CLOUD COMPUTING SECURITY

PhD Ştefan IOVAN[1,2], Eng. Alina Anabela IOVAN[2]
[1]West University of Timişoara, Computer Science Department, stefan.iovan@infofer.ro
[2]Railway Informatics SA, Bucharest, ROMANIA, alina.iovan@infofer.ro

Summary: *Cloud computing reprentes the software applications offered as a service online, but also the software and hardware components from the data center.In the case of wide offerd services for any type of client, we are dealing with a public cloud. In the other case, in wich a cloud is exclusively available for an organization and is not available to the open public, this is consider a private cloud [1]. There is also a third type, called hibrid in which case an user or an organization might use both services available in the public and private cloud. One of the main challenges of cloud computing are to build the trust and ofer information privacy in every aspect of service offerd by cloud computingle. The variety of existing standards, just like the lack of clarity in sustenability certificationis not a real help in building trust. Also appear some questions marks regarding the efficiency of traditionsecurity means that are applied in the cloud domain. Beside the economic and technology advantages offered by cloud, also are some advantages in security area if the information is migrated to cloud. Shared resources available in cloud includes the survey, use of the "best practices" and technology for advance security level, above all the solutions offered by the majority of medium and small businesses, big companies and even some guvermental organizations [2].*

Key words: cloud computing; security; public services; composite services; best practices;

1. INTRODUCTION

Cloud computing is not a new concept, but in the last years have growen into a commercial succes, reaching the point to play an major role in technologies related to information and communication. Cloud computing allowes to new service providers to offer the open public solutions on a minimal cost and infrastructure needs at first.

The name "*cloud computing*" is used starting with the nineties in the area of dymanic changes in the teleomunication sector in order to balance the use and points to the fact that the telecomunication infrastructure was virtual, the user has no ideea on the line used for transfering his data [3]. Basic concept on which is build all cloud computing can be traced to 1961 as part of a public lecture given by John McCharty, in this presentation appeard the ideea that sharing the process time may lead to supply resources and applications in utility forms.

Cloud is an elastic working enviroment that involves more than one parts and supplies services measured by diffrent grained in order to satisfy a given quality level (servicies quality) [4]. This being the transformation of the view to change calculus into a utility, having the potential of transforming the IT industry by offering software as a service. The limitation given by scale can be easily overcomed with minimal effort by the software developers, they can assigne the responsability given in managing the infrastructures resourses on which the software operates,the one available in the given by cloud service provider [5].

Cloud computing has entered in diffrents domains such as industry, science and public domain, as a result, the concept related to cloud such as "*Utility Computing*" or "***S**ervice **O**riented **A**rchitecture*" (***SOA***) have gane popularity. Making sure that the level of quality is

keept, "***Q**uality **o**f **S**ervice*" (***QoS***) even if identified as an important specific feature, is still one of the unsolved problems. In the context of cloud computing, ***QoS*** is defined as a measurement between the fulfilement of the users requests by the providers of cloud solutions [6].

The users can define the requests using lower level metrics such as processing power or memory capacity for a virtual machine, but they are actually more interested to define the requests in more abstract notions, of higher level, such as replay time and availability of a service. Increasing complexity, size and the number of domains of cloud activity make more difficult the forcast of the way that the system will behave.

Because of this, different groups of resurcers started working at createing a description for QoS levels which define the conditions that have to satisfy in order to make the service requested. Also, a lot of effort was put into developing means to manage and evolve effectively the state of this requests. In the past IT organizations used to buy equipment that they operated internally, but today more and more organizations prefer to outsource some IT infrastructure to delegate management responsibilities. In this context, the role of IT has changed, besides used to manage and troubleshoot IT infrastructure remaining under the control of this organization is also responsible for concluding contracts with different service providers in the IT field.

Typically clients require the cloud provider to implement certain security standards such as ISO 207 001 or CSA Cloud Controls Matrix, but these standards are checked just before a contract or annual. It requires a mechanism for customers to continuously monitor safety. This can be done by specifying the parameters that we want to monitor in a Service Level Agreement (SLA) and ensuring that cloud service provider monitors or provides means for monitoring these parameters.

Without defining these parameters it is very difficult for the client to evaluate the security offered by cloud service provider. It is important that SLA contain measurable parameters that define security and user access to the results of the monitoring process. In [7] It stated that although SLA's are often used, and availability is often specified, other security related parameters are not addressed, and many customers do not use continually monitors security. The authors [8] were some of the first to have focused on the role cloud computing service to deliver sustainable, competitive and secure products. They proposed using SLA as a means to define guarantees QoS.

2. SECURITY PERSPECTIVE

The main reasons of risks and challenges for cloud computing are that users delegates authority cloud providers, and having an environment where resources are shared by multiple customers / users [9]. Typical risks include: the availability of services and data; lack of mechanisms for data classification; or data integrity services; confidentiality; subjecting the legal provisions; lack of capacity to obtain data on the mode of operation; loss of control over data and services; ambiguity on liability; lack provider liability in case of security incidents; the cost and difficulty of migrating to the cloud; suppliers wish to not allow users to use the services of other suppliers.

The challenges facing cloud site emphasizes the need to consider data protection in physical environments and virtual. Main goals for security in the cloud are: protecting data against

unauthorized access, disclosure and modification; protect against unauthorized access to cloud resources; ensuring isolation; ensuring availability; ensuring efficient management, control and compliance with established processes; ensure the level of security required for cloud applications; ensuring network security; ensuring confidentiality; ensuring incidents; detecting incidents and action.
Key issues to be considered when analyzing cloud security standards are the legal differences between states, including changes in laws concerning data protection; conflict of interest between national security and cloud services customers; visibility and transparency; insurance and trust; certificates, audit and testing; access control; the use by providers of other services offered by the provider; virtualization; control over location data; permanent and safe removal process; signing the contract.

3. CLOUD SECURITY

Cloud computing has been developed to share resources in a manner as economically viable. Safe separation is possible, but the costs are unacceptable for providers of Software as a Services (SaaS). Customers of cloud services should ensure that saving methods do not compromise their important data. Moving to the cloud might not ensure the effectiveness of security that the organization had held when hardware resources. Securing networks and data centers has never been an easy task. The property's cloud to share resources makes this even more difficult. Selecting a correct approach requires an accurate assessment of security threats.
In [10] the authors propose proactively detect attacks using machine learning techniques, with three objectives. First, the system will be able to detect an attack even when it is initiated or during perpetuation. Secondly, it will alert administrators and data owners will indicate the attack type and possibly the means to counter it. Thirdly, the system can 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 was collection of tools such as: *Hping*, *Socket Programming, Httping,* etc. The second step was to generate scripts to automate attacks. The third step was finding tools to monitor the cloud's activity. From their studies, Support Vector Machine have had the best level of performance. If there is a notification system against unauthorized access, you can get to cases where the customer is not even informed of security incidents.
In [11] the authors propose a model measurable means to maintain security that allows cloud service providers and customers to measure risk that they incur when migrating data to the cloud using ***M**ean **F**ailure **C**ost* (***MFC***). MFC it is a unit of measurement that will enable cloud service providers and users to measure the risk associated with prevalent attacks and system vulnerabilities. MFC has several advantages: (i) provides a cost of failure based on a time unit; (ii) measure the impact it will have a failure of security tactics; (iii) distinguishes between stakeholders, providing a cost for each following a failure of the means of security.
The proposed metric provides the following attributes: (i) security is measured in economic terms; (ii) security is not an intrinsic attribute of the system, depending on the stakeholders and may take different values for each of them; (iii) MFC value reflects the heterogeneity of requirements for security, system architecture, security threats and perpetuation of threats.

3.1. Security parameters

An important part of contract management is to specify, monitor and verify the security parameters using SLA. The customer should ensure that cloud service provider or a third party monitor these parameters and results are provided back to the client. Regardless of the parameters to be analyzed, the following characteristics should be taken into account: (i) defining parameters: a clear definition of what is measured; (ii) monitoring method; (iii) independent testing: testing is recommended to be done independently for parameters of SLAs; (iv) given time that provides an alert for a particular incident; (v) regular reports with metrics for the monitored parameters; (vi) taking into consideration risk tolerance; (vii) penalties if SLAs regulations are violated.

It is good that security experts and IT department to be involved in establishing the requirements relating to security. Public sector projects generally have higher security requirements. Scalability should be addressed in ALS because it is one of the great advantages of cloud computing.

Classification of security incidents helps find suitable measures to counter them. During the reported incident in which security is critical to limit its impact. Availability should be tested frequently by both the client and the service provider. Data portability is critical to ensure business continuity if a cloud service provider can not provide services (bankruptcy or due to natural disasters).

In [7] it is offered a practical guide to help customers acquire and manage cloud services. It gives a detailed description of each security parameter to be monitored covering: (i) what needs to be measured, which are relevant parameters for security; (ii) how this parameters have to be measured; (iii) how independent measurements can be obtained.

The following parameters are addressed: (i) services availability: which of the functions must be covered by the monitoring process in order to determin availability; defineing an unavailable process; how is availability measured. (ii) response in case of incidents: define the tame accepted for protocol measures; incidente clasification. (iii) services ellasticity and load tollerance; (iv) data lifecycle; (v) technical comformity and vulnerability management; (vi) changes management; (vii) data isolation; (viii) acces management.

It is important to distinguish between small projects, the client will consider cloud providers offer and make a choice and large projects, the client will be able to negotiate with the service provider cloud SLA needs. One of the tasks that get increasingly important in the IT department is acquiring and managing cloud services. It is very important that the services purchased to be monitored and checked to ensure that security requirements are met.

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

3.2. Monitoring parameters

Services availability. Cloud providers will define different availability. It is important to better understand how availability is defined by them. Availability is usually defined as a percentage of total operating the service to be considered available in a certain period of time (usually a year or a month). An SLA may be defined and a mean return to normal functioning after an incident. Sometimes customers can create redundancy to ensure better availability. For example, if a provider of Infrastructure as a Services (IaaS) services are offered on the basis of which the client will build systems with higher tolerance to failure using components with less tolerance. Monitoring methodologies are based on: user reports; logs based service providers; based on periodic checks; monitoring tools based cloud service providers.

Reaction in case of incidents. An incident is an event that is not part of normal operation of the service and which may cause an interruption or reduction in quality of service. Incidents are defined in relation to other parameters specified in the SLA. In order to accurately report incidents, have established a classification scheme. Logging methods must be established to record incidents.

Services ellasticity and load tollerance. This parameter is linked to availability because it reflects how resources available vary with the application. If the user is expected to fluctuations in resource use, it must communicate this cloud providers because these fluctuations are covered in the SLA. Some cloud service providers offer guaranteed reserves of resources that can be accessed regardless of system loading. Cloud providers also offer automated elasticity in line with customer requirements. The most important factor is the ability to monitor cloud provider to provide resources where they are needed. The type of the selected resources to be monitored will vary depending on the type of service. IaaS is suitable for measuring the elasticity by counting the number of processing units available, while for SaaS application can measure the ability to respond to requests.

Data lifecycle management. This group of parameters measure the efficiency with which the service provider manages the data, including backup policies and data replication, the ability to export data and systems to prevent data loss. Data portability is one of the crucial parameters to be tested independently by the customer or a third party. Customer is responsible for building redundancy and data recovery measures in systems where they control.

Technical comformity and vulnerability management. This group of parameters measures the ability of a service to meet a security standard including actions that may be taken in the event of discovery of a vulnerability. Cloud service providers do not disclose detailed information about vulnerabilities for security reasons. Customers can receive reports deviations from the security policy. These reports can provide information on specific vulnerabilities and management efficiency trends.

Customer is responsible for taking action processes, systems, devices, and activities are not due to vulnerabilities that appear to be the service provider cloud.

Change management. These parameters are used to monitor and manage critical changes in the properties and settings relevant to the security of a system.

Data izolation. This set of parameters covering access to resources by users who have rights to access those resources. Isolation is an essential element of all types of cloud environments (IaaS, PaaS, SaaS). Isolation ensures data confidentiality, integrity and availability of data users and services offered different clients. Cloud providers are responsible for containment resources, and customers rarely have knowledge about the mechanism by which cloud service provider ensures this. Isolation and functional data is a requirement to be present all the time.

Log Management. This group of parameters provide access to informations regarding important events of using the resources in the cloud in the past. The clients may need information over the processed information or eliminated, the time, and the user data that handled the process. Monitoring the log management should include: periodic tests to verify the avalibility and the precision of the recorded events.

4. CONCLUSIONS

Cloud systems are complex ones due to the large number of resources involved and also by the bond to aply the lines set by SLA in agreement with the users. One of clouds features is elasticity, which alowes to suplay resources for a certain task at a given moment. The suplay of resources has to be dynamic and smart, this transforming the task of suplaing resources a complex one. One of the used methodes is, in order to adress this complex task, to transform it into an automatical procces.

In order for this automatical process to be possible are required informations over the status of the cloud activity, and this can be achived by monitoring the activity. Monitoring is the first step in the cycle ***MAPE*** (***M****onitoring*, ***A****nalysis*, ***P****lanning and* ***E****xecution*) [12]. According to granulity and the type of monitoring used, can be obtained an efficient or less efficient automatization of the process.

Cloud computing can be seen as an evolution of grid computing, that also not being a new concept, that is why this one has enherits all the security problems and extra new specific problems given by it's architecture [7]. National Institute of Scale and Technology of SUA, states that security, interoperability and portability are the main obstacles raised in front of large scale use of cloud computing [13].

5. REFERENCES

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

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

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

[4] **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

[5] **Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia,** (2010) *A view of cloud computing*, Communications of the ACM, Volumul 53 Ediţia 4, pag. 50-58
[6] **St. Iovan, Cr. Ivanus**, (2013) *Cloud Computing Essential Element – Data Center*, Proc. of 14th European Conference (***E_COMM_LINE 2013***), Bucharest, Romania, ISBN: 978-973-1704-23-4;
[7] **ENISA**, (2011) *Survey and analysis of security paramters in cloud SLAs across the European public sector*, Deliverable 2011-12-19
[8] **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
[9] **Cr. Ivanus, St. Iovan,** (2014) *Cloud Computing Technology Trends,* Proc. of 7th Symposium "*Durability and Reliability of Mechanical Systems*", (***SYMECH 2014***), Polovragi, pag. 264 - 269;
[10] **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, Ediţia 6, pag. 833-851
[11] **Latifa Ben Arfa Rabai, Mouna Jouini, Anis Ben Aissa, Ali Mili**, (2013) *A cybersecurity model in cloud computing environments*, Journal of King Saud University - Computer and Information Sciences, Volumul 25, Ediţia 1, pag. 63-75.
[12] **St. Iovan, Gh. I. Daian**, (2012) *Enterprise Services Architecture in the World of Information Technology*, Annals of the "Constantin Brancusi" University of Targu Jiu, Fiability & Durability, Supplement No. **1**/2012, ***(SYMECH 2012)***, ISSN: 1844 – 640X, pag. 375 – 381;
[13] **Cr. Ivanus, St. Iovan**, (2015) *Service and Security Monitoring in Cloud*, Proc. of 8th Symposium "*Durability and Reliability of Mechanical Systems*", (***SYMECH 2015***), Ranca – Gorj, pag. 60 - 66;