

Chapter 4

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.

DOI: 10.4018/978-1-5225-2449-6.ch004

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.

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.

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-problems-in-cloud-computing-environments/179806

Related Content

Web 2.0 and Enterprise 2.0

(2012). *Electronic Commerce Management for Business Activities and Global Enterprises: Competitive Advantages* (pp. 47-74).

www.irma-international.org/chapter/web-enterprise/67587

The Determination of User Satisfaction with Personal Internet Banking Services in the Context of Australia

Padid Akbarzadeh Gharib (2016). *Journal of Electronic Commerce in Organizations* (pp. 57-79).

www.irma-international.org/article/the-determination-of-user-satisfaction-with-personal-internet-banking-services-in-the-context-of-australia/160310

Viewing E-Learning Productivity from the Perspective of Habermas' Cognitive Interests Theory

Minh Q. Huynh (2005). *Journal of Electronic Commerce in Organizations* (pp. 33-45).

www.irma-international.org/article/viewing-learning-productivity-perspective-habermas/3454

Intrusion Detection and Vulnerability Analysis of Mobile Commerce Platform

Changhua Zhu and Changxing Pei (2008). *Electronic Commerce: Concepts, Methodologies, Tools, and Applications* (pp. 2047-2063).

www.irma-international.org/chapter/intrusion-detection-vulnerability-analysis-mobile/9602

Empirical Study on Multi-Channel Service Quality and Customer Loyalty of Retailers

Qi Yong-zhi (2014). *Journal of Electronic Commerce in Organizations* (pp. 1-12).

www.irma-international.org/article/empirical-study-on-multi-channel-service-quality-and-customer-loyalty-of-retailers/124072