FINANCIAL INFORMATION SECURITY IN THE CLOUD

Bogdan Ştefan Ionescu[1]
Laura Elena Tudoran[2]

ABSTRACT: For the romanian accounting market the implementation of specific accounting operations using cloud computing based solutions is now a reality. In this article we want to present the main security issues related to the financial data stored in the cloud, using both technically and financial specialists points of view.

Keywords: cloud computing, security, dematerialization of accounting documents

JEL Code: O324

Introduction

In situations of economic and financial crises as we have experienced in the last years, technologies like Cloud Computing and Business Intelligence (BI) are becoming increasingly important in gaining advantages over implementing expensive and complex software on-site (Pugna and Boldeanu, 2013).

Information technologies have changed the business environment and accounting is not being left out of the general progress of these technologies (Popescu, et al., 2009, Burinskiene, et al., 2010 Consoli, 2010 Christauskas C. and R. Miseviciene, 2012).

Currently, there are numerous definitions and interpretations given to the cloud computing concept. Expert Group (2012) believes that the responsibility for the existing confusion regarding the definition of this concept and its characteristics belongs primarily to the great variety of cloud service suppliers offering different capabilities, and secondly to the fact that the terminology used among the cloud's framework interferes with other domains such as Data Centre Clusters, Grids, High Performance Computing, Web Services (Olteanu, 2010).

The Romanian Court of Auditors defines cloud computing as "a style of computing in which the use of IT capabilities are provided as a service and allows users to access distributed services based on new technologies via the Internet without the knowledge, expertise or control of technological infrastructure to support these services".

Cloud security

Securing an information system involves identifying the unique threats that must be addressed through appropriate actions. Due to its design and architectural characteristics, cloud computing provides a number of security advantages such as centralized security and data segmentation processes, redundancy and high availability.

While many traditional risks are balanced due to the unique characteristics of the cloud infrastructure, risk assessment are required in areas such as availability and reliability, data integrity, recovery and privacy, and auditing.

Jaeger, Lin and Grimes (2008) believe that in order to start the analysis of the cloud security issues one must consider the user's expectations. They identify the minimum expectations of users as:

[1] Academy of Economic Studies, Bucharest, Romania, *e-mail: ionescub@gmail.com*
[2] *e-mail: tudoranlaura@gmail.com*

- Reliability and responsibility: users expect the "cloud" to be a reliable resource, especially if the cloud provider takes over the task of running important applications and they will expect clear delimitation of responsibility in case of serious problems.
- Security, privacy and anonymity: users expect cloud provider to prevent unauthorized access to their data and code and that sensitive data will remain private. Users can also expect that the cloud provider, other third parties or authorities will not monitor their work. The only exception might be permitted to cloud providers who need to monitor the activity in order to control the quality of service provided.
- Access and use restrictions: users expect to access and use the cloud when they want, without obstacles from the cloud provider or third parties, and they need assurance that their intellectual property rights are respected.

Jamil and Zaki (2011) and Scarfone, Singhal and Winograd (2007) identified the following major risks to security in the cloud:

1. Loss of government: while using the cloud infrastructure the user gives the required amount of control of a certain number of issues that might affect the security to the cloud provider.
2. Lock in: today there are fewer offers of tools, procedures or standard data formats or services interfaces to ensure portability of data, applications and services. This slows down the migrating process of customers from one provider to another or transferring services to a different IT environment. This introduces a dependency on a specific cloud provider to provide services, especially if data portability is not enabled.
3. Privacy: in some cases it may be difficult for a customer to check effectively cloud data handling practices of the cloud provider. This problem is accentuated when multiple data transfers occur. On the other side, cloud vendors do not provide information on the data processing practices. On the other hand, some cloud providers offer either information about data processing practices or certification summaries on data processing and data security activities (e.g. SAS70 certification).Log file analysis can detect possible attacks or system vulnerabilities (MIHAI et. all, 2008).
4. Incomplete or unsafe erasing of data: when a request is made to delete a resource from the cloud, as in most operating systems, it does not delete the actual data. Adequate or in a timely manner deletion of data can be impossible (or undesirable from the customer's point of view), either because of the unavailable additional copies stored, either because the disk which contains data that must be destroyed also contains other clients data. Sharing and reusing hardware resources it is a risk to the client, not to the dedicated hardware.

In Armbrust's vision (2010), cloud users are facing security threats that concern both the cloud inside and outside.

Unlike data centers, in the cloud, the responsibility for safety is shared between users, cloud provider and other providers. The user is responsible for cloud security at the application level and the cloud provider is responsible for physical security and foreign policy firewall application. The intermediate layer of security for the multitude of software is shared between the user and the operator. As the abstraction layer is exposed to the user is reduced, the responsibility for security increases.

Armbrust (2010) believes that virtualization is a primary mechanism for security in the cloud as it provides a strong enough defense and protects users or the cloud's core infrastructure against most attack attempted by other users. Armbrust also noted that not all resources are virtualized and not all virtualization environments are free of bugs.

In general, security concerns important aspects of confidentiality, integrity and availability, making them building blocks that are used in the design of security systems. These important aspects of security are applied to three categories of assets to be secured, namely data, software and hardware resources.

a) Confidentiality

Confidentiality refers to the ability of individuals or of authorized systems to access the protected data. The threat of data compromise is increased the cloud due to the existence of a large number of access points. The existence of large number of access points in the cloud is due to the high number of users, devices and applications that can access the cloud.

Delegating the control data in the cloud, indirectly leads to an increased risk of compromising the data as it becomes available to a large number of users. Many concerns appear about resource sharing, remanente data, application security and privacy.

Cloud computing is based on a business model in which resources are shared (e.g. multiple users access the same resource) on a network, a host and an application level (D. Zissos and D. Lekkas). Although users are isolated to a virtual level, the hardware is not separate. In a shared architecture, a software application is designed to virtually partition the data and configuration so that each client organization canwork with a virtualized and customized instance of the application.

Zissos and Lekkas are comparing resource sharing in the cloud with multitasking in a bid to highlight that both are subject to similar security threats targeting privacy. In computing, multitasking is the method by which multiple processes share the same processing resources (CPU).

Reusing objects is an important feature of cloud infrastructures, but they must be carefully controlled lest they create a serious vulnerability. Confidentiality could be breached unintentionally due to data remanence. Data remanence is the residual representation of data that were nominally erased or removed. Given the virtual separation of logical units and the lack of separation between hardware multiple users on a single infrastructure, data remanence can lead to unintentional disclosure of private data. Also maliciously, a user may require a large amount of disk space and then try to "cleanse" sensitive data.

Privacy in the cloud is related to user authentication. Protecting user account from theft is part of a broader problem of controlling access to objects, including memory, devices, software, etc.. Electronic authentication is the process of establishing confidence in the identity of a user. The lack of a strong authentication system may facilitate unauthorized access to a user account on the cloud, leading to a breach of confidentiality.

Software privacy is as important as privacy in the global security system. Software privacy refers to the confidence that certain applications or processes will maintain and manage users' personal data in a secure manner. In the cloud, the user is obliged to delegate "trust" in applications offered by the organization owning the infrastructure. Applications that interact with the user data must be certified that they will not introduce additional risks to confidentiality.

Unauthorized access can become possible by exploiting vulnerability in an application or lack strong authentication, creating privacy issues. In addition, the cloud provider is responsible for ensuring safe cloud instances.

b) Integrity

Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. Data integrity refers to protecting data from unauthorized deletion, modification or tampering.

Managing access rights to an entity and its specific resources and services ensures that data values are not abused, diverted or stolen. Unauthorized access to the database can lead to inappropriate change or delete of data, including the recording of unauthorized or non-existent transactions or inadequate recording of transactions (Geambaşu, 2010).Cloud-enabled resources can be abused because cloud providers reallocate IP addresses when a customer needs a specific address. Once an IP address is used by a customer, it is available for another client after a period of time. Cloud providers save money and do not need so many IP addresses if they reusethem, so it is in their best interest to reuse IP addresses. The existence of multiple IP addresses inactive or already in use represents a vulnerability of the cloud provider that facilitates resource abuse. There is a significant amount of time between the moment when the IP address is changed and the moment

when the DNS cache that holds the IP address is deleted. If these old or used IPs are kept in the cache then they can be accessed by giving the user access to resources available from the IP address. Also, a customer of the same cloud provider would be able to get access to the resources of another client by simply browsing through the provider network if security measures are not strong. Data and information is a bargaining chip for terrorists / cybercriminals and since the cloud can hold large amounts of data it becomes an attractive target for them, that's why security measures should not be overlooked (Wayner 2008).

By preventing unauthorized access, organizations can achieve high system reliability and data integrity. In addition, these mechanisms provide greater visibility in determining who or what changed the system data or information that may affect their integrity.

Authorization is the mechanism by which a system determines the level of access a particular authenticated user to secured resources controlled by the system. Considering the large number of entities and points of access to the cloud the authorization is important for ensuring that only authorized entities can interact with the data. A cloud provider is responsible for maintaining data integrity. The cloud presents a number of threats which include sophisticated insider attacks on such data attributes.

Software integrity refers to the protection of its deletion, alteration, theft or forgery. Deletion, alteration or falsification may be intentional or unintentional. Cloud computing providers apply a set of software interfaces or APIs that customers use to manage and interact with cloud services. In addition to the aforementioned threats, cloud security services depend heavily on the security of these interfaces. In the cloud, the responsibility to protect the integrity of the software is transferred to the owner or administrator. The integrity of the network and hardware is an additional issue to be addressed by the cloud provider because of the burden of protecting the hardware from theft, alteration and falsification.

c) Availability

Availability refers to the ability of a system to be accessible and easy to use at the request of an authorized entity. The availability of the system includes its ability to perform operations even when authorities have a certain strange behavior. The system must have the ability to continue operations even if a security breach occurred. Availability refers to data, software and hardware. Harnessing the user's hardware infrastructure applications creates a high dependency on network availability. The network is so loaded with the extraction and processing of data. The cloud's owners must ensure that the information and its processing are available to customers on request. Cloud services present a strong dependence on resources from infrastructure and network availability at all times. Understanding and documenting the specific requirements of users is imperative to design a solution that aims to ensure these needs.

Checking identities that share many fundamental safety requirements and determining the needs for data protection and information security can be the most complex step in designing a system. The multiuser environment is subject to unique security challenges, depending on the level at which the user operates: application, virtual, physically.

Research methodology and the obtained results

Our research aimed to identify the attitude tof both echnical and financial professionals regarding major security issues in cloud financial data.

The questionnaire developed by the research team and distributed to employees of the accounting and development departments of a company that provides IT services in Bucharest in November 2012 - March 2013 both electronically and in classic format included the following categories of respondents:

A. Accounting Specialists divided in:

A1. Accountants performing internship

A2. Accountants who work full time

A3. Accountant-general

B. IT Specialists divided in:

B1. Developers performing internship

B2. Developer working full-time

B3. Lead developer

After the initial processing of the statistical data obtained after applying the interview technique, 20 usable responses from IT and accounting specialists were obtained. The distribution of the responses by category of respondents is the following one:

From the accountants included in the internship program (A1) resulted 2 usable responses, representing 10% of the total

- From the accountants who work full time (A2) resulted 7usable responses, representing 35% of the total
- From the accounting-general (A3) resulted one single usable response, representing 5% of the total.
- From the developers who are included in the internship program (B1) resulted in 2 usable responses, representing 10% of the total
- From the developers who work full time (B2) resulted 7 usable responses, representing 35% of the total
- From the lead developer (B3) resulted one single usable response, representing 5% of the total.

After processing the data obtained through the questionnaire we obtained the following results:

1. **The "cloud computing" technology provides data security in transit**: 65% of the respondents said that the security of data in transit is important, 35% of respondents believing that the security of data in transit is not a criterion in choosing the cloud service provider. 60% of the accountants surveyed and 70% of the developers surveyed said that security of data in transit is important.
2. **The "cloud computing" technology ensures the security of the stored data**: 75% of the respondents stated that stored data security is of major importance, 25% of the respondents believing that the security of the stored data is not a criterion in choosing the cloud service provider. Of the 75% that said that the stored data security is of major importance, 46% are accountants, the remaining 54% being developers. Of the 25% who think that the security of the stored data is not a criterion in choosing cloud service provider, 60% are accountants, the remaining 40% being developers.
3. **The confidence in cloud service providers that have certifications**: 80% of the respondents said they prefer a cloud service provider that has certifications, while 20% of the respondents are not interested in cloud providers with certifications. 70% of the accountants surveyed and 90% of the developers surveyed said they prefer a cloud service provider that has certifications.
4. **The authentication system's security**: 80% of the respondents said that the authentication system's security is an important criterion in the decision to migrate to the cloud, 20% of the respondents believing that the authentication system's security is not an important criterion. Of the 80% who said that the authentication system's security is an important criterion in the decision to migrate to the cloud, 43.75% are accountants, the remaining 56.25% being developers.
5. **My data is separate from other customers data**: 90% of the respondents said that the separation of their date other customers data is of major importance, 10% of the respondents believing that data separation can be achieved only in 40% of the situations. Of the 90%of the respondents that said that the separation of data from other customers' data is of high

importance, 44% are accountants, the remaining 56% being developers. The 10% who believe that such separation cannot be fully ensured are accountants.

6. **The cloud service provider complies with the laws and regulations applicable to the concept of cloud computing**: 80% of the respondents said that compliance with laws and regulations applicable to cloud computing is a criterion in choosing cloud service provider. 43.75% of them are accountants, the rest being developers.
7. **The existence of a disaster recovery plan**: 85% of the respondents said that the existence of a disaster recovery plan is of major importance. 47% of them are accountants, the rest being developers.

Conclusions

Our research aimed to identify the attitude of both technical and financial professionals to key financial data security issues in the cloud. The study's results showed that for the accountants, the stored financial data security, the data security in transit and the cloud provider's certifications are the most important criteria in choosing a cloud provider. For the developers, the most important criteria in choosing a cloud provider are related to data security, the authentication system's security and the existence of a disaster recovery plan.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph , A. D., Konwinski, A., Lee, G., Rabkin, A., Stoica, I., Zaharia, M., 2010, A view of cloud computing, Communication of the ACM, Vol. 53 No. 4, pp. 50-58.
2. Burinskiene, A., & Burinskas, A., 2010, Investments into E-Business Technologies, Economics and Management, 15, 886-892.
3. Christauskas, C., Miseviciene R., 2012, Cloud Computing Based Accounting for Small to Medium Sized Business, Inzinerine Ekonomika – Engineering Economics, vol. 23, no 1: 14-21
4. Curtea de Conturi, 2012, Ghidul de Audit al Sistemelor Informatice, Bucureşti, available at: http://www.curteadeconturi.ro/sites/ccr/RO/Control%20si%20Audit/Documente/GHID_AUDIT_IT_CCR_24102012.pdf
5. Expert Group, 2012, Advances in Clouds. Research in Future Cloud Computing, Public version 1.0, European Commision, Information Society and Media, available at: http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-finalreport-experts.pdf, accessed on January, 27th, 2013.
6. Geambaşu, C., 2010, Evaluarea mecanismelor de control intern specifice tehnologiilor informaționale în cadrul auditului financiar, Revista Audit Financiar, nr. 9/2010, 2010, ISSN format electronic: 1844 – 8801, ISSN format tipărit: 1583 – 5812
7. http://blog.savvis.com/2011/06/five-security-questions-to-ask-your-cloud-provider.html
8. http://cloudhostingprovider.co.uk/cloud-computing/cloud-computing-security-questions
9. Jaeger, P.T., Lin, J., Grimes, J.M., 2008, Cloud Computing and Information Policy: Computing in a Policy Cloud?, Journal of Information Technology & Politics, Vol 5, Nr.3, pp 269-283
10. Jamil, D., Zaki, H., 2011, Cloud computing security, International Journal of Engineering Science and Technology, Vol 3, Nr 4, pp 3478 – 3483
11. Mihai F., Ionescu I., Aleca O. (2008), The auditing of e-business applications, Revista Contabilitate şi Informatică de Gestiune, nr 26
12. Olteanu C. C., 2010, Prevent, Backup and restore procedures for a web server, Lex et Scientia nr. XVII, vol. 1, p.483-489, Editura PRO Universitaria, ISSN: 1583-039x

13. Popescu Veronica Adriana, Popescu N. Gheorghe, Popescu Gh. Cristina Raluca, 2009, The Effects of Informatics Revolution on Organizing the Modern Management, Accounting, Control and Financial Audit **(**Efectele revoluției informatice asupra organizării gestiunii moderne, a contabilității, a controlului şi a auditului financiar**)**, Metalurgia International VOL XIV, Editura Ştiințifică F.M.R., Special Issue N0. 12/2009, pp. 156-164, ISSN: 1582–2214.
14. Pugna I., Boldeanu D. M., (2013), Integration of knowledge management and businessintelligence initiatives in a collaborative intelligence framework, 8thInternational Conference Accounting and Management Information Systems AMIS 2013, published inProceedings of International Conference Accounting and Management Information Systems 8thedition, pp. 444-459, ISSN: 2247-6245
15. Scarfone, K., Singhal, A., Winograd, T., 2007, Guide to secure web services, available at: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf
16. Wayner, P., 2008, Cloud versus cloud – A guided tour of Amazon, Google, AppNexus and GoGrid, InfoWord
17. Zissis, D., Lekkas, D., 2010, Addresing cloud computing security issues, Future Generation Computer System, pp583-592