A Comparative Review of Cloud Security Proposals with ISO/IEC 27002

Oscar Rebollo[1], Daniel Mellado[2] and Eduardo Fernández-Medina[2]

[1]Social Security IT Management, Ministry of Labour and Immigration, Madrid, Spain

[2]GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain

Abstract. Information Security is considered one of the main reasons why users are reluctant to adopt the new generation of services offered by cloud computing providers. In order to minimize risks, some security proposals have been developed, with the purpose of facing a wide range of security concerns. This paper reviews these existing approaches and defines a security comparative framework, based on ISO/IEC 27002, suitable for the cloud environment. The analysis process of these alternatives shows a partial compliance with the defined requirements as each one is focused on different issues. As a consequence, more investigation is needed to achieve a comprehensive cloud security framework. The results of this paper highlight the gaps and weaknesses of each proposal, so that directions are settled for future work.

1 Introduction

Cloud computing is immersed in a fast growing wave [1], which is a visible characteristic of any starting technology, and is quickly becoming a popular issue in the IT world [2]. Although it may not be considered strictly a new technology [3] and reflects a new term for a long-held idea of computing as a utility [4], the explosion of the Internet and the companies´ pressure over existing storage and computing facilities have led many providers to offer new commodity services [5].

Industry has not yet published a common definition of cloud computing [6] but, in its more widespread meaning, it is considered as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [7].

Information security is considered a major issue of the cloud model, which may prevent massive adoption of these services by users [8]. As with all new technologies, there are new risks to be discovered in cloud computing and old risks to be re-evaluated [9]. This model creates new risks and new opportunities, which does not necessarily mean that it is more or less secure than the current environment [10]. The

Rebollo O., Mellado D. and Fernández-Medina E..
A Comparative Review of Cloud Security Proposals with ISO/IEC 27002.
DOI: 10.5220/0003546900030012
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 3-12
ISBN: 978-989-8425-61-4

most significant difference when considering security from a cloud perspective is the enterprise's loss of control, as opposed to any particular technical challenge [11].

The same as information security frameworks have been developed to guarantee an all-inclusive assurance in a traditional environment, an integrated security model which deals with the different levels of security in a cloud infrastructure is needed [12]. A future standard is demanded against which the cloud model can be secured [13]. This paper compiles existing cloud security proposals which represent the state of the art of performed efforts to guarantee information assurance in a cloud environment. These approaches are analyzed so that the main strengths and weaknesses of each one are highlighted.

Some of the published cloud computing reviews, such as [14], are mainly focused on general features, but no academic research deals in depth with security concerns. In this paper, we propose a comparative review of the most relevant cloud security approaches with the purpose of locating their differentiating characteristics and laying the foundations of a comprehensive security framework.

We have defined a comparative framework, whose criteria are based on two pillars: On the one hand, the ISO/IEC 27002 standard, which represents a widely accepted set of requirements; and, on the other hand, additional specific security criteria which are specific to a cloud infrastructure. The results can be used by companies and security professionals who need to tackle every security issue in a cloud computing environment.

This paper is structured as follows: next section offers a brief description of the security approaches that have been evaluated; section 3 presents the comparative framework as well as the results of the analysis that has been performed on these proposals; lastly, section 4 concludes the review.

2 Cloud Security Approaches

Through a deep literature and academic review, the following twelve cloud security approaches have been selected, which represent the state of the art in this field. This section summarizes each one of them so that they are introduced into the subsequent analysis.

2.1 Addressing Cloud Computing Security Issues

This proposal [15] identifies unique security requirements that arise in a cloud computing environment, due to its singular characteristics, as opposed to traditional risks. These requirements are classified as related to confidentiality, integrity and availability; and also categorized as bound to the application, platform or physical service levels. Authors claim that these threats may be mitigated by introducing a Trusted Third Party, which leads to the establishment of the necessary trust level. This way, a federated cloud infrastructure is built using security domains, which relies on the use of certificates, similar to a Public Key Infrastructure model.

2.2 A Layered Security Approach for Cloud Computing Infrastructure

This approach [16] introduces a layered security model which is focused on infrastructure aspects. This approach identifies five layers in the cloud computing infrastructure: network layer, process hosting layer (servers), storage layer, systems management layer and application layer. These layers are merged in a dynamic security model based on policies, which provides a customizable framework to be applied during the system life-cycle.

2.3 A Survey on Security Issues in Service Delivery Models of Cloud Computing

The survey in [12] compiles the security issues, threats and vulnerabilities, which should be dealt with in each of the cloud service delivery models. More attention is paid to the Software-as-a-Service model, as it is where clients face a greater dependence on providers and need to trust in their security measures implementation. Nevertheless, security concerns of the Platform-as-a-Service and Infrastructure-as-a-Service models are also considered. Finally, authors summarize the existing security solutions to some specific and concrete threats, and achieve the conclusion that a more complete security framework is needed, so that the cloud may attract potential consumers.

2.4 Cloud Computing Security Risk Assessment

The ENISA is an EU agency created to advance the functioning of the internal market, giving advice and recommendations and acting as a switchboard for information on good practices. Its publication [17] assesses security risks and benefits of using cloud computing, and provides security guidance for potential and existing users. The risk assessment process proposes to evaluate a wide collection of security risks, which are classified into four categories: policy and organizational, technical, legal, and risks not specific to the cloud. Based on these risks, an information assurance framework is introduced. The framework, which is based on the controls from the ISO 27000 family, is also published separately in [18]. It provides a set of security topics that an organization must consider to assure that its information holds enough protection and to guarantee that risks are addressed in a proper manner.

2.5 Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

The ISACA has published [19], where it briefly depicts risks and security concerns regarding cloud computing. According to this paper, the strategies for addressing cloud computing risks must take into account the service level agreements (SLAs) that define the relationship between the business and the cloud provider. It also slightly deals with governance, change management and assurance considerations. An audit and assurance program is provided in [20] to be used in a cloud computing

environment, which includes an enterprise risk management framework to identify security risks and mitigate vulnerabilities.

2.6 Cloud Cube Model

The Cloud Cube Model proposed in [9] identifies four criteria to differentiate cloud formations from each other and their provision scheme. These four dimensions are as follows: internal / external, proprietary / open, perimeterised / de-perimeterised architectures, and insourced / outsourced. The model´s objective is to help determining the cloud formation best suited for business needs as well as to enable secure operation through the chosen option. The Jericho Forum´s model proposes developing a Collaboration Oriented Architecture (COA) to assure secure business in de-perimeterised environments. The COA framework [21] includes a set of guidelines to guarantee secure interaction between users and end systems located in different security domains. This framework has its components classified into five groups: principles, processes, services, attributes and technologies.

2.7 Cloud Security Alliance (CSA)

The CSA is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing. Its primary contribution to cloud security is a guidance [10] which, in its second version, provides practical recommendations on reducing the associated risks when adopting cloud computing. The proposed guidelines are not compulsory and may not be all applicable to every cloud deployment, but help identifying threats in the cloud context and choose the best options to mitigate vulnerabilities. The recommendations are divided into thirteen domains, ranging from architectural framework to application security or virtualization, going through legal and compliance issues. These domains are classified into three sections: Cloud architecture, Governing in the cloud and Operating in the cloud. The CSA also provides in [22] a Governance, Risk management and Compliance toolkit to instrument and assess both private and public clouds against industry established best practices, standards and critical compliance requirements.

2.8 Cloud Security Issues

Authors in [23] highlight a set of cloud security issues focusing on the service level agreements (SLAs) between cloud providers and their clients. SLAs are the only legal agreements and represent a mean of enhancing trust among participants. Thus, it is explained how to standardize the SLAs through the handling of the following security risks: Privileged user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigative support, and Long-term viability.

2.9 Cloud Security and Privacy

In the book [24], authors propose an introductory view to a variety of security issues related to cloud computing, so that users may be confident of dealing with the most important concerns. The most relevant security topics that are covered in this book are the following ones: Infrastructure security, Data security and storage, Identity and access management, Security Management in the cloud, Privacy, Audit and compliance, and Security as a Service. Authors propose to utilize the cloud computing pattern in [25] as a framework to illustrate core cloud functions, the security controls that require additional emphasis, and the key roles for risk mitigation. This framework may serve organizations to adjust their internal risk models and processes.

2.10 Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control

The authors of [26] summarize security concerns that may prevent companies from entering the cloud. These concerns are derived from the CSA framework [CSA], whose security domains are classified into three categories: Traditional security, Availability, and Third-party data control. New problems that arise with the widespread adoption of cloud computing are also introduced. The paper concludes with three new proposals that may provide solutions to some security threats: Information-centric security, High-Assurance remote server attestation, and Privacy-Enhanced business intelligence.

2.11 Effectively and Securely using the Cloud Computing Paradigm

The NIST offers in [7] a definition of cloud computing, which has been widely accepted by the community. This definition includes both essential characteristics and the greatly widespread service and deployment models. These authors have also published a presentation on secure use of cloud computing [27], where cloud security advantages and challenges are analyzed. In addition, they include some concerns that should be considered for a secure migration when adopting a cloud architecture, and introduce a roadmap for future standards about cloud security.

2.12 Security in a Virtualised World

In this paper [13] authors define some security building blocks that may be used to construct a cloud computing architecture, whose security characteristics are similar to the traditional n-tier architecture. These structural components are as follows: Technical assurance, Vulnerability management, Data location and privacy, Incident management, and Service management. Their authors state that this framework may serve for the future development of a cloud security standard, following the work initiated by the CSA.

3 Comparative Study

The most relevant approaches to cloud security, which have been described previously, are compared in this section. First of all, a comparative framework is proposed to define a set of reference criteria that may be employed to validate in an unbiased manner the suitability of each approach. After that, the comparison results are shown.

3.1 Cloud Security Comparative Framework

It may be easily concluded from the above summaries that each proposal focuses on different aspects of cloud environment, and seems to be a lack of a common agreement about a security framework which can be employed to guarantee a comprehensive assurance. This framework should be founded over solid security principles, covering the whole spectrum of concerns that could arise in a cloud deployment.

Cloud computing provides a new way of delivering computing resources [17], which arises twofold security approaches: some traditional concerns continue to be valid due to the underlying technology, but also new security issues arise with the development of new service models and their unique attributes. This comparative framework covers both approaches to offer a holistic reference and achieve unbiased results.

Table 1. ISO/IEC 27002 Security Control Clauses.

Security Control Clauses	
Security Policy	Access Control
Organizing Information Security	Information Systems Acquisition, Development and Maintenance
Asset Management	Information Security Incident Management
Human Resources Security	Business Continuity Management
Physical and Environmental Security	Communications and Operations Management
Compliance	

Although this new computing paradigm may change the relationship between companies and their IT providers, it maintains unchanged many of the security risks, threats and vulnerabilities that have been deeply studied in the past. Therefore, the comparative analysis will rely on an accepted and widespread security standard , such as ISO/IEC 27002 [28]. This standard is widely used among security professionals and includes a set of security control clauses which may serve as guidelines to achieve effective information security management. We have chosen this reference because it covers a wide range of worldwide agreed security issues, from technical to managerial ones. Table 1 shows a list of these security clauses, which will be used as comparative criteria.

Furthermore, cloud computing delivery models involve delegating responsibility over some technical assets to the cloud provider; therefore, new security risks may arise because of the new way of management of the underlying technology. This is the reason why additional cloud related criteria need to be added to the former ones. According to [29], cloud security is supported by three pillars that must be set and

agreed between the cloud user and provider. These three domains are Operational security, Liability and Alignment between IT security and cloud service models. Operational security is already covered by the security controls of the ISO/IEC standard so the other two domains will be included in the comparative analysis.
On the one hand, Liability represents the relationship between cloud customer, provider and applicable statutory laws. The information assets that are shared over the cloud infrastructure should be managed with due diligence and comply with current legislation. In case the cloud provider and the user reside in different countries with significant regulatory differences, both parties need to find common grounds for judicial issues and reflect them in the contract.

On the other hand, Alignment refers to the adaptation degree between client security policies and cloud provider implementation. The user may have established a set of internal controls to guarantee information assurance, which should be extended and correlated with the operational security of the provider. This relationship is usually documented on the SLAs, which need to be monitored by both entities to check the fulfilment of the defined objectives.

This set of criteria may be used to evaluate any security proposal addressed to the cloud computing environment, regardless of the service delivery model adopted (SaaS, PaaS or IaaS).

3.2 Analysis Results

All of these defined criteria have been contrasted with the twelve cloud security proposals that were previously described. A summary of the results is introduced in Table 2, in which each criterion has been given three degrees of accordance (high, medium and low) depending on its compliance proximity. This gradation is provided by the security categories defined in the ISO 27002 standard, which performs as sub-criteria in the comparative analysis.

Table information shows that some criteria are more frequently taken into account among the proposals than others. Cloud specific criteria, that are Liability and Alignment, are considered in nearly all the solutions. The following security criteria are also well described in most approaches: Compliance, Access Control, Communications and Operations Management, and Physical and Environmental Security. These criteria could be said that gather traditional security issues which are usually related to a technical or tangible security point of view.

On the other side of the balance, Security Policy, Asset Management and Human Resources Security are the least frequently considered criteria. This indicates that although most proposals take into account traditional security concerns, they lack in considering many organizational and management aspects.

The most complete security proposals are the ENISA and the CSA ones, which are well-balanced against the defined criteria. Both approaches bring out the importance of evaluating organizational security risks along with technical ones, and include a wide spectrum of guidelines to guarantee information assurance.

Table results show that, although adequate efforts have been carried out in the development of the analyzed approaches, none of them fully satisfies the defined criteria. These outcomes present a challenge for the scientific community to achieve a full comprehensive security framework which embraces traditional security

Table 2. Comparison of Cloud Security Frameworks.

	Security Policy	Organizing Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Information Systems Acquisition, Development and Maintenance	Information Security Incident Management	Business Continuity Management	Compliance	Liability	Alignment
Addressing cloud computing security issues	low	low	high	Low	high	medium	medium	low	medium	medium	high	medium	high
A Layered Security Approach for Cloud Computing Infrastructure	high	medium	low	Low	medium	high	medium	low	low	low	medium	medium	medium
A survey on security issues in service delivery models of cloud computing	low	medium	low	Low	medium	high	high	medium	medium	low	medium	medium	high
Cloud Computing Security Risk Assessment	medium	high	high	Medium	high	high	high	medium	high	high	high	high	high
Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives	high	high	medium	low	medium	high	medium	medium	low	low	high	medium	high
Cloud Cube Model	low	medium	low	Medium	high	high	high	medium	low	low	high	medium	medium
Cloud Security Alliance	medium	high	medium	Low	high	medium	high	medium	high	high	high	high	high
Cloud Security Issues	low	medium	low	Low	medium	medium	high	medium	medium	low	high	high	high
Cloud Security and Privacy	medium	high	low	Low	high	high	high	medium	medium	medium	high	medium	medium
ControllingData in the Cloud: Outsourcing Computation without Outsourcing Control	low	medium	low	Low	medium	high	high	low	low	low	high	medium	high
Effectively and Securely Using the Cloud Computing Paradigm	low	medium	low	Low	high	high	high	medium	medium	medium	medium	medium	high
Security in a virtualised world	low	medium	low	Low	high	high	medium	low	high	high	high	medium	medium

concerns and new specific issues that emerge with the cloud computing paradigm. The gaps highlighted in this analysis may serve to complete existing cloud security approaches or to develop new ones founded on the settled criteria, so that a reference cloud security framework is defined which complies with all requirements. The tracking of the defined security clauses prevents the enterprise´s loss of control over its data and processes.

4 Conclusions and Future Work

Cloud computing is gaining importance among available service delivery models in the IT world. This new paradigm also involves new risks and threats, as applications and sensitive data are moved to an emerging infrastructure. Information security of the cloud model must be a research priority to define a security framework which provides assurance to its users, and allows stakeholders to be confident about their information assets.

After analyzing the most representative cloud security proposals, a clear conclusion achieved is that neither of them tackles all of the defined requisites. Although two approaches stand out over the others, the performed analysis shows existing gaps and opens new research lines to continue these works. Future investigation is needed to develop a comprehensive cloud security framework which offers enough guarantees to both cloud users and providers. This framework will align with the whole set of defined criteria.

With this comparison, additional reasons are provided to those authors that state that an integral security model is needed in the cloud computing area, and we position our work to follow this line in the future.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557) and ORIGIN (IDI-2010043(1-5), financed by the Centre for Industrial Technological Development (CDTI) and the FEDER, BUSINESS (PET2008-0136) awarded by the Spanish Ministry for Science and Technology and SERENIDAD (PEII11-0327-7035) and SISTEMAS (PII2I09-0150-3135) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

1. Gartner: Gartner's Hype Cycle Special Report for 2010. (2010)
2. McKinsey: Clearing the air on cloud computing. (2009)
3. Chen, Y., Paxson, V., Katz, R. H.: What's New About Cloud Computing Security? , University of California, Berkeley (2010)
4. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: Above the Clouds: A Berkeley view of Cloud Computing. University of California, Berkeley (2009)

5. Qian, L., Luo, Z., Du, Y., Guo, L.: Cloud Computing: An Overview. Proceedings of the 1st International Conference on Cloud Computing 626-631 (2009)
6. Vaquero, L. M., Rodero-Merino, L., Caceres, J., Lindner, M.: A Break in the Clouds: Towards a Cloud Definition. SIGCOMM Computer Communication Review 39, 50-55 (2009)
7. Mell, P., Grance, T.: The NIST Definition of Cloud Computing v15. National Institute of Standards and Technology (NIST) (2009)
8. IDC: IDC IT Cloud Services Survey: Top Benefits and Challenges. (2009)
9. Jericho Forum: Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. (2009)
10. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. (2009)
11. Cloud Computing Use Case Discussion Group: Cloud Computing Use Cases White Paper v4.0, http://cloudusecases.org/. (2010)
12. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34, 1-11 (2011)
13. Sloan, K.: Security in a virtualised world. Network Security 15-18 (2009)
14. Sriram, I., Khajeh-Hosseini, A.: Research Agenda in Cloud Technologies. 1st ACM Symposium on Cloud Computing (2010)
15. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation Computer Systems In Press, Corrected Proof, (2011)
16. Yildiz, M., Abawajy, J., Ercan, T., Bernoth, A.: A Layered Security Approach for Cloud Computing Infrastructure. Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks 763-767 (2009)
17. Catteddu, D., Hogben, G.: Cloud Computing Security Risk Assessment. European Network and Information Security Agency (ENISA) (2009)
18. Catteddu, D., Hogben, G.: Cloud Computing Information Assurance Framework. European Network and Information Security Agency (ENISA) (2009)
19. ISACA: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. (2009)
20. ISACA: Cloud Computing Management Audit/Assurance Program (2010)
21. Jericho Forum: Collaboration Oriented Architecture, http://www.opengroup.org/jericho/publications.htm. (2008)
22. Cloud Security Alliance: Governance, Risk Management and Compliance Stack, http://www.cloudsecurityalliance.org/grcstack.html. (2010)
23. Kandukuri, B. R., V, R. P., Rakshit, A.: Cloud Security Issues. Proceedings of the 2009 IEEE International Conference on Services Computing 517-520 (2009)
24. Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly (2009)
25. Open Security Architecture: Cloud Computing Pattern, http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing. (2008)
26. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proceedings of the ACM Workshop on Cloud Computing Security 85-90 (2009)
27. Mell, P., Grance, T.: Effectively and Securely Using the Cloud Computing Paradigm v26. National Institute of Standards and Technology (NIST) (2009)
28. ISO/IEC: ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. (2007)
29. Ahmad, R., Janczewski, L.: Triangulation theory: An approach to mitigate Governance risks in Clouds. 2nd IEEE International Conference on Cloud Computing Technology and Science (2010)