THE USV ANNALS OF ECONOMICS AND PUBLIC ADMINISTRATION | VOLUME 12, ISSUE 2(16), 2012

ISSUES REGARDING SECURITY PRINCIPLES IN CLOUD COMPUTING

Mircea GEORGESCU
Ph. D. Professor „Al. I. Cuza" University of Iasi, Romania
mirceag@uaic.ro

Natalia SUICIMEZOV
Ph. D. Student „Al. I. Cuza" University of Iasi, Romania
n_suicimezov@hotmail.com

Abstract:
The introduction of Cloud Computing creates a wave of reluctance for specialists representing the information security field. This reluctance comes from end users as well, who think data stored on an internal infrastructure are much safer than those held on the servers of potential providers, and also from governments that apply different policies at the national level regarding the security of personal data. Non-acceptance and reluctance of cloud technologies also come from the impact of changing perceptions about infrastructure architectures, development and application delivery models that the emergence of these technologies had led to. Many of the technologies used for traditional security issues are no longer effective in the cloud. Meanwhile, other solutions were developed to put more focus on Governance in the Cloud. To successfully manage and ensure the efficiency and effectiveness of information technologies as a corporate resource, organizations have turned to what is IT governance. Rapid transition to cloud technologies fuel a critical issue regarding the success of information systems, communication and information security. As a consequence, the paper aims to identify, evaluate and clarify information security in the Cloud using three principles of security (Confidentiality, Integrity and Availability) and to emphasize the importance of Governance in Cloud Computing at the business level.

Key words: Information Technology, Cloud Computing, Governance, Confidentiality, Integrity, Availability.

JEL classification: L86, M15

INTRODUCTION

The history of information technology has known many attempts to give up the hardware equipments. This concept is especially pursued by the cloud technologies which involve in their utilization a minimum amount of hardware equipment and allow the organizations to focus more on the core business by providing optimized solutions within a known and simple framework. Cloud computing relies on an innovative architecture as an information system, being considered the information technology of the future.

Even if the emergence of cloud computing is quite recent, perspectives in the critical aspects of security may be drawn from experiences reported by those that adopted in a timely manner these technologies as well as from the analyses of researchers and their experiments with the available associated platforms and technologies of Cloud providers. In the next sections we shall deal with the confidentiality and security issues, which are believed to have a long-term significance in the Cloud technologies and, whenever this is possible, we shall try to exemplify through already given examples in order to illustrate existing problems. The examples are not exhaustive and cover only an aspect of a general issue. The specialists' orientation is towards problem-solving, but sometimes many of them persist and expand, having the potential to re-occur under other forms, according to the model and typology of the Cloud service.

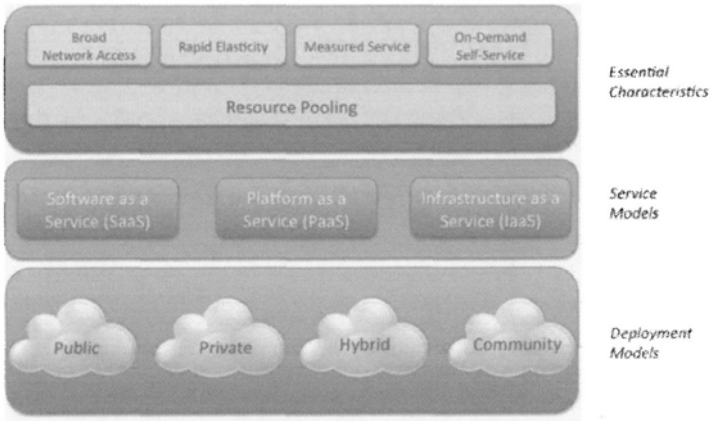

Figure 1. National Institute of Standards and Technology visual model of cloud computing definition

Since cloud computing has grown from an amalgam of technologies, including service-oriented architectures, virtualization, Web 2.0 and Utility Computing, many of the confidentiality and security issues can be seen as known problems but in a new context. In spite of this, their combined effect within this framework should not be updated.

IT GOVERNANCE AND CLOUD COMPUTING

The information technologies have become in the last decade a main principle of an organization's infrastructure, creating value (Gupta, Y., 1991; McAfee, A., 2008). In order to manage and successfully ensure the IT efficiency and effectiveness, as a corporate resource, organizations have turned to what is IT Governance.

Governance integrates IT in the corporate governmental processes (Ross, 2004). This integration also lines up the information technologies with the business processes, ensuring and providing IT effectiveness and efficiency (Schwartz, 2003).

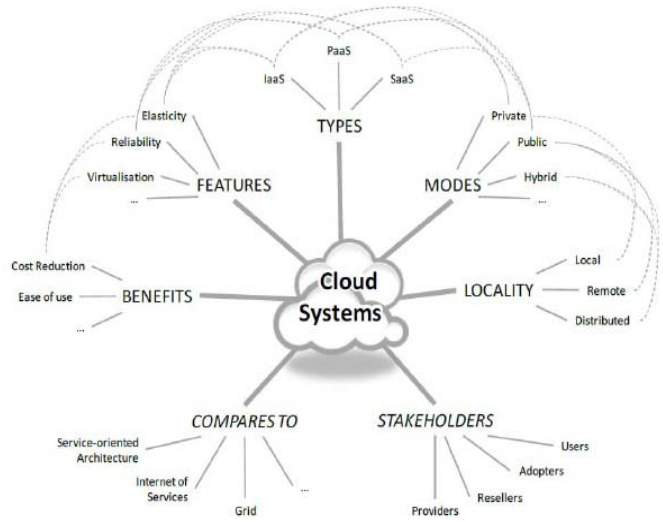

Figure 2. Main elements of a cloud system – a non exhaustive view (Schubert, 2010)

According to its "preachers", the successful IT governance will ensure the increase in competitive advantages and of organizations' financial outcomes (Weill, 2004; Van Grembergen, 2004). In other words, when weighing the pros and cons of information technologies, the IT Governance is worth it (Carr, 2003).

The previous research in the IT Governance field has suffered due to the authors Sumbamurthy and Zmud, who referred to it as an over-simplified and a too normative beginning.

This study focused on the marketing ideas and the IT Governance architecture, instead of understanding the daily practices of the IT Governance and its construction.

Nowadays, the IT Governance represents a key activity in the activities of strategic management of Information Systems in large organizations (IS is the term addressing the IT functions in an organization) (Schwartz, Hischheim, 2003).

The availability of cloud computing services implies major risks through the lack of organization controls of the employees who use such services. Even if Cloud Computing simplifies the acquisition process of IT platforms, it does not diminish the need for governance; on the contrary, it amplifies it.

An advantage of Cloud Computing is represented by the capacity to reduce the capital investments and at the same time, to satisfy the computing needs by means of operation costs. Cloud computing may reduce the initial running cost of new services and shorten the necessary time to obtain a real investment benefit (for example, the acceleration of transforming time into value), thus better aligning the used expenses. In spite of this, the standard processes and the procedures of an organization use them to get computing resources of capital expenses, slightly avoided by a department or a person and hidden as daily operation costs.

When such actions are not regulated by an organization, the security and control policies and procedures could be overcome and might represent a danger for the organization. For instance, the vulnerable systems might be dislocated, the legal regulations might be ignored, fees might rapidly accumulate to unacceptable levels or other undesired effects might occur.

SECURITY CONCEPTS IN CLOUD

The three main concepts related to security are: Data Confidentiality, Integrity and Availability. Each vendor of these solutions attempts to propose its own security solutions but their degree of development differs according to the size of the companies.

Table 1. Cloud vendors and their attributes and ranking (by online traffic)

Cloud computing vendor	Online traffic	Company size	Cloud type
CloudWorks	Low	Small	IaaS
Enki Consulting	Low	Small	IaaS
JungleDisk	Low	Small	SaaS
3Tera	Low	Small	SaaS
Cloud9 Analytics	Low	Small	SaaS
Absolute Performance	Low	Small	SaaS
Vertica	Low	Medium	IaaS
EnterpriseDB	Low	Medium	IaaS
GoGrid	Low	Medium	PaaS
Layered Technologies	Low	Medium	IaaS
IBM Lotus Live	Low	Large	SaaS
CloudAppy*	Low	—	PaaS
Rackspace Cloud	Medium	Small	IaaS
EngineYard	Medium	Small	PaaS
NetSuite CRM+	Medium	Large	SaaS
Yahoo Zimbra	Medium	Large	SaaS
Accenture	Medium	Large	PaaS
Sun Microsystems	High	Large	PaaS
Oracle	High	Large	IaaS
Microsoft Office Live†	High	Large	SaaS
Salesforce.com	Very high	Large	SaaS
Amazon	Very high	Large	SaaS
Google Apps Engine†	Very high	Large	PaaS
Google Docs†	Very high	Large	SaaS
Microsoft SQL Azure†	Very high	Large	IaaS

Confidentiality strictly refers to the authorized parties or the systems with access skills to the protected data. The threats in cloud increase with the increase in the number of components, applications and equipments involved, leading to an increased number of access points. The delegation of data control by the cloud leads on the other hand to the increase in the risk of data breach because they become accessible to a high number of participants. A significant number of

attacks occur due to the multiple locations from where data could be accessed as well as due to the application security and data preservation.

Another expression met in the characteristics of Cloud technologies is that of "multitenancy", which refers to resource sharing. Numerous aspects of Information Security are shared among memory, applications, networks and data. Cloud computing is based on a business model where resources are shared (multiple users share the same resource) at the level of network, host and applications. If the users are isolated at virtual level, the hardware components are not separated. Having a multitenant architecture, a software application is composed to virtually split data and configurations, so that each client organization should work with a customized virtual application. The multitenancy concept is similar with that of multitasking in the operating systems. Multitasking, in the computational environment, is a method by means of which multiple activities, known as processes, share common processing resources, namely the processor.

The multitenancy, viewed as multitasking, presents a multitude of confidentiality threats. Data confidentiality in the cloud is correlated with the users' authentication. The protection of a user account against data theft represents a much higher problem in the access control of items such as memory, equipments and applications while electronic authentication establishes the confidentiality of users' identity in the information system.

The application confidentiality is important in light of the system data security and refers to the confidence that specific processes or applications will maintain and manage users' personal data in a safely manner.

In the Cloud environment it is extremely important that all the clients delegate confidence to the application provided by the owner of the infrastructure, organization which should be certified in order to eliminate confidentiality and privacy risks. The cloud provider should be also responsible to provide secured instances that would ensure confidentiality and privacy to the users. The unauthorized access may be possible by exploring the vulnerability of applications or the lack of strong identification procedures, known as being great issues of confidentiality and privacy.

The cloud providers, such as other organizations operating with personal data, should meet the legal conditions imposed by state regulations, by ensuring the necessary confidentiality protection. Data are stored in multiple locations, fact which enhances the risk of confidentiality loss and the cloud has to deal with several legal challenges. If originally the employees' (users) data were stored on the company's servers, the passage to the cloud implies data storage on the service providers' servers that can be in America, Asia or in any other place. For example, in Europe, this might infringe the legal norms which require that the organization knows where the personal data are and that these should be at any time available for the organization.

Integrity

The second concept and aspect of Information Technologies is integrity that implies that the change of assets should be performed only in an authorized manner or by authorized parties, covering data, applications and equipments. In this respect data are protected through the non-authorization of creation, change or deletion.

The management of rights on certain resources of the organization guarantees the integrity of valuable data and services of the company and eliminates the risk of their loss, abuse or inappropriate use. This type of mechanisms also offers an enhanced visibility and transparency, being able to control and see who or what has led to the alteration of the information system or which could be seen as a potential risk of harming the integrity.

We have previously brought into discussion a mechanism enabling the level of specific access of authenticated users to secured resources of the system. The authorization is essential in ensuring that only authorized entities may interact with data in the Cloud environment, which implies an increased number of entities and access points.

The cloud computing providers must ensure the data integrity and accuracy while the cloud models present certain threats including sophisticated domestic attacks on these data attributes. The creation, modification or data deletion can be intentional or unintentional (Zissis, Lekkas, 2012).

A dissatisfied user can intentionally change a program and can make it work inadequately in a certain instance or at a certain hour. Providers try to fight these attacks by implementing a set of application interfaces already familiar to the users by means of which they easily access the cloud services. Moreover, the security of cloud services depends on the security of these interfaces, and if unauthorized users get control over them, the danger of data change or deletion of users' data is 100% guaranteed. The responsibility for the protection of application integrity in the cloud is transferred to the administrator or the application beneficiary. The integrity of networks or hardware equipments are issues added and addressed by the cloud provider.

Availability

The third security concept is availability and it refers to the property of a system to be accessible and usable upon the request of authorized entities. The system availability includes the system ability to operate even when the conditions of authorized access are not met. Data, application and equipment availability is requested; therefore these should be available to the authorized users upon request. The users' demands to access the physical infrastructure generate a strong overload on the network availability and make it difficult to process and recover data. The cloud owner must guarantee that information is available to the clients upon request.

The system availability refers to the capacity of a system to run applications even when there are infringements of access rights. The system must be able to run even under the circumstances of a security breach. The cloud computing services have a strong dependence on the infrastructure resources and network availability, 24 hours per day. The understanding and documentation of specific requests of all the users is necessary in designing an IT solution which should "ensure" the accomplishment of these needs. One of the most complex design elements in the information security is the identity check-up, meeting the same common security requests and determining the specific needs for data protection. This distributed work environment, with several users, creates unique security opportunities, dependent on the access level, applications, virtualized or installed on the physical platform.

CONCLUSIONS

We consider that the cloud computing technologies support and will continue to support a surplus of information systems, since the benefits and strong points are greater and more obvious than the weak points and vulnerabilities, in comparison with other systems. The implementation architectures of Cloud technologies have the capacity to approach the traditional vulnerabilities met in Information Security, while having dynamic features able to discourage the effectiveness of measures taken in the traditional information technology environments. The present paper identifies and deals with the generic design principles of the cloud environment, which resumes the need to verify and control relevant threats and vulnerabilities. Thus, the essential objectives of security in the cloud systems are the following:

- To ensure the availability of the information communicated among or held by the participating systems;
- To maintain the integrity of the information communicated among or held by the participating systems (for example to prevent the loss or change of information during an unauthorized access, breakdown of a component or other error);
- To maintain the integrity of services provided (for example confidentiality and correct operations);
- To provide control over the access to services or service components;
- To authenticate the identity of partners involved in communication and where it is necessary, to ensure the non-rejection of data;
- To provide interconnection between closed systems;
- To ensure the confidentiality of the information held by the participating systems;
- To ensure a clear separation of data and processes at the virtual level of cloud technologies, offering the guarantee there will be no data leaks among various applications;

- To maintain the same security level while data are added or deleted at the physical level.

We tend to believe that the issue of cloud technology security will be much debated in the future and ways to recover it will be sought after; still, the main and most efficient solution remains the Cloud Governance. The Governance will create the premises for certain security advanced policies and procedures imposed both to end users, in the access and work with the Cloud applications and to the Cloud providers. This remains to be observed, with the evolution and extensive use of these technologies.

ACKNOWLEDGMENT

This work was supported by the project "Post-Doctoral Studies in Economics: training program for elite researchers - SPODE" co-funded from the European Social Fund through the Development of Human Resources Operational Programme 2007-2013, contract no. POSDRU/89/1.5/S/61755).

REFERENCES:

1. Carr, N.,(2003), IT Doesn't matter, Harvard Business Review, mai 2003, pp 18-34;
2. Chakraborty, R. et al, (2010), The Information Assurance Practices of Cloud Computing Vendors, IT Professional Magazine, july 2010, IEEE Computer Society, pp 29-37
3. Cloud Security Alliance, (2009), Security Guidance for Critical Areas in Cloud Computing v2.1, p 14;
4. Cloud Security Alliance, (2010), Top threats to cloud computing, Cloud Security Alliance, june 2010;
5. Gartner, (2008), Assessing the security risks of cloud computing, Gartner Group, 2008.
6. Gupta, Y.P., (1991), The chief executive officer and the chief information officer: the strategic partnership, Journal of Information Technology, 1991
7. McAfee, A., Bryjolfsson, E., (2008), Investing in the IT that makes a difference, Harvard Business Review, 2008;
8. Ross, J.W., Weill, P., (2004), IT Gouvernance: how top performers manage IT decision rights for superior results, Watertown, MA., Harvard Business Review, 2004
9. Schubert, L., (2010), The future of Cloud Computing, Report for the European Commision, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf;
10. Schwartz, A., Hlrschheim, R., (2003), An extended platform logic perspective of IT gouvernance, Journal of strategic Information Systems, 2003, pp. 129-166;
11. Sherman, R., (1992), Distributed systems security, Computers & Security 11 (1), 1992;
12. Van Grembergen, W., De Haes, S., (2009), Enterprise Governance of Information Technology, Springer, USA, 2009;
13. Weill, P., (1992), The relationship between investment and information technology and firm performance: a study of the valve manufacturing sector, Information system research, 1992;
14. Zissis, D., and Lekkas, D., (2012), Addressing cloud computing security issues, Future Generation Computer Systems 28 (2012), p. 583.