systems, from the perspective of resources rationalization, such as its effective use and data store.

This study wishes to collaborate with CC environment providers, application developers for CC and users clients to guide how you can make reliable the Cloud environment to be used by organizations to store their data. The development and deepening of this study open perspectives for future work, such as the development of a framework for determining the level of reputation of service providers and application developers in CC environment.

2. Literature review

A good literature review creates a solid foundation for the advancement of knowledge. This will facilitate the development of the theory, closed areas where there is a plethora of research and discover areas where it is necessary to look into and provides an important contribution to the establishment of guidelines for future research that are fundamental to the strengthening in the area of the study (Webster & Watson, 2002).

First, we tried to identify the main risks involved in Cloud Computing technology, notably related to implementation of information systems and their data. In this sense, a literature survey was conducted in order to:

- Characterize the works presented on the issue at hand, identifying the relevant points, emphasized needs and the views presented;
- Critically list the issues involved in relation to the opinions of surveyed authors, in order to define the points of the author's interest;
- Highlight the assumptions and requirements for the use and availability of IS applications in the Cloud Computing environment.

The aim of the literature search was to find works that dealt the following starting questions:

- What are the vulnerabilities and risks involved in the operation of systems in the Cloud Computing environment?
- Which ones can be checked at delivery and compliance of IT services in Cloud Computing environment?

We selected the following sources according to the following criteria of priority:

- Publication of articles in scientific journals;
- Theses and dissertations;
- International conference proceedings.

In search of scientific journals, consultation was held in SCImago Journal & Country Rank (http://www.scimagojr.com) to check the visibility of magazines (SJR). It was given more attention to the qualitative aspects, taking into account the number of citations of these articles in order to select those that have the greatest impact. The following Journals were selected based on the magazine's name, description, category and study area.

- MIS Quarterly: Management Information Systems; Information Systems Research;
- ACM Transactions on Database Systems;
- Robotics and Computer-Integrated Manufacturing;
- Information Systems Journal;
- Journal of the Association of Information Systems;
- International Journal of Project Management;
- IEEE Transactions on Engineering Management;
- Information Systems Management;
- Project Management Journal;
- Enterprise Information Systems;
- Journal of Computer Information Systems;
- Information and Organization; Information Systems Management.

Bearing in mind the scope of the research, the articles were preferentially searched in the following databases taking into account the wide range of published articles related to the subject under study:

- Elsevier Science Direct (http://www.sciencedirect.com);
- IEEE Xplore (http://ieeexplore.ieee.org/);
- ACM Digital Library (http://www.portal.acm.org/dl.cfm);

- Springer Link (https://www.link.springer.com);

We also held consultations in Web of Science (http://workinfo.com), Scopus (http://www.scopus.com) and J. Stor (http://www.jstor.org). We emphasize that the articles were selected from the title, abstract and keywords. From these sources, we prioritized references produced less than five years ago. The works were selected taking into account criteria such as appropriateness to the theme of this work, relevant publications, academic production of the authors and citations of their work.

From the researched material, a preliminary reading was held based on the summaries of the articles in order to select those that are within the scope of the research. Thus, literature review was conducted, initially, depending on the title, summary and key words, but, in some cases, due to the inadequacy of the article content to the theme under investigation, some of the articles were not included in the bibliography. Results were useful to support the proposal of the "trust model" which deals with the proposition of an operational management model of the CC environment, structuring the reliability requirements for it.

3. Challenges related to reliability in cloud computing environment

Despite the advantages in the business perspective, cloud computing also presents challenges, particularly regarding the distrust of users to put their data on computers that do not have control. The Internet presents itself as a hostile environment and this becomes critical when you have confidential data traveling between terminals and Cloud servers (Mirashe & Kalyankar, 2010).

Either executives and information technology technicians, it becomes a challenge to figure out how Cloud Computing can be trusted and provide the security level required for its full operation. In this sense, there is a growing concern for safety. The level of concern varies from compliances with regulations to the issue of security in dealing with end users (Che, Duan, Zhang, & Fan, 2011).

The main approaches on information security area do not make any distinction of the environment to which they are applied, which is equivalent to deduce that the concerns and safety standards that apply to traditional systems should also be adopted for the Cloud Computing environment. In this sense, traditional approaches to information security are ruled by certifications that aims to deepen the study of the standards governing each one of the focus-related subjects. This assumption implies considering that the Cloud Computing environment, beyond traditional safety standards, still has to adopt security measures for the environment itself (Chen, Paxson, & Katz, 2010a).

Currently, several organizations have been working to develop specific safety standards for cloud computing, taking these surveys for a large number of areas including auditing, applications, encryption, governance, network security, risk management, and storage virtualization. Even after establishing who will take responsibility for the custody of the information, their owners remain the contracting organizations. At that juncture, there is the need for providers to prove they are able to keep data safe as well as to make available means for the contractor can check the administration of the offered computing environment at any time.

Below, we discuss the main points of view of the authors surveyed over the three research questions listed earlier in this article.

4. Vulnerabilities in the cloud computing (CC) environment

Vulnerabilities may be deemed security-related errors that cause weakening or removing a resistance to environment. Attackers can exploit vulnerabilities using techniques according to their ability. Cloud Computing environment has intrinsic vulnerabilities to technology that may be considered relevant, as listed below (Grobauer et al., 2011):

- The use of VPNs (Virtual Private Network). Despite the isolation provided by virtualization, many questions still remain open in order to compose a list of desired requirements to Cloud Computing systems;
- A secure encryption alone can solve a series of security problems. However, the concern is precisely the use of a bad encryption, which can be broken. The use of an outdated encryption or if it is not updated may become a great risk;
- Section issues on the HTTP protocol. Web application technologies require session state. Many techniques implement session handling and, if these implementations are flawed, it can compromise the entire environment.

Regarding the characteristic of the CC environment, some vulnerabilities are from services that are provided (self-service on-demand, network access to any IT platform, sharing resources, rapid elasticity and measurement of the service) (Grobauer et al., 2011):

- Unauthorized access to the management interface. Unauthorized access to the management interface is thus a particularly relevant vulnerability to cloud systems: there is a much greater possibility that unauthorized access may occur in CC environment than in traditional systems, where the management functionality is accessible only for some administrators;

- Vulnerabilities in Internet protocol. The typical cloud of ubiquitous access network means that cloud services are accessed over the network using standard protocols. In most cases, the network is the Internet, which should be considered unreliable;
- Data recovery vulnerability. The characteristic of elasticity in the cloud implies that the resources allocated to a user will be relocated to a different user at a later time. For memory resources or storage, it can therefore be possible to recover the data recorded by a previous user;
- Measurement and charging. The measurement feature in the cloud means that any cloud service has a measurement capability at a level of abstraction appropriate to the type of service (such as storage, processing, and active user accounts). Measurement data is used to optimize service delivery and billing. In this case, vulnerabilities are related to handling of these data, where they may come to be changed and do not represent reality anymore.

Although the development of technical and technological tools that can address these vulnerabilities are in progress, it is clear that the biggest problems refer to the lack of management control or a misapplication of them.

5. Verification of the provision and adequacy of IT services in cloud computing environments: the audit on the management of service agreements

A Service Level Agreement (SLA) is a contract between a supplier of IT services and a customer specifying, in general and often in measurable terms, what services the provider will pay. Service levels are set at the beginning of any hiring ratio of IT services and are used to measure and monitor the performance of a supplier (Armbrust, Fox, Griffith, & Joseph, 2009).

In a Cloud Computing environment, one of the challenges is to develop mutual auditing models to management agreements (SLAs), with the aim of establishing a trust between the contractor and the contracted, thus consolidating the use of this environment through a formal relationship, involving relevant legal responsibilities (Chen, Paxson, & Katz, 2010b).

To establish and control the appropriate contractual requirements, it is necessary to adopt technologies capable of collecting the necessary data to inform risk decisions, such as access usage, security controls, location and other references relating to use of the service. In the process, cloud service providers and consumers themselves must have metrics and controls to aid the management of cloud use in compliance

with SLAs (Service Level Agreement) agreed between the parties (Weinhardt et al., 2009).

To perform a verification of compliance of the computing environment, audits are carried out. The audit focuses its activity primarily on the evaluation of governance processes, risk management and control and, in a complementary way, the assessment of the main activities, processes and products of the organization, especially those considered vital to achieve the strategic objectives. With this focus, the audit aims to provide relative safety to stakeholders. The audit systems therefore involves the evaluation of information systems and technology resources that comprise the process of generation, storage and availability of information. In this sense, its function is to promote fitness, review, evaluation and recommendations for improvement of internal controls in any information systems of the company, and to estimate the use of human, material and technology resources involved in the processing of these (M. Kanchana, Sk. Nazar Hussain, Kumar, & Praveen, 2013).

Because the auditors are not yet familiar with the level of complexity of Cloud Computing and about what to audit, it is necessary to take into consideration the following aspects:

- regulatory applicability to cloud use in question;
- the division of responsibilities between the service provider and the cloud customer agreed in SLAs (Jensen, Schwenk, Gruschka, Lo Iacono, & Ieee, 2009). In this regard, it is relevant to the search for means to facilitate mutual audit, complete and bilateral, adapting them to each contracted service level (Chen et al., 2010b).

6. A "Trust Model" for Management of Reliability in the use of Cloud Computing Environment

Confidence concepts have been used by many researchers who have investigated the various challenges of trust involving the management of information systems. The amount of literature related to this subject is increasing as researchers continue to discuss different issues and propose innovative models to solve the problems that arise when two parties need to establish business relationship between them (Alhamad, Dillon, & Chang, 2010). We have integrated some of these works to present a new solution in order to implement a model in practice.

Establishing a model containing the assumptions related to the principles of information security, in line with the main challenges pointed out by experts in this area could be useful as a guiding tool for a reliability proposal of use of a cloud

environment, if it may be easy to understand and meet conditions to be adopted by providers of IT services in Cloud Computing environment.

A management model giving orientations for the processes necessary to adapt technologies, as well as indications of appropriate standards and certifications for security of each type of contract, could constitute a tool that would facilitate verification of different conditions in the provision of services in Cloud Computing. Such a model could give to the IT environment providers and Cloud application developers the opportunity to obtain a better qualification for determining a level of trust that give to their user clients of IT products in the Cloud. This management model, called "trust model" consists of eight areas of interest, as listed in Figure 1:

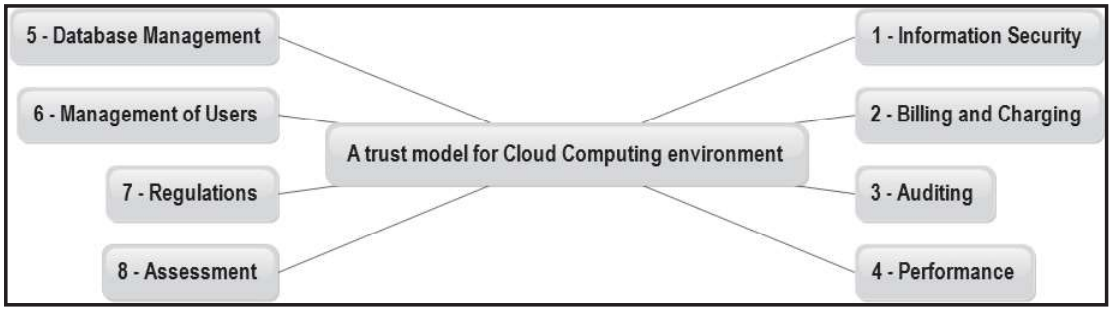

Figure 1: The eight areas of "trust model" for Cloud Computing environment

Next, the components that make up each of the areas of interest to the operational management model, called "Trust Model", are briefly described.

6.1 Information Security

Information security deals with the principles of confidentiality, integrity and availability that systems must preserve. Information Systems in the Cloud Computing Environment follow the same standards and certifications regardless of the type and topology of their applications.

According to ISO/IEC 17024 standard, which deals with the approaches in the field of Information Security, there are ten areas to be considered in IT environments to be worked, which should be taken into account in a management model for Cloud Computing environment in following aspects:

- Access control - addresses on the technology used and the access policy to CC environment;

- Telecommunications and network security - Describes the standards used for the safety of environmental infrastructure (IaaS), involving technology, equipment and settings employed;
- Information Security Governance – involves the definition of safety plans, control processes and verification of operational procedures;
- Security in Software Development - Details the application development methodology, development of layers and safety rules to be followed by developers;
- Encryption - describes the features for the code in use, versioning and update date;
- Architecture and Design Security - Define the security application framework distributed by the technology employed;
- Operations Security - Set standards and actions to be performed in the operating environment;
- Business continuity and disaster recovery planning - Contains the contingency plan of operations;
- Legal, regulations, compliance and investigations - legal basement related to legislation, research methods and compliance standards to be followed;
- Physical security (environmental) - Details the security requirements to access the facilities of the provider and its technology.

6.2 Billing and Charging

This component addresses the methods and tools of charging the service provided. Such control mechanisms must be appropriate to consider the nature of resources consumed, the quantity demanded of these resources and the time of use. The billing must be automatic, as well as the application of requisition of these resources from the environment of the user. Ideally, there is no human intervention in the process. The ways to make this technology available should be guided in the following aspects:

- Nature of the available resources - Specifies how the availability of technological resources used by user-clients in a space of time is controlled;
- Availability of resources (quantity) - Details the units employed in the definition of quantitative parameters;
- Metrics of use - Specifies the calculations used to measure the consumption of resources;

- Fee schedule - Composes the rules adopted for pricing.

6.3 Auditing

A key area in the aspect of security and verification of the agreement contractual compliance refers to the possibility of mutual IT audit between supplier and contractor. In Cloud Computing, providers and users need to have mutual auditing tools, transparently, so that the use of the services can be certified, thus establishing mutual trust between the parties (M. Kanchana et al., 2013).

Mutual audit shall provide the ability to the user and to the provider to track the actions performed on the environment, its operations and interventions in applications or information systems. A major challenge is to make these control tools available without loss of performance, since the Cloud environment is provided by a combination of complex technologies (Chen et al., 2010b).

This area of interest is represented by the following aspects:

- Types and SLAs levels - details the arrangements of standards established for marketing users;
- Common topics of interest - Define the scope and coverage to accomplish audits;
- Means of collecting available information – Define the sources of data collection to perform the audit.

The prospect of integration through the adoption of Cloud Computing audit with the security service management models if well-structured, are likely to increase the customer's own security environment in support of plans continuity and disaster recovery. These features also allow the detection of data confidentiality risks with the provider of cloud computing by making possible to share these risks.

6.4 Performance

The performance of the service usage is a major factor for acceptance of the technology by users. Since Internet access is required for access to the Cloud environment, it is important to implement technologies that can record the following domains of performance measurement:

- Link Speed - the environment access requirements, such as minimum broadband speed and measuring techniques used for verification;
- Processing time - techniques used for environmental performance measurement, such as processing speed and application response time;

- Performance control - Equipment and software used for calculation.

6.5 Database Management

Implementation of data distribution techniques for the IS applications are an important concern of experts on either data integrity and storage and recovery. The computing environment should subsidize all the conditions so that the principles inherent in the management of databases are met, since they are the most precious asset of the user.

In this regard, the following fields of study are required:

- Allocation techniques - Definition of algorithms and rules used for distribution of customer data in the data center;
- Mechanisms for storage and recovery - Specifies the technology and software used for the storage of data, including backup and recovery of data in queries and other similar operations.

6.6 Management of users

The importance of the role of people within the information security brings concern to this study area, from behaviors that can be considered a risk for maintaining the stability of information systems in IT environments. Being recognized as one of the concerns in the area of information security, actions that allow user education are important to be established a code of conduct between the user and the service provider.

The following aspects are addressed in this component:

- Users profile identification - Policy and form of registration with respect to actions processed in CC environment;
- Disclosure of rules and procedures - The means used to disseminate standards and operational procedures to all users;
- Distance training - The provision of distance training using the Web environment is an important resource in user education and should be encouraged and be available;
- Identification and records of incompatible practices - tools that detect not lawful or risk actions caused by people should allow the registration of these occurrences to specific solution. Contrasting conduct actions must be detected and recorded in different ways.

6.7 Regulations

The regulation is important in order to have a standardization of operating and ethical procedures that aims to protect the technology and the service provided by it.

It is not justified, for instance, that the establishment of more modest values for the use of the environment in the cloud expose users to threats of invasion, exposure or loss of their data. The service must contain minimum safety requirements to be acceptable, providing this way reliability to the technology.

The main aspects of study in this area are:

- Certifications - Definition of basic training requirements and certifications necessary to operationalize the environment, defined by user type (network architect, developer or end user);
- Standardization of procedures - involves the code of ethics to be adopted in the availability, application development and use of CC environment.

6.8 Assessment

The assessment of the model is an important step in order to the implemented actions can be verified through technological tools in addition to allowing the capture of statistical data relating to the environment, being possible to establish more easily the audit team and the performance data of each interest area of the operational management model. In this sense, the aspects of study are:

- Establishing metrics - Formulation and establishment of specific metrics for measuring the use of CC environmental management model;
- Assessment mechanisms - Establishment of mechanisms to ascertain the application of the model and forms of assessment;
- Ascertaining consumer confidence index - Formulation of a "confidence index" that can be used as a reference to assign to the IT service provider or application developer a qualitative "reputation" of the services that he/she is providing.

7. Conclusions

In the search for more efficient control of computing resources, as well as agility and cost savings, Cloud Computing can provide better management of IT resources and operation of information systems more efficiently than the one traditionally used.

It is then appropriate the transition from traditional operating environment to Cloud Computing environment. Bearing in mind the evolution of computing resources and

the problems caused by the operational dependence on IT by organizations, new technologies associated with administrative management techniques bring a more focused approach to the results as operational efficiency, competitiveness and rapid response. This means that the IT area, instead of producing IT services, it is improving the production and consumption of these services consistently, especially with business requirements.

In the literature review, it was found that, although many researchers and companies address issues related to problems of security and reliability in Cloud Computing environment, different approaches and studies are needed to make technology environment stronger.

The organization of these studies, their dissemination in the market in the form of a conceptual model that can establish parameters to regulate a relationship of trust between provider and user of IT services in CC environment, constitutes an interesting instrument to guide providers, developers and users in order to offer services, and secure and reliable applications.

It is expected that this operational management model fosters better management and better Cloud Computing environment management, bringing users, providers and developers the following benefits:

- The possibility of exercising the right to audit, particularly when using a provider for a service in which the customer has to regulate the fulfillment of responsibilities;
- Enable analysis of the compliance scope, making sure that the rules of compliance to which the organization is regulated are being impacted by the practices adopted by the provider of the Cloud Computing services for a given set of applications and data;
- Allow analysis of the security of applications and data. Potential end users of Cloud Computing services will consider which applications and data are being considered to be moved to Cloud Computing services and to what extent they are subject to compliance regulations;
- The compliance with the scope of ISO/IEC 27001/27002 standard. Cloud computing infrastructure should be able to verify if data are being managed in accordance with local and international regulations, with appropriate controls, log collection and reporting;
- Support elements for the development of a framework incorporating tools and technologies for environmental monitoring. With the growing need for data

processing and storage, it is increasingly challenging the data center management, especially in the cloud (Kaufman, 2009). Requirements such as availability of time become prerequisites charged by SLA in order to ensure minimum quality of service.

Mounting a CC environment for simulation and testing assessments of areas of interest listed in the management model referenced in this article is also essential for evaluation of variables and various policies set for the viability of the model.

A complementary study covering other aspects related to the feasibility of mounting an advanced learning environment in Cloud Computing environment, with the contribution of technical and operational resources, coupled with economic factors, schedule and others, will provide a diagnosis on the viability of this ongoing research project.

Acknowledgements

Our thanks to CETNRO ALGORITMI - The research unit of the School of Engineering - University of Minho – Portugal for support of this research project.

References

Alhamad, M., Dillon, T., & Chang, E. (2010). SLA-Based Trust Model for Cloud Computing. doi:10.1109/NBiS.2010.67

Armbrust, M., Fox, A., Griffith, R., & Joseph, A. (2009). Above the clouds: A Berkeley view of cloud computing. University of California, Berkeley, Tech. Rep. UCB, 07–013. Retrieved from http://scholar.google.com/scholar?q=intitle:Above+the+clouds:+A+Berkeley+view+of+cloud+computing#0

Che, J., Duan, Y., Zhang, T., & Fan, J. (2011). Study on the Security Models and Strategies of Cloud Computing. Procedia Engineering, 23, 586–593. doi:10.1016/j.proeng.2011.11.2551

Chen, Y., Paxson, V., & Katz, R. (2010). What's new about cloud computing security. of California, Berkeley Report No. UCB/. Retrieved from http://www.utdallas.edu/~muratk/courses/cloud13s_files/what-is-new-in-cloud-security.pdf

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. IEEE Security & Privacy Magazine, 9(2), 50–57. doi:10.1109/MSP.2010.115

Jensen, M., Schwenk, J., Gruschka, N., Lo Iacono, L., & Ieee. (2009). On Technical Security Issues in Cloud Computing. Cloud: 2009 Ieee International Conference on Cloud Computing. Retrieved from <Go to ISI>://WOS:000275314400015

Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. Ieee Security & Privacy, 7, 61–64 ST – Data Security in the World of Cloud Co. Retrieved from <Go to ISI>://WOS:000268639100011

M. Kanchana, Sk. Nazar Hussain, Kumar, M. K., & Praveen, C. (2013). Preserving Audit of Secure Data Storage Services in Cloud Computing. International Journal of Advanced Research in Computer Science, 4(5), 70–73. Retrieved from http://www.ijarcs.info/?wicket:interface=:3::::

Mirashe, S. P., & Kalyankar, N. V. (2010). Cloud Computing. Communications of the ACM, 51(7), 9. doi:10.1145/358438.349303

Webster, J., & Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. Retrieved January 23, 2015, from https://www.google.com.br/#q=writing+a+literature+review+webster+and+watson+2002

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud Computing – A Classification, Business Models, and Research Directions. Business & Information Systems Engineering, 1(5), 391–399. doi:10.1007/s12599-009-0071-2