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.