Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 1084 – 1089

Procedia Computer Science

The 6th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2016)

Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems

Mouna Jouini[a]*, Latifa Ben Arfa Rabai[a]

[a]*Laboratoire SOIE, Institut Supérieur de Gestion, Tunis, Tunisie*

Abstract

This paper reviews the state of the art in cyber security risk assessment of Cloud Computing systems. We select and examine in detail the quantitative security risk assessment models developed for or applied especially in the context of a Cloud Computing system. We review and then analyze existing models in terms of aim; the stages of risk management addressed; key risk management concepts covered; and sources of probabilistic data. Based on the analysis, we propose as well a comparison between these models to pick out limits and advantages of every presented model.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Cloud Computing; Cyber security; Quantitative risk assessment models; security risk assessment; Risk assessment models comparison

1. Introduction

The importance of security concerns on the development and exploitation of information systems has never stopped growing. In fact, Information Systems are today used everywhere by individuals, organizations, governments and systems are target to information security attacks and it is very clear now that this would lead to a loss of a large amount of money, time and other resources. Thus, organizations may not only spend millions of dollars on technical security equipments such as firewalls, intrusion detection systems (IDSs) and encryption tools to try to protect them against known threats, but also are confronted with great difficulties for evaluating security

* Corresponding author. Tel.:+216-96-670-070; fax: +216-71-588-514.
E-mail address: jouini.mouna@yahoo.fr (Mouna Jouini), latifa.rabai@gmail.com (Latifa Ben Arfa Rabai).

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.227

technology investments[11]. Indeed, firms aim to estimate the security breaches of their systems because organizations that best manage cyber-risk will be rewarded by a competitive market.

On the other hand, individual or enterprise users expect information systems to be secured and able to predict their risk and their strategies in reducing these risks. The drive of secure organizational information has initiated the need to develop better metrics for understanding the state of the organization's security attitude[14, 15].

The National Institute of Standards and Technology (NIST) defines risk management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level"[13]. The NIST defines risk assessment as the process of identifying, estimating, and prioritizing information security risks which requires a careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur[13].

Quantitative security risk assessment models are an effective tool to measure and assess the security levels of their systems, products, processes, and readiness to address the security issues they are facing. Metrics can also help to identify system vulnerabilities and provide guidance in prioritizing corrective actions. Moreover, metrics can be used to justify and direct future security investment[16]. Quantitative security metrics represent a means of quantifying the risks in monetary terms in such a way as to enable rational decision making.

From the risk assessment literature, a number of metrics has evolved to measure security risks. In fact, we have two types of metrics: qualitative and quantitative metrics. We focus in this article on quantitative security risk assessment models for Cloud computing systems. In fact, Cloud Computing presents a new technology for delivering computing resources as a service and on demand but it has several limits like security which is considered as the basic barrier for cloud adoption.

There are few quantitative models that estimate the security risks models for CC systems like MFC, MFCE MFC_{ext}, MFC_{int} and M^2FC[3, 5, 7, 8, 10]. We are interested in this work to review in detail quantitative security risk assessment models and then present comparisons between these models. This work is a detailed study of quantitative information security risk assessment models for Cloud Computing systems. The result will be a comparative and critic analysis of those models, and their significant concepts.

The remainder of the paper is organized as follows. In Section 2, we announce the problem dealt with by the article. Section 3 provides some background discussion on what Cloud Computing systems are and on security challenges facing them. In section 4, we review quantitative security risk assessment models for CC systems. Section 5 provides a detailed analysis and comparison of the presented models. We draw some concluding remarks in Section 6.

2. Problem statement

There are strong drivers for addressing security risk assessment in a new perspective, especially for managing information security risk. In fact, there are certain factors that provoke changes in firms. For example, the use of new technologies, the pressure of innovation and the pressure to cut costs oblige firms to take into account these aspects and the disregarding any of these factors can affect the organization's reputation and customer confidence.

Information Security risk assessment consider as a difficult and costly. In fact, if a new vulnerability or a new virus is detected, the results may be too costly. In addition, to provide fast and suitable response to security incidents and to protect their assets, organizations need for a systematic security risk assessments approach. Furthermore, individual or enterprise users expect information systems to be secured and able to predict their risk and their strategies in reducing these risks. The drive of secure organizational information has initiated the need to develop better metrics for understanding the state of the organization's security attitude[14, 15]. On the other hand, risk assessment is one of the fundamental components of an organizational risk management process[2]. It is based on security metrics to assess security risks.

3. Cloud Computing systems and cyber security challenges

Cloud Computing is considered as a new technology that has enable innovation for a growing number organizations. It allows improving Cloud Computing capabilities as part of their innovation process, for their products and services delivery, and diversification, and for their overall organizational evolution and growth.

Cloud computing is an emerging paradigm of computing that replaces computing as a personal commodity by computing as a public utility. It may be defined as the delivery of on-demand computing resources over the Internet on a pay-for-use basis. The resources (such as processor compute time and data storage) are dynamically provisioned over the internet and its subscribers are invoiced based on the use of computing resources.

There are many definitions for Cloud Computing. For example, the National Institute of Standards and Technology defines Cloud Computing as "a model which grants convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1].

Cloud Computing presents its services as three layers of services which provide infrastructure resources, application platform and software as services to the consumer. Infrastructure as a Service (IaaS) layer provides the basic computing infrastructure of servers, processing, storage, and networks. Platform as a Service (PaaS) layer presents a layer where users can deploy and install their applications. Software as a Service (SaaS) delivers applications through a web browser to thousands of customers without having to be installed on their computers.

Cloud Computing offers all the advantages of a public utility system, in terms of economy of scale, flexibility and convenience but it raises substantial issues such as loss of control and loss of security.

But as more and more information on individuals and companies are placed in the cloud, problems are beginning to grow especially about security. In fact, data users' externalization makes hard to maintain data integrity and privacy, and availability which causes serious consequences. Security is the big challenge in cloud computing systems[3, 4, 5, 6, 7, 8, 9, 10, 18]. In fact, According to a survey conducted by International Data Group (IDG) enterprise in 2014[12] security is deeply the top concern for CC. In fact, up from 61% in 2014, and higher among finance organizations (78%), 67% of organizations have concerns about the security of cloud computing solutions. The additional challenges are not even on the same playing field for decision-makers; only 43% are concerned with integration, followed by the ability of cloud solutions to meet enterprise and/or industry standards (35%)[12]. Given their high security concerns, organizations are integrating strategies and tools (like cloud security management and monitoring tools) to lessen these challenges over the next months.

4. Information security risk assessment models

We introduce in this section the basic security risk assessment models for Cloud Computing system. In fact, these models quantify the security of a computing system by a random variable that represents for each stakeholder, the amount of loss that result from security threats and system vulnerabilities. We present hence five models to quantify security breaches for Cloud Computing application.

4.1. SecAgreement: A Security Risk Assessment Model

In[18], Hale et al. presented a model called SecAgreement to enable cloud service providers to include increasing the likelihood that their services will be used. The approach defines a cloud service matchmaking algorithm to assess and rank SecAg enhanced SLA by their risk, allowing organizations to quantify risk, identify any policy compliance gaps that might exist, and thus select the cloud services that best meet their security needs.

4.2. The Mean Failure Cost (MFC)

Ben Aissa et al. introduce, in[17], a cyber security metric called Mean Failure Cost (MFC) that quantifies the security of a computing system by the statistical mean of the random variable that represents for each stakeholder, the amount of loss that result from security threats and system vulnerabilities. The MFC varies by stakeholder and takes into account the variance of the stakes that a stakeholder has in meeting each security requirement. The infrastructure in question reflects the values that stakeholders have in each security requirement, the dependency of security requirements on the operation of architectural components and the impact that security threats have on these components.

The MFC process proceeds in four steps:

- Generation of Stakes Matrix: Let ST(S, R) be the stakes matrix of dimension (i*j) where S represent system stakeholders and R represent the requirements of this system. The cell A(Si, Rj) represents the cost that stakeholder Si would lose if the system failed to meet the security requirement Rj.
- Generation of Dependency Matrix: The dependency matrix represents how to estimate the probability that a particular security requirement is violated in the course of operating the system for some period of time.
- Generation of Impact Matrix: The system architecture may present components that fail to operate properly as a result of security breakdowns caused by malicious activity. Thus, we must specify the set of threats related to this system. This matrix determines which threats affect which components and assess the likelihood of success of each threat in light of perpetrator behavior and possible counter-measures.
  Generation of the threat vector: The threat vector represents the probability that a threat materializes during unitary period of operation.

4.3. The Mean Failure Cost External (MFC_{ext}) and the Mean Failure Cost Internal (MFC_{int})

Jouini et al. proposed in[7] a new model for quantifying security threats risks by considering a classification of the identified threats: the Internal MFC (MFC_{int}) and the External MFC (MFC_{ext}). In fact, threats are classified using their sources in order to know the source of threats shaped information systems and especially the Cloud Computing systems to develop appropriate strategies to prevent, or mitigate their effects. In fact, we are based on threat sources dimensions in order to make out threats origins. The model considers that the security threat space intrusion is subdivided into subspaces according to a model of two dimensions labeled Internal, and External.

This classification lets us to propose two new extension types of the threat vector (PT) of the MFC metric. Consequently, there will be two extensions measures of the mean failure cost (MFC). We can calculate the external mean failure cost (MFC_{ext}) and the internal mean failure cost (MFC_{int}) depending on the attack space vector AS that present the probability that a threat is either internal or external.

These new extensions of MFC model improve analysis of the vulnerability of the system. They allow specifying the nature of security solution that minimizes the mean failure cost.

4.4. The MFC Extension model (MFCE)

Jouini et al., suggested, in[5], the Mean Failure Cost Extension (MFCE) as a new cyber security metric for information systems and for Cloud Computing environment particularly. The model is based on a threat classification model called as the Hybrid threat Classification model (HTC) and proposed in[9]. The HTC is generic model that combines several threats criteria or characteristics like: threat source, threat perpetrators, motives, intent, threats consequences.

The MFCE model focus on refining the estimation of the impact matrix IM and the threat vector PT of the Mean Failure Cost model (MFC) introduced in previous section. This model allows studying the impact of a whole class of threats rather than a mere threat. Indeed, threats are variable in time and security solutions change over time.

For the impact matrix IM, it was generated two new matrices: the impact matrix IMC and the threat classes Matrix CM. The ICM matrix presents the probability that a component Ck fails once a threat class Clr has materialized and the CM matrix presents the probability of having a threat class Clr once a threat Tq has occurred.

The MFCE model represents a cyber security metric as a decision making technique for Cloud Computing environment to derive relevant decision making security solutions. This quantitative decision making metric allows selecting countermeasures per threats class rather than a threat to better study and identify security threats.

4.5. Multi-dimensional Mean Failure Cost Model (M^2FC)

Jouini et al. propose, in[10], adopt the multi-dimensional approach to assess security threats. They propose a new model for assessing the cost of the failure of an information system security that takes into account threats dimensions to better assess threats risks. The model called Multi dimensional Mean Failure Cost (M^2FC) and considered that the threat world is divided into several threats perspectives each having several orthogonal

dimensions. In fact, any security threat presents several aspects, called perspectives, which increase the risk level faced by a system. These perspectives can decompose this space into several slices called as dimensions.

For decomposition purpose, the model considers a leading dimension to allow focusing more on one dimension than the rest of the dimensions of the threat world. For example, to assess the mean failure cost per architectural components we choose the components dimension as the leading one. In other situations, we would like to focus not on components but on deployment site of the enterprise, then we will have the mean failure cost per location.

The M^2FC model takes into account the stakeholders assessment of the cost related to their requirements with regard to the elements of two dimensions. Thus, the model considers a set H of stakeholders and a set R of their requirements are distinguished from a set of the leading dimension and a set of the other considered dimensions (time, system's component…).

5. Comparative Study

The study of the four quantitative security risk analysis models for CC systems aims to compare in greater detail the three different approaches and to present as well limits and advantages for each model.

The SecAgreement model is a quantitative approach that is used to compare between cloud providers to select the best one basing on calculation of risk factor of each one and do not estimate risks due to security breaches for Cloud Computing environment.

The Mean Failure Cost model (MFC) has several advantages. In fact, it quantifies the security of a system in financial terms, specially, in terms of how much each system stakeholder stands to lose as a result of security threats and system vulnerabilities. Indeed, this metric varies according to the stakes that each stakeholder has in meeting each security requirement. However, it presents several shortcomings. After studying and analyzing security threats and the MFC metric, we noticed the following MFC limits:

- Security threats are evolutive and variable over time and have several characteristics, and in PT vector, there is no logical or hierarchical structure between the different catalogued threats as they are not based on a particular attribute to classify them.
- Underestimation of the MFC: In fact, in the threat vector PT, the term used to define the threat can be ambiguous; this can lead to an overlap between the various threats i.e. each threat may belong to several classes at once and thus it is computed many times, so we have an underestimation of the mean failure cost.
- Users who may use this method to derive threats may have completely different results.
- Managers cannot identify the source of threats risks in order to suggest appropriate countermeasures.
- The MFC is blind toward the structure and the dimensions of security threats. It considers that any failure due to a threat is a failure with respect to the whole specification. But stakeholders may have different stakes in different security threats dimensions and perspectives which are not reflected in the MFC.

The MFC_{ext} and the MFC_{int} give the critical threats space to help managers to take the appropriate countermeasures. They improve the analysis of the system vulnerability. They specify the type of solution to minimize the average cost of failure. In fact, using the threat classification source dimension, they allow identifying the source of the threats space (either internal or external source) to let managers concentrate on the intrusion space having the higher mean failure costs. However, it do not take into account all threats characteristics and just consider one criteria which does not accurately describe a threat (like the source), so they do not give accurate values on the cost of security failure. In addition, the considered criteria (source) are based on a binary classification (internal or external) while threat sources may include three subclasses.

The Mean Failure Cost Extension model (MFCE) considers threat classification on the basis of a model of threats classification and allows giving a threat solution by class, this model does not represent the cost according to security threats dimensions or perspectives. Also, we pointed out that the used threats classification model is not complete model in terms of size. In addition, if managers want to know critical criteria or dimension that influences the cost values of security failure, they cannot determinate them using these models. So we must develop a metric that accurately estimates security breaches and gives critical dimension to better manage security policies in organizations. Therefore, if the decisions makers want to have dimensions or critical criteria that influence actions of the cost of failure of security, they cannot determinate them using these models.

Finally, this M^2FC is an improvement of the Mean Failure Cost (MFC)[17]. This model varies by stakeholder, and takes into account the variance of the stakes that a stakeholder has in meeting each security requirement but it does not take into account threat perspectives and dimensions. Moreover, this it considers a multi-dimensional appearance as a threat contains several dimensions, it takes into account threats perspectives to reduce security risk to each system and it considers changes in systems like changes in the deployment, components and changes in user access policies. Thus, it takes into account threats dimensions and perspectives aspect and allows identifying critical dimensions that cause the biggest costs.

6. Conclusion

Risk assessment is a crucial mechanism in the wheel of Information Security Management. It is important for enterprises to adopt a systematic and well-structured process for assessing information security risks to its assets. The main purpose of the study is to review and compare and quantitative security risk model for Cloud Computing systems since these systems represent a prospect technology for firms that reduce cost and improve as well organizations' brand. The resulting comparison help decisions makers to select the suitable models to assess security risks for CC environment and indeed for other information systems. In fact, it helps evaluating the models' applicability to an organization and their specific needs.

References

1. Mell P, Grance T. Effectively and Securely Using the Cloud Computing Paradigm, *ACM Cloud Computing Security Workshop*; 2009.
2. NIST. *An introduction to computer security: The NIST handbook. Technical report*, National Institute of Standards and Technology (NIST), Special Publication 800-12, Gaithersburg, MD: NIST 2012.
3. Jouini M, Ben Arfa Rabai L, A Security Risk Management Metric For Cloud Computing Systems, *International Journal of Organizational and Collective Intelligence (IJOCI)* 2014;4(3): 1-21.
4. Jouini M, Ben Arfa Rabai L. Surveying and Analyzing Security Problems in Cloud Computing Environments, *The 10th International Conference on Computational Intelligence and Security (CIS 2014)*; 2014. p. 689-493.
5. Jouini M, Ben Arfa Rabai L. Mean Failure Cost Extension Model Towards A Security Threats Assessment: A Cloud Computing Case Study, *Journal of Computers (JCP)* 2015;10(3):184-194.
6. Saripalli, P., & Walters, B. QUIRC: A quantitative impact and risk assessment framework for cloud security. *Proceedings of the IEEE 3rd International Conference on Cloud Computing* 2009, 280–288.
7. Jouini M, Ben Arfa Rabai L, Ben Aissa A, Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study, *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 2012;1(3):265-279.
8. Ben Arfa Rabai L, Jouini M, Ben Aissa A, Mili A. A cybersecurity model in cloud computing environments, *Journal of King Saud University - Computer and Information Sciences*; 2013.
9. Jouini M, Ben Arfa Rabai L, Ben Aissa A. Classification of security threats in information systems, *ANT/SEIT 2014* 2014:(32)489-496.
10. Jouini M, Ben Arfa Rabai L, Khedri R. A Multidimensional Approach Towards a Quantitative Assessment of Security Threats, *ANT/SEIT 2015* 2015, 507-514.
11. Boehme R, Nowey T. *Economic security metrics*. In: Irene, E., Felix, F., Ralf, R. (Eds.). Dependability Metrics 2008;(4909):176-187.
12. IDG Cloud Computing Survey, *Cloud Continues to Transform Business Landscape as CIOs Explore New Areas for Hosting*, http://www.idgenterprise.com/news/press-release/cloud-continues-to-transform-business-landscape-as-cios-explore-new-areas-for-hosting/, (Accessed: 14 January 2016) 2014.
13. Wang JA, Xia M, Zhang F. Metrics for information security vulnerabilities. *Proceedings of Intellect base International Consortium* 2009;(1)284-294.
14. Demchenko Y, Gommans L, De Laat C. Web Services and Grid Security Vulnerabilities and Threats Analysis and Model, Bas Oudenaarde, *Advanced Internet Research Group*, University of Amsterdam, Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands 2000.
15. ISO/IEC 27005:2007 Information Technology-Security Techniques-Information Security Risk Management, *Int'l Org*. Standardization 2007.
16. Emam A.H.M. Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. *International Journal of Soft Computing and Engineering 2013*; 3(2):110-113.
17. Ben Aissa A, Abercrombie RK, Sheldon FT, and Mili A. Quantifying security threats and their potential impact: a case study. Innovation in *systems and software engineering* 2010;6(1):269–281.
18. Hale, M., & Gamble, R. SecAgreement: Advancing security risk calculations in cloud services. *Proceedings of 8th IEEE World Congress on Services*, 2012.