Towards Cloud Computing SLA Risk Management: Issues and Challenges

Jean-Henry Morin
Institute of Services Science
University of Geneva – CUI
Switzerland
jean-henry.morin@unige.ch

Jocelyn Aubert
Centre de Recherche Public
Henri Tudor (CRPHT)
Luxembourg
jocelyn.aubert@tudor.lu

Benjamin Gateau
Centre de Recherche Public
Henri Tudor (CRPHT)
Luxembourg
benjamin.gateau@tudor.lu

Abstract

Cloud Computing has become mainstream technology offering a commoditized approach to software, platform and infrastructure as a service over the Internet on a global scale. This raises important new security issues beyond traditional perimeter based approaches. This paper attempts to identify these issues and their corresponding challenges, proposing to use risk and Service Level Agreement (SLA) management as the basis for a service level framework to improve governance, risk and compliance in cloud computing environments.

1. Introduction

Cloud computing has become mainstream technology offering metallization of IT infrastructures as services along several paths such as Software (SaaS), Platform (PaaS), and Infrastructure (IaaS) [15]. Companies such as Amazon, Microsoft, IBM, and Google, to name but a few, offer such services, which rely on virtualization and pay-as-you-go business models. There are several issues that are likely to emerge in this context. Among them is the question of multi-tenancy and the control over where the processes actually run and where the data reside. While this might not appear to be a major issue for many users at first sight, we see several reasons to actually challenge this point. The main one with regard to this work is the general concern over Governance, Risk and Compliance (GRC) management.

Organizations and individuals are increasingly forced to comply with specific rules imposed either by regulating bodies or legal frameworks often territorially bound. Therefore, not knowing exactly where your data reside and where your processing takes place is likely to become a major problem in the near future. In this context, information security, risk management, and SLA have become important emerging issues surrounding cloud computing.

This paper attempts to identify these issues and their corresponding challenges, proposing to use risk and Service Level Agreement (SLA) management as the basis for a service level framework to improve governance, risk and compliance in cloud computing environments.

The next section further describes the motivation and background of the work. Section 3 provides a detailed description of the issues and state of the art of the three main aspects of the work. Section 4 proposes a research agenda and roadmap towards Cloud Computing SLA Risk Management. Finally we conclude with future work in section 5.

2. Motivation and Background

An emerging vision for the future of the Internet suggests the intensive use of the Internet of Services; where users (individuals or companies) no longer own their computing resources (e.g. servers) but use services on demand (Software as a Service, SaaS) without having to deal with their complexity.

This technological breakthrough raises serious issues regarding information security and data privacy. The distributed nature of the approach challenges many principles of IS (Information System) that need to be adapted, even re-thought. Moreover, many new threats are emerging, for example due to multi-tenancy (infrastructure and services). Due to the almost unlimited computation capacities of cloud computing platforms, any vulnerability may be the source of disastrous consequences.

In this context, IS Security Risk Management (ISSRM) is paramount because it helps to adopt relevant and cost-effective security measures. However, current ISSRM methods only provide a snapshot of the current situation of an IS. This snapshot generally needs to be updated occasionally (once or twice a year for example), but it does not need to be dynamic.

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.602

In our context, the situation is different, with services that may be added, removed, or modified very often. The current ISSRM approaches are thus inadequate and need to be adapted and improved in order to enable efficient use in such versatile and dynamic environments as cloud computing systems.

Moreover, in terms of risk management in a service-oriented context, the risk treatments are often done through Service Level Agreements (SLA). SLAs have become increasingly important, as they define the terms and conditions for the provisioning and delivery of services, including those related to security. ITILv3 defines SLA as "an agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, document Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers" [19]. In other words, SLAs associate financial penalties with adverse outcomes; indeed a customer having signed with a provider such agreement may claim compensation in case of non-compliance. Non compliance, in the context of cloud computing may include for example loss of Quality of Service (QoS), privacy of data issues, vulnerabilities in the execution environment, locality of execution given legal jurisdiction conflicts, etc. Given the diversity of providers of on-demand services (infrastructure, platforms, and software as a service), SLA management will increasingly rely on digital approaches, thus enabling / requiring them to be taken into account in real time within ISSRM frameworks. As a result, the paradigmatic evolution towards cloud and on-demand computing requires major re-thinking of information security. Traditional perimeter-based approaches are no longer sufficient in a highly versatile, nomadic, and service-based environment, which rather calls for studying novel approaches capable of integrating flexibility by design, that should be integrated within broader ISSRM frameworks. The overall objective is to improve GRC (Governance, Risk management and Compliance) through SLA and policy management in a cloud computing environment through relevant and flexible models and tools. To this end, a service-level framework integrating ISSRM and SLA capabilities appears to be a promising and challenging direction.

3. Issues and State of the Art

3.1. Cloud Computing

Cloud computing is location agnostic and provides dynamically scalable and virtualized resources as services over the Internet. It uses virtualization, service-oriented software, and grid-computing technologies, among others. Being a distributed model, cloud computing allows accessing resources and services offered by servers from different places. It is therefore important to address and investigate some of the most fundamental issues concerning cloud service development and deployment.

Many recent efforts have investigated how to move existing capabilities onto the cloud. This is the case for different aspects of cloud computing related to QoS as well as security and compliance [11]:

In terms of QoS, in the IaaS, the resource-level QoS is mostly solved through SLA, but not in PaaS nor in SaaS. This implies that for a user, a basic quality is guaranteed, but the QoS is of little use in cloud-based services lacking higher-level representation and mapping.

With respect to security and compliance, encryption, identification, authentication and authorization, and data rights management are generally supported. Except for IaaS, virtual machines are isolated. However, for many services, the configuration is done manually and does not take into account constant changes and legislative regulation. Besides, support for compliance with specific security requirements is missing. The current state of cloud computing security is described in [12], where risks (policy, organizational, technical, legal, etc.), vulnerabilities, assets, etc. are covered and various recommendations are proposed. Furthermore, a complete use case based on SME is detailed.

Some aspects of privacy and security are taken into account in current commercial products and research works, but a gap still exists, as stated in [11] and [12]. Indeed, strongly related to the issues concerning legislation and data distribution is the concern regarding data protection and other potential security holes arising from the fact that the resources are shared between multiple tenants and the location of the resources is potentially unknown. In particular, sensitive data or protected applications are critical when it comes to outsourcing. In some use cases, the information that a certain industry is using the infrastructure at all is enough information for industrial espionage.

While most tools address essential security aspects, additional issues arise due to the specifics of cloud systems, in particular related to the replication and distribution of data in potentially global resource infrastructures. While data should be protected in a form that addresses legislative issues with respect to data location, it should at the same time still be manageable by the systems and the people who use them.

In addition, the many uses of cloud systems and the variety of cloud types imply different security

models and requirements for the users. As such, classical authentication models may be insufficient to distinguish between the aggregators / vendors and the actual user, in particular in IaaS cloud systems, where the computational image may host services that are made accessible to users. Particularly in cases of aggregation and resale of cloud systems, the mix of security mechanisms may not only lead to problems of compatibility, but may also lead to the user distrusting the model due to lack of insight.

A review of the recent literature around security management on cloud computing identifies some activities such as the following. A new declarative language framework (based on XML) for addressing cloud computing management problems is presented in [10]. This language introduces various concepts found in the context of cloud computing, such as servers, applications, etc.

A simulation framework that enables modeling is presented in [13]. It addresses simulation and experimentation of large cloud computing infrastructures. Although the framework does not provide modeling per se, it does support simulation. The work done upstream can list the common elements of a cloud computing infrastructure.

An integrated cloud computing stack architecture that classifies cloud technologies and services into different layers is described in [14]. This classification can serve to list the various services that may be encountered in such architectures and thus deduce the elements to be considered during modeling.

Nevertheless, the management of information security is addressed only to a very limited extent by existing research work reported in the cloud computing literature. No methods or tools are proposed for concretely tackling the security problems. It is thus necessary to investigate existing methods and approaches used in classical architecture, and to assess their applicability in a cloud computing environment. Further study is therefore needed to explore the risk management and the SLA domains in the context of information security.

3.2. Information Security and Risk Management

Information security has become an essential requirement of Information Systems (IS) and is now factored in by design. In this context, IS Security Risk Management (ISSRM) is paramount because it helps companies adopt cost-effective security measures. Indeed, given the number and diverse forms of security threats, mitigation costs or limited resources have made it impossible to act upon all of them. Hence, companies want to make sure that they adopt only solutions for which the Return On Security Investment (ROSI) is positive. This is done by comparing the cost of a solution with the risk of not using it, e.g., the cost of a business disruption due to a successful security attack. In this sense, ISSRM plays an important role in the alignment of a company's business with its IT strategy.

Existing ISSRM methods and standards [1], [2], [3] are generally focused on structuring the different steps and activities to be performed. Their added value also depends on the knowledge bases of risks [2], [3], [4] and/or security requirements [2], [4] they require. They are the input to the activities performed. The methodological aspects are thus generally rigorous because they build on a well-defined process and structure to be followed.

However, products (i.e., documents produced as output of the different steps of the process) are generally informal, most often in natural language, possibly complemented with tables for structuring the information. This lack of formality prevents the automation (reasoning, evolution, monitoring, and traceability) of 'actionable' Risk Management related information.

For a long time, IS engineers (including requirements engineers) have been using 'models' as a way to achieve better formality and quality, mostly to benefit from abstraction in order to tackle complexity. Previous work [5] has addressed this issue and led to several results:

An ISSRM domain model: The objective of the ISSRM domain model is to define the concepts that should be present in a modeling language supporting ISSRM. Following a structured research method, the domain was analyzed and the model was built. This conceptual model takes the form of a UML class diagram, completed with definitions for each concept. Various kinds of validation of the domain model were performed [6].

ISSRM domain model metrics: Based on the ISSRM domain model, relevant metrics were defined in order to perform and reason on ROSI. A new research method was defined and used to identify these ISSRM metrics [7].

An assessment of ISSRM support by security-oriented modeling languages: Finally, we investigated ISSRM support provided by security-oriented modeling languages and how it could be improved. Several languages were assessed, such as Misuse cases [8], KAOS extended to security [5], and Secure-Tropos [9].

This work, while essential, also highlighted various limitations requiring improvement. First, modern business contexts are highly distributed, loosely coupled, and service-oriented. The developed

approach is not well suited in such a context, and we do not know how to measure service security. Second, this work did not lead to a modeling language proposal, but only to an assessment of existing security-oriented languages. Therefore, further work is needed to propose a modeling language adapted to ISSRM. Finally, tool support for the modeling language is essential in this context and needs to be investigated.

3.3. Service Level Agreements and Exception Management

SLA often studied in the context of QoS have received little attention in terms of the link between normative frameworks for Governance Risk and Compliance (GRC) and the operational side of their usage. A governed and persistently protected SLA is an emerging idea well worth considering, as its features might greatly benefit ISSRM based on real-time tracking and monitoring. Underlying security technologies such as Digital Rights Management (DRM) can be considered as prime candidates in the area of persistent protection and managed content for GRC issues [17]. Unfortunately, such approaches lack the flexibility required by business operations while still maintaining a required or mandatory level of traceability and accountability. Recent approaches to this problem have proposed addressing this issue through Exception Management [16] by challenging a fundamental security assumption, namely the 'distrust assumption' commonly underlying most security infrastructures. Exception Management relies on a priori trust, with the possibility to request / grant exceptions based on simple claims, provided accountable traces are logged. Such logs are auditable and can serve real-time security management dashboards, consequently raising alerts based on specific policies. The combination of this approach with DRM [17] technologies in the context of SLA and ISSRM is a challenging opportunity for enhancing operational GRC in cloud computing. Moreover, as suggested in [18], compliance might be factored in by sound rights managed infrastructures. The case for inter-organizational structures (IOS) is raised as a potential adoption factor, which could be considered by analogy in environments based on cloud computing. However, by their nature, logs can be falsified or forged, which could allow one or other involved parties to cheat, either by attempting to avoid paying penalties for which they are liable; or by forcing the other party to pay a penalty. Faced with this risk, different approaches are possible; [20] describes the design and evaluation of a domain-specific language for SLAs that tend to exhibit different properties including *monitorability* and [21] introduces the notion of a Service Level Management Authority. Such authority – by definition, neutral, independent and objective – facilitates the interaction between the provider and the customer, by monitoring performance and availability of cloud services.

4. Challenges for Cloud Computing SLA Risk Management: Towards a Framework

After surveying the literature of the domain, we claim that much work is needed to improve information security in cloud computing information systems. Having identified and described the issues in this area, we propose a research agenda to be carried out to address them.

Our assumption is that risk management and SLA are relevant tools and that they would help improve trust in cloud computing systems. They can also enhance related fields, for instance leading to better governance of cloud computing systems. Moreover persistent protection (i.e., DRM technologies) in this context offers an interesting technique allowing to address the issue of managed content beyond traditional perimeter based security approaches. However, the lack of flexibility of such technologies being likely to dramatically hamper usability and effectiveness issues, we propose to complement the use of DRM techniques for persistent protection with Exception Management techniques relying on traceability. Recent developments in the Enterprise DRM industry indicate such approaches are increasingly being considered (e.g., provisional licensing).

Therefore the following research objectives are proposed to improve cloud computing governance, risk management and compliance (GRC):

Design a complete framework geared towards security professionals in the context of service-oriented architectures such as cloud computing platforms. Such a framework should mainly consist of a method, supported by a modeling language and a tool.

Moreover, the objective of the framework is to further stress and raises the awareness and incentives underlying security management issues in the emerging global cloud computing landscape. Thus resulting in major contributions to normative initiatives. Indeed, there is currently a lack of clear best practices regarding cloud computing and related issues. To support this objective, and considering risk management, SLAs and exception management as key elements supporting our approach, we propose: the definition of a service-level framework supporting dynamic (i.e., real time) risk management of service-oriented infrastructures such as cloud computing

architectures. Such a framework, based on models that should allow for the representation of any kind of infrastructure and scenario, would provide a continuous representative vision of the current level of risk of architectures.

The service-level framework should provide SLA support directly linked to the operational risk management and modeling layers. Policy-based approaches will be used for SLA management and exception management will be used to introduce the required level of managed flexibility in the planned persistently governed framework.

5. Conclusion and Future Work

We think that although preliminary and ambitious, this work in progress addresses a critical issue in the growing domain of accountable and trustworthy cloud computing. In this context, real time risk management is an attempt to bridge a gap between the operational and management levels of cloud computing. The main contribution of this paper is a statement and discussion of the problem and its issues based on prior art surrounding the areas we propose as contributing elements towards the design of a service level cloud computing SLA risk management framework. The planed framework will be organized around two interrelated themes: dynamic risk management coupled with SLA and exception management. Thus, continuous risk management will help drive SLA and exception management, which in turn may serve as input for ISSRM.

Acknowledgements

This work is part of the CLOVIS project jointly supported by the Swiss SNF and Luxembourg FNR Lead Agency agreement; under Swiss National Science Foundation grant number 200021E-136316 / 1 and Luxembourg National Research Fund (FNR) grant number INTER/SNSF/10/02.

References

[1] Bundesamt für Sicherheit in der Informationstechnik (2005). BSI Standard 100-3: Risk analysis based on IT-Grundschutz.

[2] DCSSI (2004). EBIOS – Expression of Needs and Identification of Security Objectives. http://www.ssi.gouv.fr/en/condence/ebiospresentation.html, France.

[3] ISO/IEC 27005 (2008). Information technology - Security techniques - Information security risk management. International Organization for Standardization, Geneva.

[4] ISO/IEC 27001 (2005). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Geneva.

[5] Mayer, N. (2009). Model-based Management of Information System Security Risk. PhD thesis, University of Namur.

[6] E. Dubois, P. Heymans, N. Mayer and R. Matulevicius, "A Systematic Approach to Define the Domain of Information System Security Risk Management", Book Chapter in: S. Nurcan et al. (eds.), "Intentional Perspectives on Information Systems Engineering", Springer-Verlag. ISBN: 978-3-642-12543-0.

[7] Mayer, N., Dubois, E., Matulevicius, R., and Heymans, P. (2008). Towards a Measurement Framework for Security Risk Management. In Modeling Security Workshop (MODSEC '08), in conjunction with the 11th International Conference on Model Driven Engineering Languages and Systems (MODELS '08). Toulouse, France.

[8] Matulevicius, R., Mayer, N., and Heymans, P. (2008a). Alignment of Misuse Cases with Security Risk Management. In Proceedings of the 4th Symposium on Requirements Engineering for Information Security (SREIS'08), in conjunction with the 3rd International Conference of Availability, Reliability and Security (ARES'08), pages 1397-1404. IEEE Computer Society.

[9] Matulevicius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., and Genon, N. (2008b). Adapting Secure Tropos for Security Risk Management during Early Phases of the Information Systems Development. In Proceedings of the 20th International Conference on Advanced Information Systems Engineering (CAiSE '08), pages 541-555. Springer-Verlag.

[10] Hughes, G.; Al-Jumeily, D. & Hussain, A. A Declarative Language Framework for Cloud Computing Management. In 2nd International Conference on Developments in eSystems Engineering (DeSE'09), pp. 279 -- 284, 2009.

[11] Lutz Schubert. The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010. Expert Group Report version 1.0. European Commission, 2010.

[12] Daniele Catteddu, Giles Hogben. Cloud Computing – Benefits, risks and recommendations for information security. Enisa, Nov 2009.

[13] Calheiros R.N., Ranjan R., De Rose C.A.F. and Buyya R. CloudSim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Service. In Arxiv prepring arXiv:0903.2525, 2009.

[14] Lenk, A., Klems, M., Nimis, J., Tai, S. and Sandholm, T. What's inside the Cloud? An architectural map of the Cloud landscape. In Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp.23—31, 2009.

[15] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition", SIGCOMM Comput. Commun. Rev., vol. 39, 2009, pp. 50-55.

[16] J.-H.Morin, "Exception Based Enterprise Rights Management: T owards a Paradigm

Shift in Information Security and Policy Management", International Journal On Advances in Systems and Measurements, ISSN 1942-261x, vol. 1, no. 1, 2008, pp. 40-49.

[17] J.-H. Morin, "Rethinking DRM Using Exception Management", chapter III, in Handbook of Research on Secure Multimedia Distribution, S. Lian and Y. Zhang (Eds.), Information Science Reference (ISR), ISBN: 978-1-60566-262-6, IGI Global, March 2009.

[18] J.-H. Morin and A. Zeelim-Hovav, "Strategic Value and Drivers behind Organizational Adoption of Enterprise DRM: Setting the Stage", in proceedings of 7th Annual Security Conference,Las Vegas, NV, USA,June 2-3, 2008.

[19] OGC 2007. Official Introduction to the ITIL Service Lifecycle. Stationary Office Books.

[20] J. Skene, F. Raimondi, and W. Emmerich, "Service-level agreements for electronic services", IEEE Transactions on Software Engineering, IEEE Computer Society, 2010, pp. 288-304.

[21] A. Korn, C. Peltz, and M. Mowbray, "A service level management authority in the cloud", Technical Report HPL-2009-79, HP Laboratories, 2009.