A Privacy Maturity Model for Cloud Storage Services

Carlo Marcelo Revoredo da Silva[1], Jose Lutiano Costa da Silva[1], Ricardo Marinho Melo[1], Ricardo Batista Rodrigues[1], Lucien Rocha Lucien[2], Sandro Pereira de Melo[3], Adolfo Colares[4], Vinicius Cardoso Garcia[1]

[1] Informatics Center, CIn, Federal University of Pernambuco, UFPE, Recife, Brazil
{cmrs, jlcs2, rmm, rbr, vcg}@cin.ufpe.br

[2] Computer Networking, Estácio Seama College, Macapá, Brazil {lucien.rocha@estacio.br}

[3] Computer Networking, Bandtec College, São Paulo, Brazil {sandro.melo@bandtec.com.br}

[4] Federal University of Amapá, UNIFAP, Macapá, Brazil {adolfo@unifap.br}

***Abstract* — The purpose of this article is to present a Privacy Maturity Model of services offered by Cloud Computing Providers in the context of Cloud Storage. This study aims to present an overview of the current barriers in these scenarios and present a model based on technical analysis of maturity in these environments. We present the goals to be achieved in this research, as well as the strategies to be pursued to the contents of sensitive data in order to establish a level of effective privacy. Also featuring is planning an architectural model as a prototype, and set in stages as its research and implementation.**

Keywords-component; Cloud Computing, Privacy Maturity Model, Storage;

I. INTRODUCTION

Cloud computing offers consumers reductions as regard the costs of investment in IT infrastructure through its elastic provides features that enable computing power on demand, besides enabling heterogeneous environments, which cooperate with each other in real time [1]. This provides benefits for many models of services. A fair example are the cloud storage providers which benefit by easily providing a high level of scalability according to the need of their users, and also provide their resources in environments outside their areas in which outsource their services [2].

Despite countless advantages, one of the main barriers in adopting this type of solution is the concern of its users with the privacy of theirs stored data, and this concern becomes even more complex when the service is outsourced [2]. Consequently, this concern becomes even more complex when the service is outsourced, creating uncertainty for the users of the contractor about privacy of sensitive data from their end users.

II. PRIVACY FOR CLOUD STORAGE SERVICES

Thus, to solve the problems in this context, 3 questions arise about these concerns: (i) How to identify a particular data is considerably sensitive? (ii) What strategies should be exercised to protect access to the contents of sensitive data in these environments? (iii) How to establish a level of privacy that meets the needs of the users?

Based on (i) the concern about the violation of privacy is very common in cloud computing, especially in scenarios involving financial transactions, medical records and social networking profiles. According to [3], a sensitive data is any type of personal information which when viewed without proper authorization may result in some inconvenience to the owner of the information. Currently there is not yet established a clear way as the user himself to take control of what is being considered or not as sensitive as the storage environment , and no one better than the person in question to assess the value of privacy to be applied on your own data.

Upon questioning (ii), an approach, which deserves mention, is the encryption. However, a major challenge to the cloud provider is to ensure to its users that their respective data are been submitted to some sort of encryption or even that this encryption is been performed properly. According to the Cloud Security Alliance (CSA), a false or missing definition of rigid internal processes in the cloud provider can compromise the privacy of information through a known threat as Malicious Insiders [4].

At the time, this issue is related to the convergence of IT and customers of storage services in a single environment services. When the provider in question does not have a proper policy to control physical access to its internal resources, someone malicious can access sensitive client files, violating privacy [4], and this becomes more critical when this type of behaviour is not punished.

Another threat also raised by the CSA is the Data Loss or Leakage [4], which reports that the data compromise increases in the cloud computing environment due to the number of interactions that are unique or more dangerous as a result of the architectural and operational characteristics the cloud. The lack of a good backup policy or Data Loss in part of the file or in its encryption key can result in permanent loss of data, affecting its availability.

Finally, based on the question (iii), currently there is still no formal agreement establishing a privacy level agreement between the service provider and client. Something similar is the Service Level Agreement (SLA), which effectively emphasizes on the availability of computing resources offered by a particular service [5], in other words, does not cover anything about privacy in service in question.

Another context is with respect to Compliance, which is characterized as a condition of someone or group of people or processes conform to the desired or predetermined, the target in question are the Standards Specifications. Quite often these specifications are developed by companies that conduct external audit with the aim of analyzing whether a particular environment is in accordance with the requirements. An example is HIPAA, short for Health Insurance Portability and Accountability Act, which is a

978-1-4799-5063-8/14 $31.00 © 2014 IEEE
DOI 10.1109/CLOUD.2014.135

standard in order to protect the health related data, ensuring privacy and fraud prevention [6]. The conformities do not meet all of the fields. Many of them, firstly, are regional or originated from statutory laws. The other issue is that the costs of maintaining control for the requirements is of some complexity and in some cases it reaches impracticable costs to be applicable in small or medium cloud providers.

III. Work in Progress

The objective of this research is to present a Privacy Maturity Model for Cloud Storage Services, PMMCS, for assessing the Maturity Level as the Privacy afforded by services of Cloud Storage providers. A macro view of the proposal is based on the CMMI-SVC model, which aims to assess the Maturity Level of a particular Service [7].

Regarding privacy, the proposal will make use of the concepts defined in the model BSIMM-CP , which is facing the normative Compliance Policies and governance exercised by a particular service [8], identifying absences or flaws in Specifications relating to Personally Identifiable Information (PII). Privacy is a concept that varies greatly, is intrinsic to a particular country or jurisdictions cultures [2]. Likewise, there is no universal consensus on what is defined as a given be considered sensitive. Following the Generally Accepted Privacy Principles [9], GAPP, specification, the privacy rights of certain data are related to the collection, use, retention and disclosure of personal information.

Managing these processes for handling personal data must be performed from the time information is conceived until the end of its availability, ie, the entire life cycle of the item in question. Mather et al [2] proposed a model based on phases for the management of the Data lifecycle in the cloud, as illustrated in Figure 1.

Figure 1. Data Lifecycle in the Cloud

As in [5], 15 security domains more applicants to cloud services were outlined. Our proposal aims to deepen the results presented by Silva et al [5] of which are adherents compliances related to Privacy.

IV. Conclusion and Further Works

In order to achieve the objectives mentioned in the previous section, a four phases working methodology has been defined:

A. Phase 1: Planning and Systematic Review

At this stage, we will make a determined planning of the activities to be performed during the search. A Systematic Literature Review on various topics relevant to this work will also be performed. At the end of this, we will characterize more precisely the problem addressed, concluding with a specification for the proposed solution. Just below are listed the sub activities of this macro activity:

- Gathering Data and Formulation of the Problem
- Construction of Hypotheses and research
- Definition of methods

B. Phase 2: Development of the solution

At this time, we will build an architecture for a prototype of the proposed solution, make a schedule for implementation, and follow it;

- Organization of the resources and Implementation

C. Phase 3: Evaluation of the solution

In this phase, we will conduct a detailed evaluation of the proposed technique through experiments. To this end, we will define hypotheses to be tested and objectives to be reached, based on metrics to be defined;

- Systematization and Analysis of the Data

D. Phase 4: Publication of results

At this stage, which can occur in parallel with one another, we will engage in writing articles, as well the proposal of qualification and the gradual evolution of the architectural model. Hence, in order to offer to the consumer of Cloud Storage a range of varied options regarding the Maturity Level for Data Privacy, our specific objectives are:

- Offer to users a satisfactory Privacy Level;
- Autonomy to the user to establish what should be considered sensitive;
- Analyze what techniques, technologies and architectures are more appropriate to apply Privacy in Cloud Storage;
- An Architectural model based on PMMCS;
- To evaluate the proposed tool through experiments which, at first, check whether the point of view of the end user, the privacy level was satisfactory and studying the viability for use in the real market.

References

[1] Velte et al, “Cloud Computing, A Practical Approach”, McGraw-Hill Osborne Media, 1ª edition, 2009.

[2] Mather et al, “Cloud Security and Privacy: A Enterprise Perspective on Risks and Compliance”, O'Reilly Media; 1ª edition, 2009.

[3] Allen, Julia H., 2001. “The CERT Guide to System and Network Security Practices”. Addison-Wesley, 1ª edition, 2001.

[4] Cloud Security Alliance, “The Notorius Nine: Cloud Computing Top Threats in 2013”, December 2013, Avaliable on: https://cloudsecurityalliance.org/research/top-threats/

[5] Silva et al, "Security Threats in Cloud Computing Models: Domains and Proposals". IEEE CLOUD 2013.

[6] Health Insurance Portability and Accountability, HIPAA, 1996, Avaliable on: http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf

[7] “CMMI for Services (CMMI-SVC) v1.3”, Avaliable from: http://www.cmmi.de/#el=CMMI-SVC/0/HEAD/folder.CMMI-SVC

[8] “The Building Security”, Avaliable from: http://bsimm.com/

[9] “Generally Accepted Privacy Principles”, Avaliable on: http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx