SERVICE AND SECURITY MONITORING IN CLOUD

PhD Candidate, Cristian IVANUŞ[1], PhD, Stefan IOVAN[2,3]
[1]University of Economic Studies, Bucharest, ivanuscristian13@stud.ase.ro
[2]West University of Timisoara, Computer Science Department, stefan.iovan@infofer.ro
[3]Railway Informatics SA, Bucharest, stefan.iovan@infofer.ro

Abstract: *In the cloud computing context,* ***Q****uality* ***o****f* ***S****oftware (QoS) is defined as the extent to which user requirements are met by the providers of cloud resources. Users can define their requirements using low level metrics such as processing power of the Central Processing Unit (CPU) or the amount of memory for a virtual machine, but they are interested in defining their requirements using more abstract concepts at a higher level, such as response time and service availability. Increasing complexity, size and number of areas in which cloud penetrated makes it difficult for anticipating how the system will behave. Because of this, different research groups have started to work on QoS level fields for defining the conditions that must be accomplished by a service in order to be delivered. Likewise, it was invested effort in developing of means for managing and assessing efficiently the status of these conditions.*

Keywords: cloud computing, security, services, monitoring

1. INTRODUCTION

Cloud computing concept is not new, but in recent years this had commercial success, estimations revealing the fact that it will play a major role in information and communication technology. Cloud enables new service providers to offer a wide audience, initial infrastructure needs, at a minimal cost. The term "*cloud*" is used since the 90's in the context of dynamic changes of routes in telecom, for balancing the utilization and indicates that telecom infrastructure is virtualized, user not knowing on which channel data will be routed [1]. The basic concept for cloud computing can be dated since 1961 in a speech by John McCharty, when he predicted that sharing processing time can lead to the provisioning of resources and applications in the utility form.

A Cloud is a flexible execution environment involving multiple stakeholders and providing measurable different granularity to meet a certain level of quality (quality of service) [2]. This is the materialization of the vision to transform the calculation into a utility having the potential to transform IT industry (***I****nformation* ***T****echnology*) by offering software as a service. Limits such as scalability can be surpassed with minimal effort by application developers, who can delegate the responsibility for the infrastructure management on their cloud service providers [3].

Cloud computing has penetrated in various fields such as industry, science, governmentconsequently cloud related concepts such as "***U****tility* ***C****omputing*" or "***S****ervice* ***O****riented* ***A****rchitecture*" (*SOA*) have gained popularity. "***Q****uality* ***of*** ***S****ervice*" (*QoS*)application insurance, although identified as being an important feature, is one of the fundamental problems still unsolved. In the past organizations used to buy IT equipment internally administrated, but today more and more organizations prefer to outsource part of their IT infrastructure to delegate responsibilities. In this context, the role of IT has changed, besides the role for managing and troubleshoot IT infrastructure (remained under the control of the organization), outsourcer is also responsible for signing contracts with various IT services suppliers.

Usually clients require that cloud service provider to implement certain security standards such as *ISO 27001* or *CSA Cloud Control Matrix*, but these standards are checked just before a contract is concluded or annually. It requires a mechanism by which clients to continuously monitor security. This can be done by specifying parameters that we would like to monitor in a ***S**ervice **L**evel **A**greement* (*SLA*) and making sure that the cloud service provider monitors or provides means for monitoring these parameters. Without defining these parameters it is very difficult for the customer to evaluate the security offered by the cloud service provider. It is important for SLA to contain measurable parameters that define security and user to have access to the results of the monitoring process.

In [4] it is noted that, although SLA's are often used, and availability is often specified, other security-related parameters are not addressed and many customers do not monitor continuously the security. The authors of [5] were among the first who focused attention on the role of *Cloud Computing* to deliver a sustainable, competitive and secure service. They proposed the use of SLA as a means of defining the QoS guarantees.

2. CLOUD COMPUTING

By cloud computing we understand both applications provided as a service over a network, as well as hardware and software from the data centers. When a cloud provides services to the general public this is a public cloud. If a cloud is only used by an organization, or is not accessible to the general public, this is a private cloud. There are a hybrid approach in which an user or organization can use services offered by a cloud both public as well as by a private one. In terms of hardware used, the cloud offers the following benefits:

- *apparently unlimited computing power*, cloud provider being able to allocate resources on demand or automatically;
- *necessity of a minimum initial investment*, cloud users being able to acquire only the necessary processing power at a time without worrying about the hardware infrastructure expansion later to increase processing power;
- *ability to pay only for the used resources*, without requiring the purchase of resources in advance.

To obtain the elasticity and the appearance of unlimited resources available on request it is necessary to automatically assign and manage resources, in practice this fact being achieved by using virtualization. Although the cloud bring benefits, there are several barriers that stand in the way of its widespread adoption: availability of services, lock-in, data confidentiality, errors that occur in cloud systems are difficult to reproduce and debug, etc.

Currently there are applications that could benefit from the support of QoS in cloud. Multimedia and real-time applications need computing power, instant medical applications must ensure that they meet legal requirements on security etc. Cloud systems are complex due to the large of resources involved and because of constraints to comply with the SLAs signed with users. One of the cloud's features is the elasticity, by enabling resource allocation for a given task at a given moment in time.

Resource allocation should be dynamic and agile, making from the resource allocation a very complex task. One approach for addressing this complexity, is to automate the process.

To perform this automation we should get information about the state of the cloud, and this we can achieve through monitoring. Monitoring is the first step in the cycle *MAPE* (***M**onitoring, **A**nalysis, **P**lanning and **E**xecution*) [6]. According to the granularity and the type of implemented monitoring, we can obtain efficient or less efficient automation.

3. CLOUD MONITORING

Compared to other media, cloud's have some specific features such as using SLA, elasticity and virtualization. Monitoring users' needs are different from those of cloud service providers. Moreover, monitoring of the virtual systems as well as of the traditional physical systems usually have different monitoring requirements. Monitoring systems cloud depends on:

- *cloud's services model,* i.e. cloud services offered by the provider (*IaaS* - Infrastructure as a Service, *PaaS* - Platform as a Service, *SaaS* - Software as a Service)
- how is the intended to be use produced information (customer feedback, internal management system, etc.)
- initial source monitoring (physical resources, virtual machines, applications software. etc).

For addressing these specific cloud systems requirements, during the last years have been developed many monitoring tools. These tools either adapts traditional methods for monitoring distributed systems [7], extend cloud platforms [8] or propose new alternative [9, 10]. Each of these cloud systems monitoring tools is focused on certain issues, providing only a partial solution to the monitoring problem. To perform a monitoring covering all interesting aspects, it is necessary a combination of these tools, but the use of several monitoring systems may introduce an additional workload for the cloud system.

Several studies have tried to analyze and define the basic concepts related to the monitoring of distributed systems and cloud in particular. One of the important methods used to monitor cloud environments is to verify the compliance with certain SLAs. In the majority of commercial cloud systems, Service Level Agreement determines the relationship between cloud users and service providers. To ensure that these SLAs are respected the system must be continuously monitored. When we establish and guarantee the SLAs, monitoring tools plays an important role in transforming system-specific requirements in terms of specific SLAs.

From the technical perspective, monitoring of distributed systems was successfully achieved using different methods and tools. For example, *Ganglia* [11] is a monitoring system for high-performance computers, being widespread. The success of this system is the result of its robustness and of the ability to run on systems using various hardware configurations and different operating systems.

4. SECURITY IN CLOUD

Cloud computing has been developed to share resources in a more economically viable manner. Safe separation is possible, but the costs are unacceptable for SaaS providers. Customers of cloud services must ensure that saving methods do not compromise their important data. Transition to the cloud might not provide effective security in the organization it had when owned hardware resources. Securing networks and data centers has never been an easy task. The cloud feature to share resources makes this even more difficult. Selecting the correct approach on security requires an accurate assessment of threats.

In [12] the authors propose proactively the detection of attacks using machine learning techniques, with three goals. First, the system will be able to detect an attack when it is initiated or even during perpetuation. Second, the system will alert managers and data owners about the type of attack and eventually find means to react. Third, the system will be able to provide customers with information about the type of attack, where the cloud service provider does not wish to do so. In their experiments, the first step has been collecting of some tools such as *Hping*, *Socket Programming*, *Httping*, etc. The second step was to generate scripts to automate attacks. The third step was the finding of tools to monitor the cloud state. From their studies, Support Vector Machine had the best level of performance. If there is no a notification system against unauthorized access, it can reach the cases in which the client is not even informed of security incidents.

In [13] the authors propose a measurable model of means for maintaining security that enables cloud services providers and clients to measure the risk they assume when migrating data to the cloud using the ***M**ean **F**ailure **C**ost* (*MFC*). MFC is a unit of measure that will allow cloud service providers and users to measure the risk associated with the predominant system attacks and vulnerabilities. MFC has several advantages:

1. provide a cost of failure per unit time;
2. measure the impact that will have a security failure of tactics;
3. makes a distinction between stakeholders, providing a cost for each following a failure of the means of security.

The proposed metric provides the following attributes:

1. security is measured in economic terms;
2. security is not an intrinsic attribute of the system, depending on the stakeholders and being able to take different values for each of them;
3. MFC value reflects the heterogeneity of security requirements, the system architecture, security threats and perpetuation of threats.

4.1. Security parameters

An important part of management contracts is to specify the monitoring and verification of safety parameters using the SLA. The customer should ensure that cloud service provider or a third party monitors these parameters and the results are provided. Regardless of the parameters to be analyzed, the following should be taken into account:

1. defining parameters: a clear definition of what is measured;
2. the tracking method;
3. independent testing: testing is recommended independent of the parameters of SLAs;
4. the time in which is provided an alert for a particular incident;
5. regular reports with metrics of the monitored parameters;
6. taking into account of the risk tolerance;
7. penalties if SLAs are violated.

It is good that security experts and IT department to be involved in establishing the security requirements. In general, public sector projects have higher security requirements. Scalability should be addressed in the SLA because it is one of the major benefits of cloud computing. The classification of security incidents helps to finding appropriate measures to counter them. Time duration in which a security incident is reported is critical to limit its impact.

Availability should be frequently tested by both the client and the service provider. Data portability is critical to ensure business continuity in the event that a cloud service provider can not provide the services (or fail due to natural disasters). In [4] is provided a practical guide to help clients to acquire and to administer cloud services. It provides a detailed description of each security parameter to be monitored covering:

1. what must be measured, which are security relevant parameters;
2. how to measure these parameters;
3. How to obtain independent measurements.

The following parameters are addressed:

1. Service availability
   a. what are the functions that must be covered by monitoring to establish the availability;
   b. defining a system that is not available;
   c. how the availability is measured.
2. Reaction in case of incidents
   a. defining the time frame for taking appropriate measures;
   b. incident classification.
3. The elasticity of the services and load tolerance
4. Data life cycle
5. Technical compliance and vulnerabilities management
6. Change management
7. Data isolation
8. Access management

It is important to distinguish between small projects, in which the client will take into account cloud service providers offer and will make a choice and large projects, where the client can negotiate with the cloud service provider SLA needs. One of the tasks that get more and more importance in the IT department is the purchasing and administration of cloud services. It is very important for the acquired services to be monitored and checked to ensure that related security requirements are met.

It is important for organizations to move from regular security audits to continuous monitoring of vulnerabilities and remediation. When certain aspects of IT services represent a risk or have significant impact on the organization, monitoring of these aspects must be included in the SLA.

5. CONCLUSIONS

Because the cloud does not refer to a specific technology, which is a paradigm for providing extended capabilities, it is mandatory to be taken into account non-functional, economic and technical aspects.

Non-functional aspects represent qualities or properties of the system, which can be achieved through different modalities and interpreted in many ways, leading to compatibility and interoperability problems between different vendors because they pursue their methods in order to meet the needs and they differ from provider to provider [14, 15]. Non-functional aspects are the main reason why cloud solutions offered by different vendors differ so much. Economic aspects are one of the main reasons why the cloud came in business environments. Main topics are related toward reducing costs and effort by outsourcing or automating resource management components. Technical aspects come from the non-functional and economic aspects during the implementations of resource management components.

Acknowledgement

This work was partially performed within the project POSDRU /159 /1.5/S/142115 entitled "Performance and excellence in doctoral and postdoctoral research in the field of economics in Romania", financed from the European Social Fund through the Sectorial Operational Programme Human Resources Development 2007 – 2013

REFERENCES

[1] **Malis, A.** (1993) *Routing over Large Clouds (rolc) Charter*, 32nd IETF Meeting in Danvers, URL http://www.ietf.org/proceedings/32/charters/rolc-charter.html

[2] **Iovan Şt.** (2014) *FOLOSIREA TEHNOLOGIEI "CLOUD COMPUTING" ÎN SECTORUL PUBLIC*, Cluj-Napoca: Editura Presa Universitară Clujeană, ***INTELIGENŢĂ, TERITORII ŞI DEZVOLTARE UMANĂ***, (Coordonatori: Mihai Pascaru, Lucian Marina, Călina Ana Buţiu), ISBN: 978-973-595-707-0, pag. 193 – 204;

[3] **Keith Jeffery, Burkhard Neidecker-Lutz,** (2009) *The Future Of Cloud Computing, Oportunities For European Cloud Computing Beyond 2010*, URL http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

[4] **Iovan, St. and Ionescu, P.-V.** (2011) *Cloud Computing: A Short Introduction*, Proc. of 12th European Conference (***E_COMM_LINE 2011***), Bucuresti, Romania, ISBN: 978-973-1404-20-3;

[5] **R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic,** (2009) *Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility*, Future Generation Computer Systems, Volumul 25, Editia 6, pag. 599-616. URL http://www.sciencedirect.com/science/article/pii/S0167739X08001957

[6] **M.C. Huebscher, J.A. McCann,** (2008) *A survey of autonomic computing degrees, models, and applications*, ACM Computing Surveys (CSUR), Volumul 40, Editia 3;

[7] **Iovan, St. and Ionescu, P.-V.** (2012) *Security Issues in Cloud Computing Technology*, Proc. of 13th European Conference (***E_COMM_LINE 2012***), Bucuresti, Romania, ISBN: 978-973-1704-22-7;

[8] **Amazon**, (2014) *CloudWatch*, 2014. URL https://aws.amazon.com/cloudwatch/

[9] **Iovan, St. and Daian, Gh.** (2013) *Impact of Cloud Computing on Electronic Government*, Proc. of 6th Symposium "*Durability and Reliability of Mechanical Systems*", (***SYMECH 2013***), Ranca – Gorj, pag. 71-77;

[10] **Ivanus, Cr. and Iovan, St.** (2013) *Providing Products and Services in Cloud Computing Technology*, Proc. of 14th European Conference (***E_COMM_LINE 2013***), Bucuresti, Romania, ISBN: 978-973-1704-23-4;

[11] **M.L. Massie, B.N. Chun, D.E. Culler**, (2004) *The ganglia distributed monitoring system: design, implementation and experience*, Parallel Computing, Volumul 30, pag. 817-840;

[12] **Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi,** (2012) *A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing*, Future Generation Computer Systems, Volumul 28, Editia 6, pag. 833 – 851;

[13] **Iovan, St. and Daian, Gh.** (2013) *Security Issues in Cloud Computing*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University, Engineering Series,* Issue **4**/2013, (***CONFERENG 2013***), ISSN: 1842 – 4856, pag. 147-152;

[14] **Ivanus, Cr. and Iovan, St. (2013)** *"Internet of Things" – A new Technological Evolution*, Targu Jiu: "Academica Brancusi" Publisher, *Annals of the "Constantin Brancusi" University*, Engineering Series, Issue **4**/2013, (***CONFERENG 2013***), ISSN: 1842 – 4856, pag. 165 - 170;

[15] **Iovan, St. and Ivanus, Cr.** (2014) *"Open Source" Technologies used in Cloud Computing Implementations*, Proc. of 7th Symposium "*Durability and Reliability of Mechanical Systems*", (***SYMECH 2014***), Polovragi – Gorj, pag. 32 - 38;