Chapter 37

A Security Risk Management Metric for Cloud Computing Systems

Mouna Jouini
ISG, Tunisia

Latifa Ben Arfa Rabai
ISG, Tunisia

ABSTRACT

Cloud computing is a growing technology used by several organizations because it presents a cost effective policy to manage and control Information Technology (IT). It delivers computing services as a public utility rather than a personal one. However, despite these benefits, it presents many challenges including access control and security problems. In order to assess security risks, the paper gives an overview of security risk management metrics. Then, it illustrates the use of a cyber security measure to describe an economic security model for cloud computing system. Moreover, it proposes a cloud provider business model for security issues. Finally, the paper shows a solution related to the vulnerabilities in cloud systems using a new quantitative metric to reduce the probability that an architectural components fails. The main aim of this article is to quantify security threats in cloud computing environments due to security breaches using a new security metric.

1. INTRODUCTION

Security concerns become more and more serious thanks to the development and exploitation of information systems. In fact, Information systems are today used everywhere by individuals or organizations and systems are target to various kind of attacks. Cloud computing technologies represent a revolution in information technologies development that offer several gains. It is an environment that offers infrastructure, platforms, data, software and security as a services and it is used to speed up and reduce the costs of existing processes.

As cloud computing technology develops will continue to centralize and simplify, allowing for increased employee productivity and more efficient use of limited resources. Interest has continued to increase and many organizations have moved

DOI: 10.4018/978-1-4666-8111-8.ch037

elements of their IT into the cloud. Despite these positive gains, security in the cloud remains a valid concern due to customer's data that are stored to third parties datacenters. Security comes from hackers, viruses or internal employees' attacks and leads to information loss or corruption, large amount of money loss, time and other resources loss. Thus, cloud providers and users (organizations or individuals) must find efficient means to protect their assets from threats damage and prevent financial losses which come from technical security equipments such as firewalls, IDSs and encryption tools. In this context, information security risk management model comes to reduce cost investment without increasing the risk. Risk identification allows organizations to be more competitive and to take appropriate security decisions (Jonsson & Pirzadeh, 2011). There are few quantitative models that estimate the security risks (Speaks, 2010; Sangroya et al., 2010; Johnson, 2003) and the other work are based on qualitative model like in Zhang et al. (2010).

In this article, we explore a quantitative cyber security metric in cloud computing emerging technologies to quantify security breaches. The risk assessment metric that we use evaluate for each stakeholders costs due to security failures. Indeed, we illustrate how this measure can be used to analyze cloud computing as a business model. The security metric we use in this article is quantified in economic terms, in that way it enables providers and subscribers to weight these security risks, and then to evaluate the cost effectiveness of some security countermeasures. We also, recommend a solution related to the vulnerabilities in cloud environment, based on a cyber security model, in order to reduce the probability that architectural components fail.

- The first part shows literature review of basic security metrics for risk estimations. The section discusses as well advantages and drawbacks of these metrics.
- The second part illustrates the quantification of security breaches in Cloud Computing systems using the Mean Failure Cost (MFC) metric.
- The third part illustrates how this security cost model allows rationalizing security decision making in cloud computing environments.
- Finally, the fourth part illustrates our proposed security metrics to reduce vulnerability in cloud systems by reducing the probability components failure.

2. INFORMATION SECURITY RISKS MANAGEMENT

Individual or enterprise users rely on information systems to be secured and able to predict their risk and their strategies in reducing these risks. Thus, it is an investment to be measured in dollars saved as a result of reduced losses from security breaches, or in profits from new ventures that would be too risky to undertake without investments in security (Schechter, 2004). It represents, for instance, an essential business function that allows organizations to perform with some difficulties their operations and deliver services to the public (Chew et al., 2009).

The drive to secure organizational information has initiated the need to develop better measures for understanding the situation of the organization's security attitude (Bryant, 2009). For more explanation, Wang states in Wang et al. (2009) that is widely acknowledged that metrics are essential to information security because they can be an efficient tool to measure the security strength and levels of their systems, products, processes, and readiness to address security concerns that they are face.

The National Institute of Standards and Technology (NIST) which defines risk management as the process that has several steps: risk identification, risk assessment, risk reduction using some