Chapter 46
Security Problems in Cloud Computing Environments:
A Deep Analysis and a Secure Framework

Mouna Jouini
Laboratoire SOIE, Institut Sup´erieur de Gestion, Tunisia

Latifa Ben Arfa Rabai
Laboratoire SOIE, Institut Sup´erieur de Gestion, 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 chapter, we 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, we present first a deep analysis of 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.

INTRODUCTION

Cloud Computing technology is a new concept of providing dramatically scalable and virtualized resources, software and hardware on demand to consumers. Cloud Computing offers a whole new paradigm to allow the users having high end and scalable infrastructure at an affordable cost. It is based on many new technologies like virtualization, distributed computing, utility computing, cryptography and web services. However, security concerns are terrible for these systems whose infrastructure and computational resources are owned by an outside party that sells those services to the general public. In fact, data breaches to Cloud services are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities of the Cloud architecture.

DOI: 10.4018/978-1-5225-5634-3.ch046

In this chapter, we provide a detailed analysis of security issues of Cloud Computing systems besides the countermeasure of each one. We also present potential risks and impacts of these challenges in Cloud customers and security requirements.

The remainder of this chapter organized as follows. Section 2 presents related work. Section 3 shows security threats in Cloud Computing systems. Section 4 presents security issues in Cloud Computing environments. Section 5 illustrates a quantitative security risk model that we will use in our new approach. Section 6 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 7.

SECURITY ON CLOUD COMPUTING SYSTEM

Cloud Computing is a new way of delivering computing resources, as a public utility. Computing services such as data storage and email handling are now instantly available, and on demand. It is an on demand service model for IT provision, often based on virtualization and distributed computing technologies. It offers many benefits like highly abstracted resources, services on demand with a ''pay as you go'' billing system, immediate provisioning, shared resources (hardware, database, memory…) and programmatic management tool (Grobauer, Walloschek, & Stocker, 2011). Cloud Computing is such a type of computing environment, where business owners outsource their computing needs including application software services to a third party; and when they need to use the computing power or employees need to use the application resources like database, and emails, they access the resource via internet.

Cloud Computing can be considered a new computing paradigm as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. Because of the implications for greater flexibility and availability at lower cost, Cloud Computing is a subject that has been receiving a good deal of attention lately (Grobauer, Walloschek, & Stocker, 2011). It received a considerable attention from global and local IT players, national governments, and international agencies (Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2012; Jouini, Ben Arfa Rabai, Ben Aissa & Mili, 2012; Ben Arfa Rabai, Jouini, Ben Aissa & Mili, 2013). But as more and more information on individuals and companies is placed in the Cloud, concerns are beginning to grow about just how safe this environment is. The externalized aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability and demonstrate compliance. For example, IDC Enterprise Panel recently conducted a survey of 244 IT executives/ Chief Executive Officers (CIOs) and their line-of business (LOB) colleagues to gauge their opinions and understand their companies' use of IT Cloud services. Security ranked first as the greatest challenge or issue of Cloud Computing by 74,6%, then we find performance and availability by 63,1% (Gens, 2009). Furthermore, hackers could take advantage of the massive computing power of Clouds to fire attacks to users who are in the same or different networks. For instance, hackers rented a server through Amazon's EC2 service and carried out an attack to Sony's PlayStation Network (Amazon, 2011). Therefore, a good understanding of Cloud security problems and threats is necessary in order to provide more secure services to Cloud users.