Chapter 11
A Security Framework for Secure Cloud Computing Environments

Mouna Jouini
Institut Supérieur De Gestion De Tunis, Tunisia

Latifa Ben Arfa Rabai
Institut Supérieur De Gestion De Tunis, Tunisia

ABSTRACT

Cloud computing technology is a relatively new concept of providing scalable and virtualized resources, software and hardware on demand to consumers. It presents a new technology to deliver computing resources as a service. It offers a variety of benefits like services on demand and provisioning and suffers from several weaknesses. In fact, security presents a major obstacle in cloud computing adoption. In this paper, the authors will deal with security problems in cloud computing systems and show how to solve these problems using a quantitative security risk assessment model named Multi-dimensional Mean Failure Cost (M^2FC). In fact, they summarize first security issues related to cloud computing environments and then propose a generic framework that analysis and evaluate cloud security problems and then propose appropriate countermeasures to solve these problems.

1. INTRODUCTION

Cloud computing is an emerging technology which recently has shown significant attention lately in the word. It provides services over the internet: users can utilize the online services of different software instead of purchasing or installing them on their own computers. The National Institute of Standard and Technology (NIST) definition defines cloud computing as a paradigm for enabling useful, on-demand network access to a shared pool of configurable computing resources (Mell & Grance, 2010). It offers several services presented in three models: Software as Service (SaaS), Platform as Service (PaaS), and Infrastructure as Service (IaaS). Software as Service (SaaS) provides services existing in the cloud or

DOI: 10.4018/978-1-5225-8176-5.ch011

applications to end users, Platform as Service (PaaS) provides access to platforms and Infrastructure as Service (IaaS) offers processing storage and other computing resources.

Cloud computing offers many advantages. But as more and more information on individuals and companies are placed in the cloud, concerns 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 (Zissis & Lekkas, 2012; Ukil, Jana & De Sarkar, 2013; Sun, Chang, Sun, Li & Wang, 2012; Malik & Nazir, 2012; Mell & Grance, 2010; Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2012; Jouini, Ben Arfa Rabai, Ben Aissa & Mili, 2012; Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2013; Jouini, Ben Arfa Rabai & Ben Aissa, 2014; Sampathkumar, 2015). In fact, according to survey conducted by International Data Group (IDG) enterprise in 2014 (IDG Cloud Computing Survey, 2014), security is deeply the top concern for cloud computing. 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 tech decision-makers; only 43% are concerned with integration, followed by the ability of cloud solutions to meet enterprise and/or industry standards (35%) (IDG Cloud Computing Survey, 2014). Given their high security concerns, organizations are integrating strategies and tools (like cloud management and monitoring tools, and cloud security management tools) to lessen these challenges over the next 12 months.

In this paper, we will show how to solve security problems in cloud computing systems using a quantitative security risk assessment model. We aim to present a generic framework that evaluate firstly cloud security by identifying unique security requirements, secondly to identify architectural components affected by this risk, thirdly to make out security threats that damage these components and finally to attempt to present viable solutions that eliminates these potential threats.

The remainder of this paper is organized as follows. Section 2 presents related work. Section 3 presents security issues in cloud computing environments. Section 4 illustrates a quantitative security risk model that we will use in our new approach. Section 5 presents our security framework that solves security problems in Cloud Computing environments in a quantitative way. Finally, conclusions and a direction for future work are given in section 6.

2. RELATED WORK

Literature review was shown that there are many works that studied cloud security issues (Zissis & Lekkas, 2012; Ukil, Jana & De Sarkar, 2013; Hu, Wu & Cheng, 2012; Sun, Chang, Sun, Li & Wang, 2012; Sun, Chang, Sun, Li & Wang, 2012). All works provide a qualitative discussion of security related issues in CC environments submitting a quick analysis and survey of security issues. In fact, they develop and deploy a qualitative security management framework on cloud computing environment by proposing some security strategies (countermeasures).

Arijit Ukil et al, have analyze in (Ukil, Jana & De Sarkar, 2013) security problems in cloud computing. They proposed a framework for satisfying cloud security ensuring the confidentiality, integrity and authentication of data. In fact, they provide security architecture and necessary security techniques for cloud computing infrastructure. The presented architecture incorporates different security schemes, techniques and protocols for cloud computing, particularly in Infrastructure-as-a-Service (IaaS) and