Audit financiar, XIV, Nr. 3(135)/**2016**, *302-311*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Auditing Security for the Cloud

Dragoş Marian MANGIUC,
Bucharest University of Economic Studies,
e-mail: mangiuc@gmail.com

Abstract

Following the pattern of any major paradigm shift in the history of computing, the migration to cloud-based computing has known both praise and criticism. As its advantages, especially for the small and medium-sized companies, are too obvious to be doubted or questioned, the critics mainly focus on the drawbacks. Among the drawbacks, security is considered to be the most important.

The paper proposes an outline of the real image behind the many cloud computing security-related myths and misconceptions that an auditor has to deal with. The research is based on the literature review in the field of cloud-based computing and it is built starting from a synthesis of results achieved by means of a thorough analysis of the recent opinions and experience of Romanian and foreign auditors that were available for interviews. The main purpose of the paper is to find whether cloud-systems are more or less secure than traditional in-house systems from an auditor's perspective. The paper is part of a broader research process in the field of cloud computing and the neighboring technologies.

***Keywords**: Cloud computing security, Software as a Service, Platform as a Service, Infrastructure as a Service, Security audit*

***JEL Classification**: L86*

To cite this article:
Mangiuc, D.M. (2016), Auditing security for the Cloud, *Audit Financiar*, vol. XIV, no. 135-3/2016, pp.302-311, DOI: 10.20869/AUDITF/2016/135/302.

Permanent link to this document:
http://dx.doi.org/10.20869/AUDITF/2016/135/302.

Introduction

The field of security in the process of deploying, managing and auditing cloud-based applications is the main theme of criticism of the aforementioned software distribution system. While suppliers of cloud services advertise the new cloud-related technologies as the safest wave of technologies in IT history, often ignoring the obvious issues, skeptics tend to "demonize" the new paradigm, by presenting it as the end to true security and the beginning of a new and dark era, where privacy is nothing but a well preserved illusion. Both opposing views demand further analysis, as they tend to focus on collateral, and, in some cases, non-existent issues, and present them as the "great impediment of cloud technologies", often ignoring more important ones. Caught in the middle, the auditor has to further the analysis and improve own knowledge to a reasonable level, so as not to fall in an "extremist" position and compromise professional fair-mindedness.

The cloud computing paradigm, by its nature, cannot be completely different from the previous approaches for the management and use of software applications, and, therefore, it inherits much of their associated security concerns. On the other hand, the delivery and use of software applications via Internet makes them highly dependent on the nature and operating features of the network, which leads to a whole new wave of "Internet-inherited" security problems which are completely omitted in many instances (intentionally or not), by both the supporters and critics of the new approach. Some of the issues brought forward as "major reasons for the failure" of the new technology are, in fact, as old as information technology itself, and time has proven unequivocally to what extent (and at what cost) the associated risks may be managed or minimized.

The present paper aims to use both the literature relevant to this field (which is becoming more consistent every day), and the data collected by interviewing professionals involved in the process, locally and internationally, to achieve a clear image of an auditor's perception over the real cloud security issues, unaffected by commercial interests or aggressive marketing policies, which are usually characteristic to any new product on the market. Although currently there are not sufficient quantitative data to propose a coherent model for the estimation of a cloud computing system security or to formulate a comparison with traditional information systems (which is the purpose of a more extensive research in the field), it is possible to comparatively estimate the levels of security for both types of systems.

1. Research methodology

This paper is one of the results of a broader research in the field of cloud computing and *Enterprise 2.0* technologies, and it develops a research in the field of computer-assisted audit tools and techniques.

Wherever possible, a direct identification of the practitioners' expectations was attempted by means of direct interviews and also by means of a questionnaire. The questions for the empirical study were designed so as to get unbiased, objective answers. The members of the target group were encouraged to add their own observations regarding the questionnaire. Validation of the research conclusions was performed by means of an informal discussion with practitioners, members of organizations which performed or are in the process of performing a migration to cloud-based services. Also, professionals from a cloud migration assistance and consulting company were interviewed. Some of the discussions and conclusions in the paper are based on the results of previous scientific or market research studies.

2. Who is the real owner of cloud-based information?

On August 17th, 2009, the United States Justice Department publicly announced that 130 million credit card numbers were stolen, in what was to become the largest identity theft in information technology history (US Department of Justice, 2009). A few days after the announcement, the author, in the person of a former secret services employee, specialized in tracking and identifying hackers, was formally charged of stealing credit card data by exploiting security deficiencies in major retailers' computer networks.

Based on the aforementioned fact, it can be noted that many breaches in security systems do not arise from the negligence of those responsible, but as a result of extremely ingenious attacks by experts in the field of information systems security, whose expertise exceeds, in some cases, the typical knowledge level of the

employees of a company dealing with the implementation of security mechanisms, and sometimes, even the experience of the experts entrusted to audit the security level of the aforementioned systems. Therefore, although companies continuously assess and periodically reassess the level of security risks, implement internal control systems, install and configure firewall equipment and other assimilated technologies, establish backup processes and protocols and request for audited security features for the acquired hardware and software equipment, security breaches continue to occur. In addition, more and more frequently, providers of security solutions offer new alternatives, considered to be 100% secure, which obviously proves to be at least an exaggeration.

Looking back in time, one of the most famous "miraculous" security solutions was *Kerberos*, offered at the beginning of the '90s as the universal solution to computer security (Perez-Mendez et al., 2012). However, its glory soon faded (Bajpai, Vardhan and Kushwaha, 2012), and the associated security issues continued to exist. A few years later it was believed that the NASA information system had reached the absolute level of information security (Reed, 2012). Nevertheless, the few successful attacks have led to a NASA computer system security audit by the Congress of the United States, through its investigative body, called the *General Accountability Office – GAO* (Purpura, 2013). Audit findings have revealed that the results reported by the space agency were highly exaggerated, and the implementation costs for the security systems were not justifiable in correlation with the results (Berriman et al., 2012). NASA was not the only organization to exaggerate the results in the field, as subsequent attacks on *Microsoft* and *Citibank* revealed a real trend in this respect (Nunes and Merrihue, 2007).

Based on the review of the relevant literature in the field, the following conclusions can be stated:

- The data on Web servers are, in the majority of cases, unencrypted, as security systems focus on limiting outside access and trying to build a "wall" around every server; once the wall is penetrated, there are no more internal security systems in place;
- Most on-line transactions do not have a *post factum* auditing system; the audit is performed on the security system as a whole, and the results are subsequently extrapolated to all transactions;
- The manner software providers and their users manage their own systems' security is far from being transparent (and that is understandable, in most cases).

All these phenomena have been observed a long time before the emergence of the cloud computing model, and, therefore, the cloud cannot be held responsible for their existence. The main difference is that even if such cases existed before the emergence of cloud computing, they were relatively isolated, and, therefore, the negative effects were relatively easy to manage, and security breaches were soon being covered. The emergence of cloud computing has led to the existence of millions of servers, with a number of client accesses that would have seemed impossible a few years before (Han, Susilo and Mu, 2013). The best proof in this respect is the famous "crisis of the IP addresses", which showed that, at that point, even the Internet was reaching its physical limits. Under these circumstances, for an auditor, it is compulsory to find the correct answers to two essential questions:

- Who is the real owner of the information stored in the cloud?
- Which stakeholders are primarily responsible for the security of the information stored in the cloud?

The answer to the first question seems to be "the organization which benefits from the cloud-based services and takes the role of the user". The pieces of information a cloud service provider stores and manages belong to its customers, its employees, its accounts etc. Consequently, the security issues become highly debatable, as it becomes obvious that informational values are not managed and monitored by their rightful owner, but by an external entity (the cloud infrastructure provider).

This "reversal" of responsibilities leads to a second important question: Does the cloud provider assume the legal responsibility in the case of data leaks or identity theft, covering all damages? To the knowledge of the author, and also in the opinion of some surveyed auditors (Li et al., 2013), the cloud has not yet been tested in the judicial system, as there have not yet occurred any cases or issues important enough to create a precedent; however, the behavior of information services providers in similar cases (although not involving cloud computing) cannot be considered as reassuring. For example, in a case of identity theft,

hackers have "cleared" a French bank's customer entire credit line. Under these circumstances, the bank not only did not assume any of the blame, but it requested the payment of installments by the customer, with interest, for the full amount stolen by hackers. A court of law has ruled against the bank's intent to charge interest, but it did not order the latter to bear the amount stolen, as the account management was performed by the customer through an *Internet banking* service, and not by the bank (Edwards, 2014).

Identity theft usually follows a standard model. The offender is in the possession of an essential set of basic information about the victim (identity information, passwords, account numbers, etc.), that is used in order to access the victim's financial resources and even new financing opportunities (credit lines, credit cards, and so on). It is even possible that the offender makes a series of deposits and loan payments for a while, so as to increase the credit limit and not to arouse suspicion, pending a final large hit. The moment the debt is overdue, the creditors will turn to the victim as the real debtor, and the latter will have to initiate legal actions to identify and prosecute the perpetrator, otherwise being solely responsible for the loan payments. Considering that, according to a recent study (Ren, Wang and Wang, 2012), only in the United States alone there are about 750.000 successful identity theft attempts every year, the obvious question is: "Will the set of cloud technologies allow for a worldwide recurrence of this scenario?" Unfortunately, the answer cannot be given as easily, since it is not that obvious.

3. Responsibility vs. accountability

The analysis of the current situation leads to the conclusion that in the absence of coherent cloud security management, the negative phenomena caused nowadays by security breaches will likely increase by an order of magnitude. A recent study of the manner in which contracts are negotiated between cloud services beneficiaries and providers (Carlsson and Fuller, 2013) suggests that if a cloud services beneficiary will suffer major damages from computer crime while its database is hosted by a cloud provider, that provider will not be held liable for any part of the consequences. From an auditor's point of view, this perspective is at least interesting, given that the level of security and servers access control is ensured completely by the company that owns the servers (the cloud provider), and not by its customers. Therefore, the providers of cloud services should have clear and direct legal responsibility for the safety and protection levels associated with the service they provide. In addition, the organizations benefiting from these services should understand that the term "public cloud" involves the following:

- The level of access is arranged so as to allow free access to all the potential beneficiaries of the service;
- The service recipients may be individuals with malicious intentions, posing as legitimate users.

From a conceptual point of view, security objectives are implemented through a set of applications and service design principles (which define the conceptual framework of security technologies), as well as through hardware devices and software applications that implement the defined framework. By its nature, technology has a dual character, as the design principles that implement security and the principles that generate cheaper and more flexible operational systems are often conflicting, forcing organizations to achieve unwanted but unavoidable compromises. These conflicts occur not only between IT technologies, but are also affecting the underlying business processes. If the premise is accepted that the use of cloud technologies allows for costs cuts and facilitates access to services, then every increase in service access leads to a proportional increase in security concerns (or the number of attempted frauds).

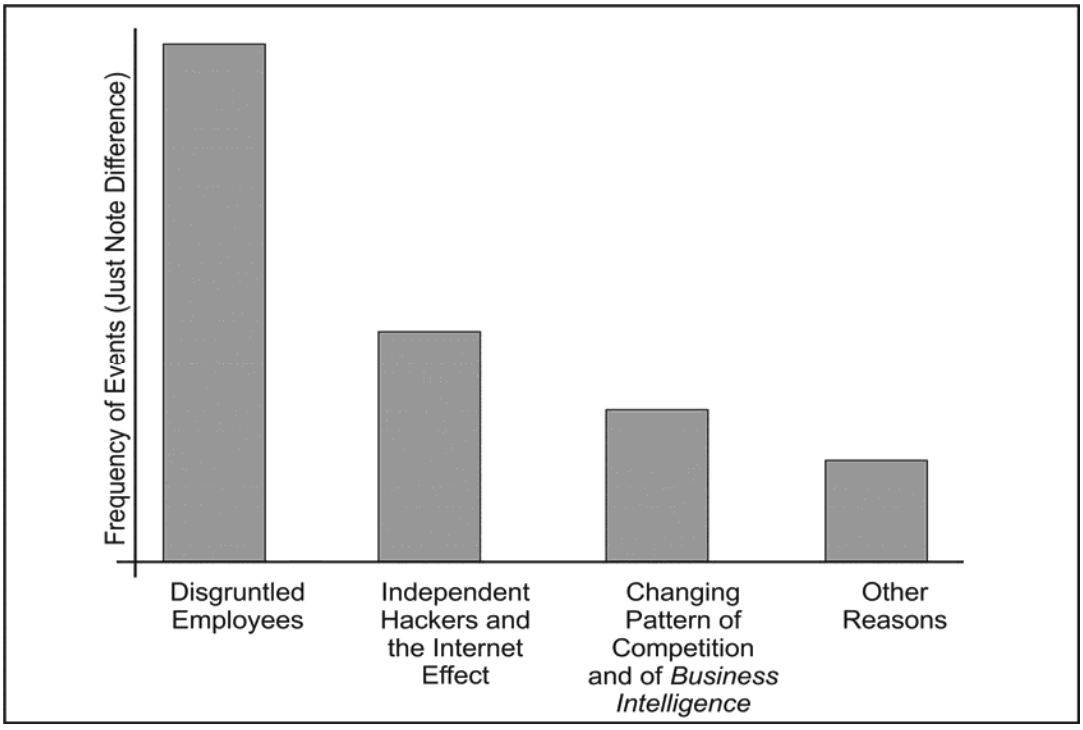
It can be considered that, sooner or later, everyone will try to benefit from cloud computing services, because most of them are available for free and are supported by advertising. If a cloud-based e-mail service is provided free of charge, the real costs of this service can be completely invisible to its users and, by consequence, the weight of security measures and data privacy enforcement in the total cost of the service will be completely unknown to a recipient of the service. These issues are becoming more relevant not only for the current cloud services recipients, but also for the companies exploring the possibility of a migration to the cloud. SMEs are attracted to a cloud-based electronic mail offer, especially if it allows the direct integration (through the browser) of other applications, like customer relationships management or enterprise resource planning applications. However, as the number

of service beneficiaries increases, security concerns are beginning to take shape. Empirical evidence (Pervez et al., 2013) reveals that "to a certain extent" consumers are willing to give up their privacy in order to enjoy a completely free of charge service; nevertheless, when that threshold is exceeded, the situation must be reevaluated. A survey conducted among users of such services, holding advanced knowledge in computer science, has led to the following results:

- When asked "*Do you believe that you have a sufficient level of control over personal data?*" over 87% of the respondents provided a positive answer, using the current legal provisions concerning the processing of personal data to argue the expressed opinion.
- When asked "*Are you aware that the service provider has the right to use your personal data to target the advertising process?*" only 32% of respondents had a positive response, and they believed that the possibility to edit their profile is an efficient solution to this particular problem.

All of these aspects, whether of technical, personal, or business-related nature, affect the way individuals, companies and auditors perceive the security of information. In addition, the discussions with cloud computing professionals suggest that the explosion of cloud-based technologies will generate extremely complex and perhaps unmanageable responsibilities in the field of information security. Moreover, the possibility of "inside" attacks cannot be completely eliminated. A survey performed by the FBI in 2012 (US House of Representatives, 2012) reveals that the number of malicious attacks made by disgruntled ex-employees is twice as large as the number of attacks made by hackers. According to the same survey, third in line are "business intelligence" attacks, translated as economic espionage actions taken by competitors, also facilitated by the cloud-based technologies. The results of the survey are shown in **Figure 1**, as presented by the original source, without any quantitative information, its purpose being to provide awareness to the weight of each type of attack in the total of security issues.

Figure 1. Origins of information security risks



Source: FBI, 2012.

When compared to public cloud systems, the private cloud infrastructure is better in terms of security, as the user organization also has ownership and full control over the service infrastructure. However, most private cloud structures have broadband connections to public cloud systems (in order to assure elastic scalability), which does not render them immune to the security issues affecting the public services.

The solution to keep cloud systems risk at a manageable and reasonable level is the formulation and the enforcement of common security standards both at the level of cloud service providers and the level of the user organizations. Moreover, at the level of the European Union, or even at an international level, the foundation of a cloud security and auditing authority, endowed with regulatory and enforcement powers is a must. Even if a lot of voices (both inside and outside the academic environment) have stated the need for such an organization, the proposal was not really taken into account by the ones empowered to regulate the foundation and the functions of such an authority.

As revealed by a previous survey (Mangiuc, 2012), the organizations benefiting from cloud services should be more realistic when dealing with security issues, starting from the moment the services are contracted. Some of the surveyed organizations seemed to massively neglect security issues, and stated that the cost cuts allowed by the migration to the cloud are far too important to be missed. Under these circumstances, it is obvious that the migration from an *in-house* solution to a cloud-based solution will require a trade-off between security, performance and costs. However, the following rules are considered to be of outmost importance:

- The security level required from a cloud services provider should not be assessed based on the offered price, but on the level of the operational risk involved;
- Major trade-offs in the field of security reveal, essentially, a huge lack of professionalism from the management of the user organization, which may render the managers directly responsible and accountable in the event of a massive information leak having major consequences at the business process level. The auditor has an obligation to express concerns if such a situation occurs.

Such carelessness may prove to be extremely harmful for the user organization and also very expensive from the legal point of view, both at security and conformity levels. Inside the European Union, a quite detailed regulation package is in force. The package includes:

- The 1999/93/EC Directive on a Community framework for electronic signatures;
- The 2000/31/EC Directive on electronic commerce;
- The 97/7/EC Directive on the protection of consumers in respect of distance contracts;
- The 2002/65/EC Directive concerning the distance marketing of consumer financial services;
- The 2002/58/CE Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.

In addition, the providers and beneficiaries of cloud-based services must take into consideration the global nature of this technology, and the fact that many state authorities require, through their own legislation, the preservation of personal data and copyright materials within their own state borders.

The legal foundation of the relationships between cloud services providers and beneficiaries is represented by the Service Level Agreement Contracts (or SLA's), which, in many cases, are limited to the general terms definition of the security-related obligations, without openly identifying the security protocols, standards, and procedures which are mandatory to be used for clients, servers, network routers and hubs, network bridges, connection concentrators, firewalls and other equipment which implement the security policies. Such practices cannot be but harmful for all the stakeholders, as information systems security is declared to be a key competitive differentiator and a key performance indicator for both the users and the providers of cloud-based services. When SLA contracts will include bullet-proof clauses regarding responsibilities of each of the involved parties in the field of security, such agreements will lead to safer, security-enabled architectures, starting from the analysis and design phases.

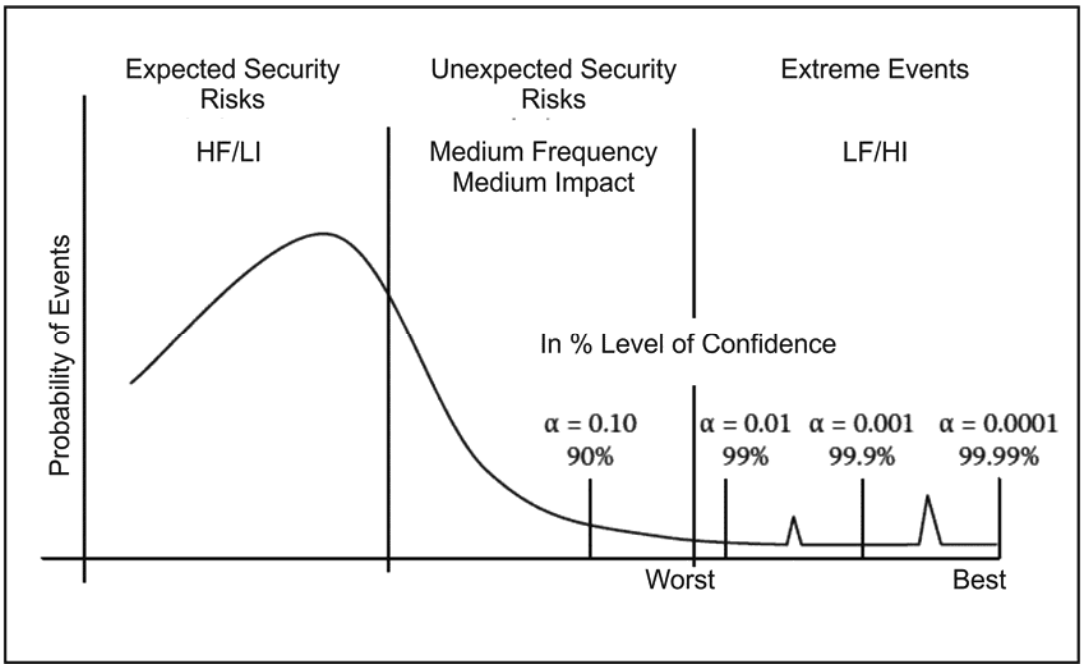
4. A security prioritization model proposal

As a general answer to all the aforementioned issues, the author intends to build a model able to allow a cloud services provider, consumer or auditor to assess the real priorities in the field of security. The first stage of the

model implies the identification, the analysis and the evaluation of the vulnerabilities attached to the chosen cloud-based solution. There is a large possibility that the model will generate a very long list of vulnerabilities and possible threats, but not all of them will be major concerns for the company.

The major criteria for the priority of a security threat should be as follows: a vulnerability bears high security risk if its exploitation may expose or compromise a physical or intellectual property asset of the company. Moreover, the threats that are considered to have high priority must be cross-checked against all other vulnerabilities, in order to assess the combinations that have the maximum destructive effects. As the frequency of certain vulnerability can be determined on a statistical basis (based on internal or external relevant data), the aforementioned procedures can be employed in order to determine the impact of vulnerability (**Figure 2**).

Figure 2. The vulnerability impact determination model



Source: Mangiuc, 2016.

By taking and adapting the operational risk assessment-specific approach, the subsequent directions will be followed:

- *High frequency, low-impact events* (HF/LI) – which may be addressed by using the currently available control system, at least until a coherent security policy design process is performed.
- *Medium frequency, medium impact events* (MF/MI) – the *known unknowns*, will require the creation and analysis of different scenarios able to project their possible effects at the level of the cloud-based infrastructure.
- *Low frequency, high impact events* (LF/HI) – the *unknown unknowns*, which require the adequate design of dedicated elements in the field of security strategy.

Assuming the information systems have access to a minimum of audit tools and techniques, a continuous sampling process may reveal the deviations from the normal system use (such as unnatural server load, a large number of requests having the same source etc.). The trust level for the LF/HI events should be at least 99.99%, which means at most one case in ten thousand may escape undetected to the infrastructure monitoring

system. Such a goal cannot be fulfilled at once, but only after a reasonable time lapse, through repeated analysis and increased levels of experience.

The actions presented and proposed by the current paper are also based on a series of best practices in the banking industry, designated to identify and monitor the operational risk level, as requested by the Basel Committee on Banking Supervision (Chorafas, 2004).

The aforementioned analysis pattern provides the auditor with the ability to discover vulnerabilities and the ability to establish priorities. No company, whatever its size, can afford to follow and address all the discovered vulnerabilities at once, so, it has to concentrate first on the vulnerabilities having high impact risk, no matter how low their frequency is. This approach, which may be called *the design of a security policy*, should be centered on the selection of the most efficient counter-measures (from an economic point of view), so as to decrease exposure to high impact vulnerabilities:

- A significant increase in the costs incurred for each attack by a hacker or an intruder who has found a security breach;
- A decrease of the damages that an attack can cause, by establishing more complex internal control procedures, leading to a higher degree of integrity.
- The increase of the probability that the attack is detected and stopped before it reaches its final goal.

The aforesaid proposal is considered to be only a suggestion regarding the main directions for action, as, in order to reach maximum efficiency, the model should also enclose a large number of cultural and behavioral variables, which cannot be predefined, but must be carefully evaluated in each particular case (for example, the employees' knowledge level, the level of understanding and acceptance of the new security measures, the expected level of punishment, as stated in the enforceable legislation for the security-related crimes).

Moreover, the design of a distributed security architecture has to be performed, so as the final result will be able to search, capture and analyze the behavioral models at the network access and use levels. The distributed architecture approach is far more efficient than the centralized architecture approach (Pinzon et al., 2011), as it is more sensitive to the local behavior patterns at the network level, and it also generates less load on the network equipment. Such a security architecture must be able to gather all the proof and data required to document a security event, so as to serve the purpose of internal audit, an insurance claim, or a court of law. Studies (Munoz-Canavate and Hipola, 2011) reveal that one of the most important impediments companies in the European Union meet when instrumenting the legal action in the case of a security attack is to prove that the attack actually took place. Anomalies detection and identification mechanisms alert system administrators about the events or the connections that have not been observed before, or, if they have been observed, did not enter the attention zone of the alert systems. The use of learning-specific technologies (like neural networks, agent based networks, event identification systems, etc.) may significantly speed up the implementation process for a properly designed security system. These technologies may also be able to sensibly reduce the number of false alarms whose apparition is thought to be inevitable, no matter the nature of the system (mainly automated or mainly manual system).

Discussion and conclusions

The paper at hand identified the main types of security threats for a cloud-based information system solution, both the ones inherited from the previous generations of software solutions and the ones who arose as a consequence of founding the information system on the Internet connection.

Even if the foundation of an authority able to regulate and verify compliance for the enforcement of security requirements in the cloud was requested by many voices in the economic and academic environment, the idea was not really taken into account by the decision makers, which leads to the conclusion that, from an auditor's perspective, the fraud potential of the cloud-based infrastructure, as perceived by most of the user companies, has two major causes:

- The lack of standardized security practices whose implementation would be mandatory for the cloud services providers and consumers alike (and also would be verifiable by means of the Internet);
- The persistent ambiguity and uncertainty existent from the legal point of view, concerning the implementation mode and the scope of the legal framework applicable in the field of on-line businesses.

The risk to be held legally responsible for the manner cloud information was managed and protected belongs to the rightful owner of the aforementioned information, and the consequences of a faulty security management can become very serious, very quickly. As the paper at hand is trying to prove, the ability to provide a reasonable level of data security in the cloud is at least open to discussion nowadays, and is likely to stay that way as long as the increase in infrastructure complexity will outrun the increase in the efficiency of the security mechanisms.

Thus, the paper proposes a model blueprint for the identification and the prioritization of the security threats inside cloud-based software architectures, inspired by the operational risk assessment model, and able to be employed in order to describe the most important development directions for the security policies.

It may be concluded that designing the absolute and perfect security solution is an utopia, even in the cloud. However, this should not be a "deal breaker", as the recourse to the best available technologies and the use of imaginative techniques to gain protection against the cloud and Internet-specific security threats may significantly increase the efficiency and the impact of the recommended security solutions.

REFERENCES

1. Bajpai, D., Vardhan, M. and Kushwaha, D.S. (2012), Authentication and Authorization Interface Using Security Service Level Agreements for Accessing Cloud Services, *Contemporary computing, Book Series: Communications in Computer and Information Science*, vol. 306, no.1, pp. 370-382.
2. Berriman, B., Deelman, E., Juve, G., Rynge, M. and Voeckler, J.S. (2012), High-Performance Compute Infrastructure in Astronomy: 2020 Is Only Months Away, *Astronomical Data Analysis Software and Systems XXI Book Series: Astronomical Society of the Pacific Conference Series*, vol. 461, no. 1, pp. 91-94.
3. Carlsson, C. and Fuller, R. (2013), Probabilistic Versus Possibilistic Risk Assessment Models for Optimal Service Level Agreements in Grid Computing, *Information Systems and E-Business Management*, vol. 11, no. 1, pp. 13-28.
4. Chorafas, D.N. (2004), *Operational Risk Control with Basle II. Basic Principles and Capital Requirements*, Butterworth-Heinemann, London.
5. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
7. Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC.
8. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.
9. Edwards, C. (2014), Ending identity theft and cyber-crime, *Biometric Technology Today*, vol. 2014, no. 2, pp. 9-11.
10. Han, J., Susilo, W. and Mu, Y. (2013), Identity-based data storage in cloud computing, *Future Generation Computer Systems – The International Journal of Grid Computing and E-Science*, vol. 29, no. 3, pp. 673-681.
11. Li, M., Yu, S., Zheng, Y., Ren, K. and Lou, W. (2013) "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143.
12. Mangiuc, D. (2012), Cloud Identity and Access Management – A Model Proposal, *Journal of Accounting and Management Information Systems*, vol. 11, no. 3, pp. 484-500.
13. Munoz-Canavate, A. and Hipola, P. (2011), Electronic administration in Spain: From its beginnings to the present, *Government Information Quarterly*, vol. 28, no. 1, pp. 74-90.

14. Nunes, P.F. and Merrihue, J. (2007), The continuing power of mass advertising, *MIT Sloan Management Review*, vol. 48, no. 2, pp. 63-77.
15. Perez-Mendez, A., Pereniguez-Garcia, F., Marin-Lopez, R. and Lopez-Millan, G. (2012), A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network, *International Journal of Information Security*, vol. 11, no. 6, pp. 365-388.
16. Pervez, Z., Awan, A.A., Khattak, A.M., Lee, S. and Huh, E.N. (2013), Privacy-aware searching with oblivious term matching for cloud storage, *Journal of Supercomputing*, vol. 63, no. 2, pp. 538-560.
17. Pinzon, C.I., Bajo, J., De Paz, J.F. and Corchado, J.M. (2011), S-MAS: An adaptive hierarchical distributed multi-agent architecture for blocking malicious SOAP messages within Web Services environments, *Expert Systems with Applications*, vol. 38, no. 5, pp. 5486-5499.
18. Purpura, P.P. (2013), *Security and Loss Prevention – An Introduction (Sixth Edition)*, Butterworth-Heinemann, London.
19. Reed, B. (2012), The 8-Year Effort to Address Systems-Level Space Solar Power Issues for Us Government Satellite Programs, *2012 38th IEEE Photovoltaic Specialists Conference*, vol. 38, no. 1, pp. 2811-2814.
20. Ren, K., Wang, C. and Wang, Q. (2012), Toward Secure and Effective Data Utilization in Public Cloud, *IEEE Network*, vol. 26, no. 6, pp. 69-74.
21. US Department of Justice, Office of Public Affairs (2009), Alleged International Hacker Indicted for Massive Attack on U.S. Retail and Banking Networks. Data Related to More Than 130 Million Credit and Debit Cards Allegedly Stolen, [online] Available at http://www.justice.gov/opa/pr/2009/August/09-crm-810.html [Accessed February 10th, 2016].
22. US House of Representatives, Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management (2012), America Is under Cyber Attack: Why Urgent Action Is Needed", [online] Available at *http://www.hsdl.org/?view&did=707644* [Accessed February 10th, 2016].