International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:6, No:6, 2012

Addressing Data Security in the Cloud

Marinela Mircea

***Abstract*—**The development of information and communication technology, the increased use of the internet, as well as the effects of the recession within the last years, have lead to the increased use of cloud computing based solutions, also called on-demand solutions. These solutions offer a large number of benefits to organizations as well as challenges and risks, mainly determined by data visualization in different geographic locations on the internet. As far as the specific risks of cloud environment are concerned, data security is still considered a peak barrier in adopting cloud computing. The present study offers an approach upon ensuring the security of cloud data, oriented towards the whole data life cycle. The final part of the study focuses on the assessment of data security in the cloud, this representing the bases in determining the potential losses and the premise for subsequent improvements and continuous learning.

***Keywords*—**cloud computing, data life cycle, data security, security assessment.

I. Introduction

THE globalization, the technological development and the increased use of the internet have lead to the appearance of new business models and informatics solutions that would capitalize the technological opportunities and transform them in value offered to customers. Many implementations have evolved over time, due to the increased requirements and to the desire to exploit new technologies and communication media. These are added to the effects of the recession within the past years, which have intensified the focus on the development and use of solutions that maximizes the performance and minimizes the investment costs. The large investments in traditional IT (information technology) solutions are unpractical and unappealing most of the time. The solutions based on cloud computing, also called on-demand solutions, are thus becoming more popular [1].

The cloud computing and virtualization technologies are preferred by many organizations. A survey performed by Info-Tech shows that 76% of the IT decision makers are interested in private clouds that complies with the security requests and with the organization's standards [2]. Cloud computing will also acquire greater popularity in 2012, particularly in the Business Intelligence sphere. Although the number of users of cloud computing is in continuous growth, organizations are still confronted with adoption problems. A survey, performed in 2011 on a sample made up of 521 IT professionals, shows that the training of users in cloud computing (43%) and the security challenges (36%) are still barriers in adopting cloud computing [3].

Marinela Mircea, Department of Economic Informatics and Cybernetics, The Bucharest University of Economic Studies, Romania (email: mmircea@ase.ro).

The cloud computing-based solutions offer numerous benefits (fast development, lower costs, scalability, adjustability, payment for use, flexibility), but also challenges and risks specific for the cloud environment (regarding accessibility, virtualization, data verification, data loss, data security). As regards the types of specific risks of the cloud environment, identified and evaluated in [4], the focus of the present study is on data security risks. Security represents one of the major barriers in adopting cloud computing, and data protection and confidentiality continues to represent market challenges [5]. According to a study carried out by EDUCAUSE, based on 372 member institutions, these are considered peak barriers [6]. Approximately 75% of Chief Information Officer and IT specialists also consider security as the number one risk [7]. Data security assurance represents a necessity both for avoiding losses determined by security incidents and for complying with the legal regulations regarding the protection and access to information. A periodic assessment of security is also needed. Data security represents one of the four dimensions (efficiency and effectiveness; responsiveness and compliance; social responsibility and accountability; and security [8]) of the information systems audit. The information system audit focuses on the quality ensuring of the economic activities and processes within organizations [9]. Through the audit processes, we can discover, relatively fast, the weak points and parametrization issues of systems related to the specific of activities, which represent the object of implementation. Thus, it is possible to find answers regarding the data quality, the way of accessing and extracting data from the system, the structure of user rings and of content trees, the structure of data cubes and of aggregation-disaggregation type interrogations within the process of information compatibility and of data integrity and availability.

Any organization that adopts could environment will be confronted with challenges regarding the politics and the security of the shared data, and third party IT infrastructure [10]. These challenges, as well as the security risks specific for the cloud environment, reduce the effectiveness of the traditional protections means [11]. Some of the fundamental challenges of cloud security are data storage security, data delivery security, application security and third party resources security [5].

A special attention must be paid to the sensitive data in the organization (for instance, the critical source of competitive advantage, the key performance indicators). For that matter, some analysis must be performed at the level of organization in order to take decisions concerning the opportunity of data storage in cloud.

Here are some options [12]:
- maintaining the sensitive data within the organization's data centers and externalizing other data, with the risk of creating a great latency for several applications and users;
- externalizing all data in order to obtain performance and maximum scalability, with potential security risks.

The present study offers a complete approach on cloud data security, in terms of the stages of data lifecycle. The main risks and techniques/methods of data security protection are identified and presented for each stage. The final part of the study focuses on the assessment of data security in the cloud, as its stand for security improvement and continuous learning.

II.2 Ensuring Data Security in the Cloud

Ensuring data security in the cloud requires the identification and analysis of the risks and security measures/techniques that can be applied in every stage of data life cycle. The omission of one of the stages, at least in the case of the sensitive data for organization, may lead to important loss for the organization. Table 1 presents some examples of data security risks in the cloud, categorized according to the stages of data life cycle, namely: create, store, share, use, maintain and destroy.

TABLE I
Main Risks of Data Security in Cloud

Stage	Specific risks
Create	- Creation/discovery/actualization of data by individuals/unauthorized groups; - Data integrity issues created in unknowns geographic areas;
Store	- Unauthorized data access (to storage or movement of data between different locations); - Breach of legal regulations regarding data security that must be stored in different geographical locations; - Integrity/availability/confidentiality data issues; - Data loss and the impossibility of their recovery; - Insecure cryptography and poor key management;
Share	- Unauthorized data access; - Alteration of data integrity during transfer; - Internet protocol, Domain Name System server, Dynamic Host Configuration Protocol problems;
Use	- Data use by unauthorized persons; - Breaching legal regulations through the inappropriate use o data; - Use of data for other purposes than those they have been collected for;
Maintain	- Unauthorized data access; - Data loss and the impossibility of their recovery; - Deviations between the period of data retention and that established by the organization;
Destroy	- Data replication before their destruction and keeping copies; - Unauthorized data destruction; - Incomplete destruction of data (with possibilities of recovery).

The use of cloud computing involves certain changes in the traditional methods of data security. These are mainly determined by cloud-based architectures that lead to multi-tenancy and geographic diversity. The data security along their life cycle may be achieved on different levels (fig. 1). On every security level there may be applied different techniques/methods that would ensure the compliance of the security policy established at organization level. The data access will be achieved by following one or several security levels, according to the requirements established through the security policy.

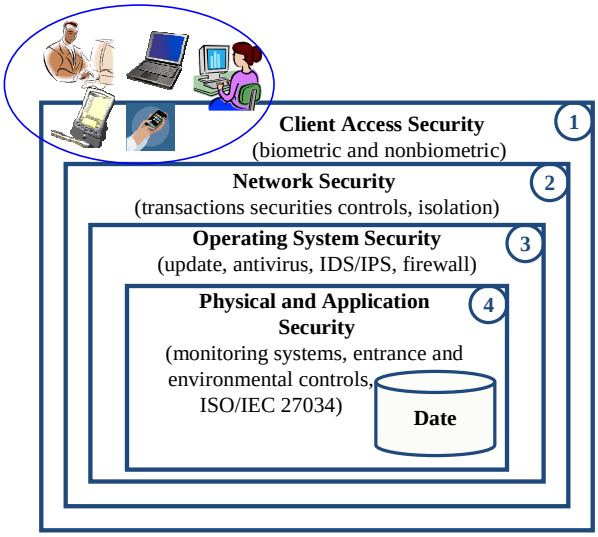

Fig. 1 Data security levels

The first level of security is represented by the user's authentication (by biometrical or non-biometrical means) on a device (laptop, computer, personal digital assistant) necessary to access data in cloud. After authentication, the user will access the network that protects the access to the data server through controls (level two). The security controls at the level of the operation system (level three) protects the access to applications and database. After authenticating on a physical level and on an application level (level four), the data access will be carried out according to the user's rights.

According to the chosen cloud model, data security and protection will be ensured in one/several/all stages of data life cycle using specific techniques/methods of control (fig. 2, adapted from [13]).

Any violation of security will also be researched in order to establish:
- if the respective data were compromised;
- if the unauthorized persons, who had or could have had access to data, show sufficient trust, so that the result of the compromise does not create prejudices;
- the impact and cost of data security violation;
- the corrective measures that are recommended;
- the cost of the corrective measures that will be applied.

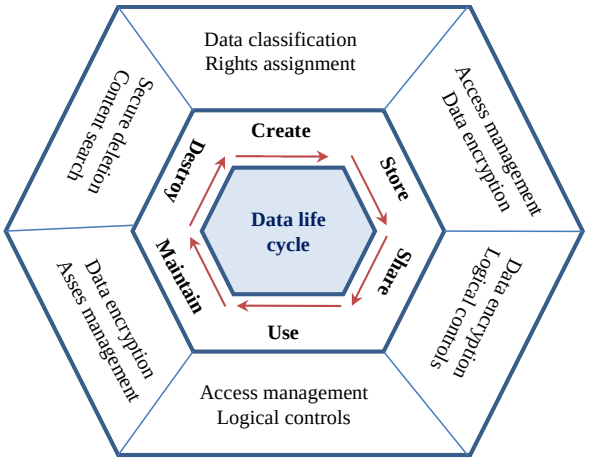

Fig. 2 Ensuring data security in cloud

A. Data Security on Creation

Data creation supposes the generation / discovery / actualization of digital content. Throughout this stage, data classification and rights assigning techniques can be used.

1) Data Classification

For the use of a cloud solution, any organization must adopt data classification schemes according to their level of confidentiality. The classification is important for the establishment of data strategies and for the profile of their risks. The classification demands the creation of certain data classes that can be accessed in cloud computing based on rights. Not all data offers the same value and not all require the same degree of protection. The data classification will be based on the assessment of risks and on the inadvertence impact, as well as on data loss. In order to illustrate this aspect, table II presents a data classification scheme for the business environment. It supposes three large data classes that can be further divided in subclasses.

TABLE II
EXAMPLE OF DATA CLASSIFICATION SCHEME

Class	Risk	Description
Public	Low	The data is public and demands a minimum control, necessary for the prevention of unauthorized modification or deletion. For instance, this category may include information of public interest regarding the activities or the results of activities of a public institution, according to Law 544/2001. Here are some examples: the regulatory documents that govern the organization and activity of the public institution, the organizational structure, the responsibilities of the departments, the working hours, the schedule of the public institution, the name of the persons managing the public institution and of the official responsible with the transmission of public information.
Private	Average	The data is available only for authorized persons and it requires an average security control. Here are a few examples of private data: information regarding personal data (according to the law), or information that may cause prejudice to protection measures of young people, when published.
Confidential	High	The data is available only for authorized persons and it requires a higher security control. We may consider as examples the critical data, with a high degree of sensitivity for the organization and that have to be protected against unauthorized access.

The classification is performed by persons authorized by the organization, with a preliminary notice from the executive coordinating the activity. The classification may be carried out manually (mainly for unstructured data) or automatically, through the logic of application (for structured data). Periodically, or when certain conditions are achieved, the reclassification of data takes place. Reclassification may occur if: a) the term of classification expired; b) providing information can no longer prejudice the interests of the holding persons/organizations; c) the classification was assigned by an unauthorized person.

The security policy must comply with the valid legal regulations concerning data protection and information access. Here are some of the controls that can be applied in the creation stage: application logic (automatically, through key words, content analysis) and labeling (manually, through key words, associations).

In order to choose the cloud model it is useful to perform a data analysis according to several criteria, such as mission, sensitivity, volume, integrity, availability. Moreover, this analysis helps to identify the models and security techniques according to each level of security.

2) Assignment of Rights

The process of rights' assignment supposes the application of rights to data, according to their classification. The rights/permissions may be assigned to individuals/groups and may limit the access to different devices/content and/or location. The technical controls that can be applied in assigning rights are security label, which implies associating a label to a data element, based on which there will be implemented logic and access controls and digital rights management [13].

B. Data Security at Storage

Data storage takes place immediately after their creation and it implies their saving into storage devices. Data can be stored in their initial form or can be encrypted, according to the security level associated to the legal regulations. Data storage can take place in internal, external, public, private, or hybrid locations, within the same or different geographical areas or in the same or different data centers. The security of data storage requires information about the storage locations, the techniques/methods of security, the possibilities and necessities of data movement between locations, the modalities and channels of data transfer, the possibilities of

data replication. Within this stage, there can be used security solutions, such as access management and data encryption.

1) Access Management

The access to data must be allowed only to authorized persons, in keeping with the access policy defined at the level of organization. The security policy may use different types of access based on identity, role, group, context (for example location), rules (example: nobody, deny, required, any, anybody). Access management contains processes and security controls performed both at the level of external storage systems (cloud), and at the level of organizations (customers and cloud providers).

The authentication of users may use models based on one factor or on a combination of factors: data (password), instruments (security token, firewalls, and intrusion-detection systems), and biometric elements (fingerprints, hand or palm geometry, retina, iris, signature analysis, voice recognition, and facial characteristics). The solutions of identity and rights management reduce the complexity and error risks throughout the lifecycle of the accounts and rights associated to users.

The control of data access differs according to their type (structured, like Database Management System Access Controls and unstructured, like File System Access Controls Application/Document Management System Access Controls) [14] and uses different models/combinations of models (Discretionary Access Control, Role Based Access Control, and Mandatory Access Control). The logic controls intensify the content security and the access controls, particularly in the applications and systems of structured data. The verification procedures are generally centralized and standardized and offer the necessary information to the audit and security control for data access.

2) Data Encryption

Data encryption is generally used for the organization's critical data and for those provided by law. The data encryption at storage can be carried on by using one or more levels, such as: hardware disk, director, file, application, and database. For the network transfer it is possible to use programmed means and/or file transfer manuals and security protocols (HTTPS - Hypertext Transfer Protocol Secure, TLS – Transport Layer Security, or SSL – Secure Socket Layer). The encryption of date ensures the keeping of their confidentiality. The encryption control will consider the mechanisms used for data encryption, the encryption key management, the use of simple or multiple keys, the data categories that require encryption.

C. Data Security on Sharing

The stage focuses on data sharing between users, customers, partners and systems. The transfer is made through authorization, based on the associated rights and permissions. According to the data sensitivity and to the valid legal regulations, data can be encrypted throughout the transfer. In the recent years, the efforts made for encrypting data ensured the secured transfer of network data.

In this regard, several solutions can be mentioned: Advanced Encryption Standard (uses symmetric and asymmetric keys), Rivest Shamir Adelman (RSA) (use digital signatures) with benefits in transmitting multimedia content on the Internet, Voice over IP technology (VoIP), which offers benefits in rendering digital signatures on the Internet platform [15]. The security of network data transactions focuses on five key characteristics [16]: confidentiality, authentication, integrity, non-repudiation of origin, non-repudiation of receipt.

Different logic control can also be used throughout this stage, in order to ensure authorized data access. These can be carried out at the level of application (through design and programming) and/or at the level of database (restriction rules and structural controls).

D. Data Security on Use

The data use requires the insurance of data availability in cloud and their use (visualization, processing, and access) by the authorized persons. Access management occupies an important part within this stage. The rights and permissions associated to individuals/accounts, devices or locations allow the controlled and authorized access to data use. The use of logic controls should also focus on ensuring data integrity (besides data access) throughout their use.

The use and safe transfer of network data can also be achieved through isolation, using different strategies, such as Multiprotocol Label Switching (MPLS), Virtual Private Networks (VPNs) and Virtual Local-Area Networks. In the MPLS-VPN process, isolation is performed through routing network devices to a Virtual Routing and Forwarding system [17].

E. Data Security in the Maintenance Stage

Data maintenance includes data recovery and data archiving operations for established periods. The process of archiving will take into consideration the type of device where the data will be archived, the physical requirements regarding the process of archiving, the data that must be encrypted, the encryption mechanisms that will be used, as well as the key management. Several security techniques will be used within this stage, such as [13] data encryption and attributes management.

F. Data Security in the Destruction Stage

This stage must ensure a complete and secure deletion of data (including the deletion of the encryption keys). The cloud provider should also offer the confirmation of data destruction (including the security copies) as well as the impossibility of their recovery. The control methods of data destruction security depend on the cloud services provider and its infrastructure. The SLAs (Service Level Agreements) must specify, both for destruction and for archiving, the security methodologies of the data offered by the provider. In order to reduce the risk of incomplete destruction, different search controls of the cloud content may be used.

III. Assessment of Data Security in the Cloud

Security assessment is considered a very good practice on determining the system's capacity of responding to potential exposures and incidents. In also helps the organization in identifying the deviations between the proposed security strategies and the actual state of the security system. The assessment represents the foundation in determining the potential losses and the premise in the subsequent security improvement.

The methods of security assessment include the international standards (for instance, ISO/IEC 27002:2005, NIST's SP800-53) as well as efficient practiced developed by security organizations, such as Cloud Security Alliance (CSA) [18], European Network and Information Security Agency (ENISA) [19], Information Systems Audit and Control Association (ISACA) and the Payment Card Industry (PCI) [20]. Moreover, in recent years efforts were made in ensuring security, such as CERT's OCTAVE [21], Cloud Audit (A6) [22] and Open Cloud Computing Interface (OCCI) [23].

The Cloud Security Alliance suggests in "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" [24] that they must offer guides in selecting cloud services providers; they must include small and medium enterprise security in the contractual obligations; they must analyze the changes in security metrics by passing to cloud, and they must include metrics and security standards in any SLAs and contracts.

The assessment of data security in the cloud must be performed for all types of data in the most important areas of the business. In order to be successful, the security assessment process must involve staff from the following departments [25]: human resources, corporate legal, audit, risk management, IT security, physical security, organization security and other business units. The assessment must also be connected to the other stages of the life cycle of the security insurance process, in order to implement the results and to obtain real advantages (fig. 3).

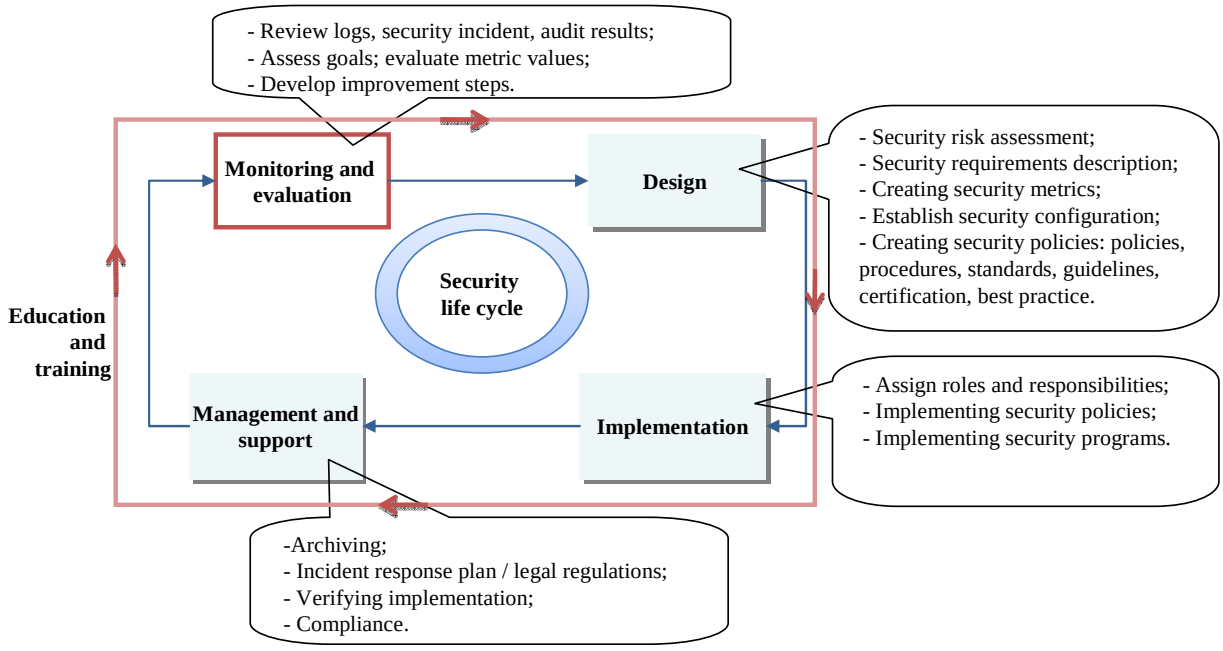

Fig. 3 The life cycle of data security process

The assessment of data security concerns both the internal assessment and the external assessment (in the cloud). The challenge that most organizations are confronted with is the impossibility of monitoring and evaluating the different requirements of data security in the cloud. Moreover, the cloud infrastructure is shared and the location of data might be hard to reach, which leads to new challenges concerning security assessment.

In order to support the settlement of this issue, the cloud providers offer individual or universal reports regarding the security of data in the cloud. The cloud providers may offer an interface or a diagnose port, which give clients the possibility to monitor the conformity of the security requirements and the service metrics relevant for the business [10]. Another solution might be using an audit certificate, universally accepted, that can be reported in Enterprise Risk Management, and Governance, Risk, and Compliance Reporting [26].

Data security assessment can be achieved through the assessment of the security risks and through the calculation of possible losses caused by the security incidents. The first step in assessing data security risks is identifying the organization's critical data asset [25], [27]. These data can be tangible (physical infrastructure and software elements) or intangible (digital and business data; organizational knowledge, company reputation, intellectual property) stored within the organization's systems. For each category of critical

data, the audit team must identify the vulnerabilities and threats and must assess the security risks.

The security risks can be measured using different quantitative techniques, such as the risk exposure quantification (Single Loss Exposure, Annual Rate of Occurrence, and Annual Loss Expectancy [27]) and the risk value, calculated as an asset function (A), vulnerability of assets (V), threats (T), security control measures (C), according to (1) [28].

$$R = A \times V \times T - C \quad (1)$$

There must be a correlation between the potential losses and the investment expenses. The security investment should not be perceived as an objective itself and it should be aligned to the organization's strategy. For this purpose, calculating the ROSI (Return of Security Investment - *Inv*) according to (2) may be useful [27].

$$ROSI = \frac{ALE_{without\ \ Inv} - ALE_{with\ \ Inv} - Cost_{of\ \ Inv}}{Cost\ \ of\ \ investment} \quad (2)$$

ALE (Annual Loss Expectancy) stands for the total amount of money the organization may lose within a year, if no action is performed in diminishing the risk. According to [28], ALE measures what people believe rather than the objective reality. This is the result of the fact that most organizations do not have systematic programs for collecting and analyzing historical data concerning incidents and data vulnerability and intangible losses (reputation and mark).

The cloud providers generally treat most risks specific for the cloud environment (mainly those of average and low level that do not produce important damages to the business). In this case, organization must take into account (besides investments and possible losses) the compensations (*Comp*) paid by the cloud providers for the losses determined by the security incidents in the cloud (costs connected to legal sanctions, reputation ruin, data loss and others). Thus, (2) may be written:

$$ROSI = \frac{Comp + ALE_{without\ \ Inv} - ALE_{with\ \ Inv} - Cost_{of\ \ Inv}}{Cost\ \ of\ \ investment} \quad (3)$$

In the case of ROSI formula, the losses avoided though the improvement security are considered benefits of investments in data security. The formula does not take into account the benefits of using different security techniques (for instance Firewalls, IDS, antivirus), which are hard to measure from the point of view of the generated incomes. Moreover, the cloud provider can use ROI as a marketing means. It may use it in combination with the price and support offered to customers in order to point out the benefits of its own solution.

Another indicator that can be used in security assessment is TCO (Total Cost of Ownership). It represents the afferent costs of the security system during its use. TCO offers a superior exactness to ROI indicator, but it is limited to the purchased security and not to the whole system of security. The cloud providers may use TCO, as well as ROI, as a comparison indicator to other providers and as an instrument that can influence the purchase decision.

Although ROI, NPV (Net Present Value), IRR (Internal Rate of Return), and TCO metrics are widely accepted, they have limitation in terms of the value brought by the security program. Many of time, these metrics are not well understood or they are created with subjective data (such as opinions of certain specialists), which leads to the need of further analysis [29].

The measuring of a complex phenomenon, such as data security in cloud, requires a complex approach that does not only focus on cost-benefit assessment metrics, but on qualitative metrics too. Even though, the complexity must be kept within normal limits, in order to ensure the organization's success. For the success of security assessment, the assessment program must be founded on the organizational decisions and must join the organizational strategy. In order to achieve this desideratum, the first step in carrying out the assessment program is the establishment of metrics that best define the organization's requirements and priorities. For that matter, the organization selects those quantitative (cost-benefit) and qualitative metrics that align with the targeted purposes.

The chosen objectives and metrics differ according to the type of organization (private or public), to the growth of organization, to the range of activity, and to the legal regulations of the area. They will be calculated using different techniques/systems of pursuit, gather, elaboration and data analysis. Fig. 4 illustrates examples of control techniques/systems of data security (grouped according to the security levels of figure 2), that can offer the necessary information in assessing data security.

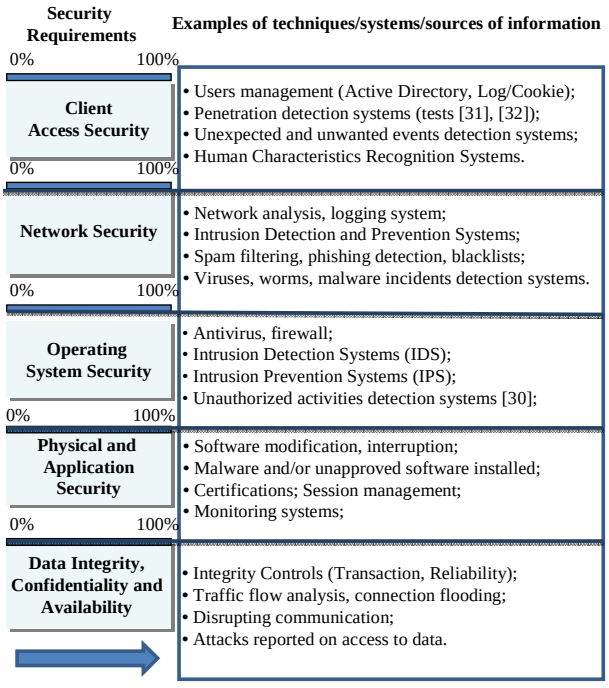

Fig. 4 Assessment of data security requirements in the cloud

In order to create the whole picture, the security metrics can be chosen so that they correspond to the four perspectives of the Balanced Scorecard: Financial, Customer, Internal Processes, and Learning and Growth.

The created pictures must be clear, concise and broad. Fig. 5 illustrates examples of metrics for each perspective, which can be used in a security management program.

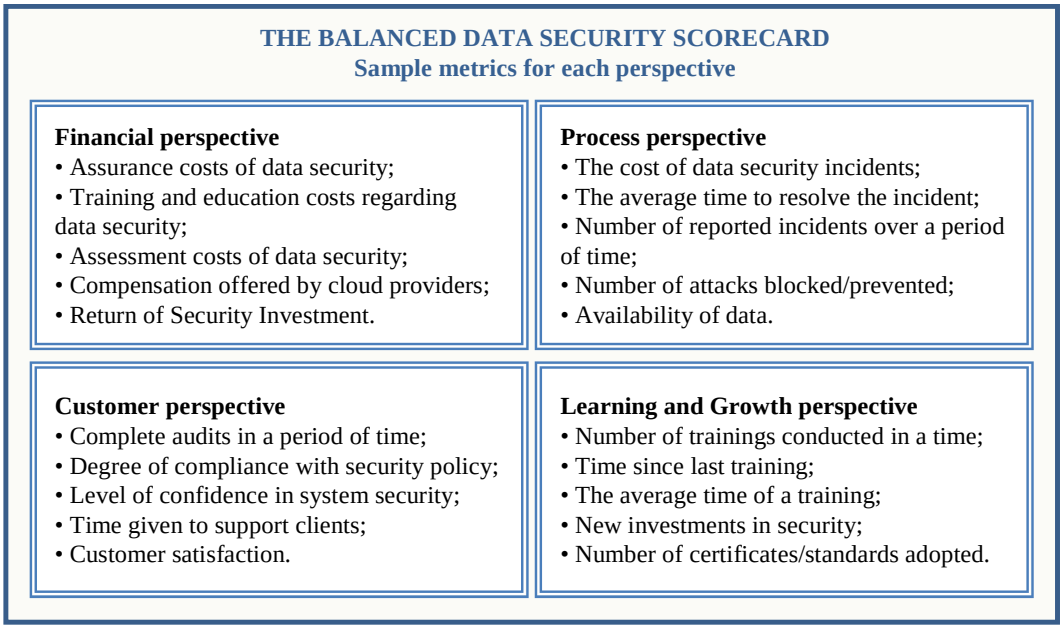

Fig. 5 Example of balanced data security scorecard

The calculus of metrics may be carried out manually, semi-automatically or automatically, using an audit system of data storage concerning the security incidents. It has to include processes, such as data collection, data storage in log library, association of rules, audit analysis and notification regarding the breach of security rules. Throughout this stage, the audit team can use the data mining technology in order to analyze the network security logs and in order to mine out the association rules of user behavior, further audit the abnormal behavior, thus to ensure network security [33]. The data can be extracted from the system reports (system logs), network analysis and firewall files, and stored in the database. The stored data is then processed and used for statistic analysis and included in the audit reports. The reports generated by this system can be offered to the cloud user for data security assessment. Taking into account the importance of data and of information access, any organization must take into account the achievement of a process of data security assurance. The complexity of this process differs from one organization to another but it must include at least the following: a data security policy, a response plan to security incidents and a periodic evaluation of security.

IV. Conclusion

Within the current economic and business context, the economical organization must gradually adapt itself both for the purpose of development but especially for the purpose of survival. For that matter, a solution based on cloud computing may represent a feasible answer to the challenges of the economic crisis.

Through such a solution, the economic organization may speculate market opportunities that, under normal conditions could not be accessed. Moreover, from the point of view of cloud computing characteristics, the transition to the cloud environment may constitute a premise for organizations in passing to the virtual organization.

Through its three models of provision (Software as a Service, Platform as a Service, Infrastructure as a Service), cloud computing offers numerous opportunities to organizations, but risks and challenges as well. In order to be successful, organizations must carry out a data analysis, must create a security policy, and an appropriate process of ensuring it. Also, it must take into account the existence of mixed solutions (in cloud and in house) and the use of one or several cloud models (private, public, mixed, community) that should best suite the business strategy.

The present study offers a perspective on the data security in the cloud (from the point of view of risks and methods of ensuring security) and on the possibilities of its evaluation. The proposed approach is not an exhaustive one, but an approach oriented on the importance of security insurance through the life cycle of data. Furthermore, the spectacular development of technology will permanently generate opportunities for research, analysis and implementation of new solutions as answer to the challenges and security risks.

Acknowledgment

This work was supported by CNCSIS-UEFISCSU, project PN II-RU (PD), “Modern Approaches in Business Intelligence

Systems Development for Services Oriented Organizations Management", code 654/2010, contract no. 12/03.08.2010.

REFERENCES

[1] M. Mircea, B. Ghilic-Micu, and M. Stoica, "Combining Business Intelligence with Cloud Computing to Delivery Agility in Actual Economy," *Journal of Economic Computation and Economic Cybernetics Studies*, vol. 45 (1), pp. 39-54, 2011.
[2] I-Newswire, "BI Trends 2012 From Hype to Breakthrough", http://www.onenewspage.com/n/Press+Releases/74mxa6hsy/BI-Trends-2012-From-Hype-to-Breakthrough.htm
[3] D. Teneyuca, "Internet cloud security: The illusion of inclusion," *Information security tehnical report*, pp. 1-6, Sept. 2011.
[4] D. Catteddu, and G. Hogben, "Cloud computing: benefits, risks and recommendations for information security," *European Network and Information Security Agency*, 2009.
[5] S. Subashini, and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, pp.1–11, July 2011.
[6] P. Goldstein, "Alternative IT sourcing strategies: From the campus to the cloud," *EDUCAUSE Center for Applied Research*, 2009.
[7] Jitterbit Inc., "Five Integration Tips to Cloud Computing Success," pp. 1-3, 2009.
[8] S. Kanhere, and V. Kanhere, "IS Audit and Security Professionals: An Emerging Role in a Changing World Order," *ISACA Journal*, vol. 5, pp. 50-53, 2009.
[9] B. Ghilic-Micu, M. Mircea, and M. Stoica, "The Audit of Business Intelligence Solutions," *Informatica Economica*, vol. 14 (1), pp. 66-77, 2010.
[10] P. Wilson, "Positive perspectives on cloud security," *Information security tehnical report*, pp. 1-5, Sept. 2011.
[11] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, pp. 583–592, March 2012.
[12] M. Mircea, and A.I. Andreescu, "Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis," *Communications of the IBIMA*, pp.1-14, 2011.
[13] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 2009. https://cloudsecurityalliance.org/csaguide.pdf
[14] J. Rich, "Cloud Data Security: Store (Rough Cut)," 2009. https://securosis.com
[15] A. Acquisti, S.W. Smith, and A. Sadeghi A, "Trust and Trustworthy Computing" In: *Third International Conference, TRUST 2010* Berlin, Germany. New York: Springer Heidelberg, 2010.
[16] H. Bidgoli, "Security Issues and Measures: Protecting Electronic Commerce Resources," *Electronic Commerce*, pp. 363-398, 2002.
[17] S. Jordan, and A. Bruno, "CCDA 640-864 Official Cert Guide, 4th Edition," Indianapolis: Cisco Press. 2011.
[18] Cloud Security Alliance, "CSA Guide V2" http://cloudsecurityalliance.org/
[19] European Network and Information Security Agency, "Cloud Computing Information Assurance Framework".
[20] Business assurance for the 21st century. Common Assurance. 2011 http://common-assurance.com/resources/Business_Assurance_for_the_21st_Century-final.pdf.
[21] B. Kaliski, and W. Pauley, "Toward Risk Assessment as a Service in Cloud Environments," pp. 1-7, 2012. http://www.usenix.org/event/hotcloud10/tech/full_papers/Kaliski.pdf
[22] Cloud Audit, "The Automated Audit, Assertion, Assessment, and Assurance API". http://www.cloudaudit.org/
[23] *Open Cloud Computing Interface.* OCCI Working Group. http://www.occiwg.org/doku.php
[24] T. Mellor, "Maintaining Security Governance in the Cloud - The Role of the Security Specialist" http://ezinearticles.com/?Maintaining-Security-Governance-in-the-Cloud---The-Role-of-the-Security-Specialist&id=5421468
[25] R. Bernard, "Information Lifecycle Security Risk Assessment: A tool for closing security gaps," *Computers & security*, vol. 26, pp. 26-30, 2007.
[26] P.G. Dorey, and A. Leite, "Commentary: Cloud computing. A security problem or solution?" *Information security tehnical report*, pp. 1-8, Sept. 2011.
[27] R. Bojanc, and B. Jerman-Blažič, "Towards a standard approach for quantifying an ICT security investment," *Computer Standards & Interfaces*, vol. 30, pp. 216–222, May 2008.
[28] S. Fua, and Y. Xiao, "An Effective Process of Information Security Risk Assessment," *Energy Procedia*, vol. 11, pp. 1050-1057, December 2011.
[29] L. Hayden, "IT Security Metrics: A practical framework for measuring security & protecting data", 2010.
[30] J. Zhao, and S. Zhao, "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly*, vol. 27, pp. 49–56, January 2010.
[31] M. Ciampa, "Security guide to network security fundamentals" 3rd ed. Boston: Course Technology, Cengage Learning. 2009.
[32] I. Winkler, "What is a security audit?" *Tech Target*. http://searchcio.techtarget.com/sDefinition/0,,sid182_gci955099,00.html
[33] L. Zhuoa, and Z. Wang, "Research and Implementation of Log-based Network Security Audit System," *Energy Procedia*, vol. 11, pp. 2021-2026, December 2011.

Marinela Mircea received her degree on Informatics in Economy from The Bucharest University of Economic Studies, Romania in 2003. In February 2009, she finished the doctoral stage, and her PhD thesis has the title "Business management in digital economy". Since 2003 she is teaching in The Bucharest University of Economic Studies, at Economic Informatics Department. Her work focuses on the programming, information system, business management and Business Intelligence. She published over 60 papers in conferences and journals in computer science, informatics and business management fields, and served as conference organizing chair, member of program committees and reviewed several papers for international conferences. She is the author of one book and coauthor of six books. She was member over 15 research projects, and project manager of the national research project titled "Modern Approaches in Business Intelligence Systems Development for Services-Oriented Organizations Management". Lect. Marinela Mircea became a member of the Association for the Promotion of Economic Informatics Education (INFOREC) in 2008, and senior member of the International Association of Computer Science and Information Technology (IACSIT) in 2010.