

Chapter 8

Security and Trust in Cloud Computing

Eric Kuada

Ghana Institute of Management and Public Administration, Ghana

ABSTRACT

The discussion of security and trust issues in this book chapter will follow from the discussions on the role of virtualization in cloud computing and hence the impact that the various categories of virtualization such as server virtualization, network virtualization, storage virtualization, and application virtualization have on the security and trust issues in cloud computing. It will be evident from these discussions that virtualization introduces a number of security and risk related challenges in cloud computing based on the three security objectives of confidentiality, integrity, and availability; and the two main other related security objectives of authenticity and accountability of information systems that were adopted for this discussion. It was however also noted that if the necessary recommended best practices of virtualizations are faithfully adhered to, then virtualization can actually lead to improvement or enhancement in the security posture of cloud environments.

INTRODUCTION

Cloud computing is about the offering of computing resources as a service rather than as a commodity. This means that customers pay for the amount of resources used instead of purchasing complete hardware to build their own Information Technology (IT) infrastructure or purchasing whole licenses, which are often woefully

DOI: 10.4018/978-1-5225-0741-3.ch008

Security and Trust in Cloud Computing

underutilized or they even often find out later that they do not need. This relatively new trend of computing is essentially the repackaging of traditional Information and Communication Technology (ICT) infrastructure and software solutions such as processing capacity, storage and storage network systems, networking capabilities, user and enterprise software solutions, as virtualized resources that are then delivered by a cloud service provider to its customers as an on-demand, pay-per-use, and a customer self-provisioned service normally through a Web portal over a network such as the Internet (Kuada, Adanu, & Olesen, 2013).

The reason cloud computing appears to have captured the attention of businesses is the numerous benefits it offers despite the security risk challenges it poses to both the cloud service providers and their customers. It definitely has different appeals to different businesses or organizations depending on the nature, size, industry, age, etc., of the institution; but generally, it is mostly taken as a given that cloud computing provides flexibility, increase IT efficiency, elasticity, obviation of capital expenditure for acquiring IT resources, and improves reliability and recovery from disasters. It should be obvious that without the necessary technologies to support this trend of computing, and the addressing of the risk challenges it poses, despite all the benefits it promises, it wouldn't have come to fruition. Some of the technological factors that are facilitating cloud computing include the availability and drastic increase in reliable broadband internet access, the advancements in virtualization technologies, and the shift of the development of majority of both enterprise and desktop applications as web services and web application. For the purposes of the topic being treated in this work (security and trust in cloud computing), the focus of the discussion on the technological advancement will be on virtualization technologies and application or service development for cloud computing environments.

The main purpose of this book chapter is to discuss security issues in cloud computing. The chapter also seek to discuss the concept of trust and the issues of trust in the context of cloud computing. It also tries to demonstrate the role of security in modelling the concept of trust in cloud computing environments. Finally, it sets a research agenda for further work on this topic.

Motivations for Cloud Adoption

Cloud computing provides several potential benefits to enterprises. These benefits are usually so appealing that despite the equally major risks of adopting cloud services, companies are willing to give it a try. Some of these major motivating factors for cloud adoption by enterprises include flexibility, efficiency, resource utilization, availability, initial capital cost for IT infrastructure obviation, operational cost reduction, speed in resource acquisition and time to market, and business agility. Enterprises normally acquire IT resources for their business processes (e.g. develop-

25 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-and-trust-in-cloud-computing/164697

Related Content

Risk Management in a Pandemic Crisis at a Global Non Profit Health Care Organization

Drew Sugarett (2012). *International Journal of Risk and Contingency Management* (pp. 1-17).

www.irma-international.org/article/risk-management-pandemic-crisis-global/74749

Privacy-Preserving Data Mining and the Need for Confluence of Research and Practice

Lixin Fu, Hamid Nematiand Fereidoon Sadri (2007). *International Journal of Information Security and Privacy* (pp. 47-63).

www.irma-international.org/article/privacy-preserving-data-mining-need/2456

Reducing Risk by Segmentation

Michael Todorov Todinov (2017). *International Journal of Risk and Contingency Management* (pp. 27-46).

www.irma-international.org/article/reducing-risk-by-segmentation/181855

Security and Privacy Challenges in Big Data

Dharmpal Singh, Ira Nathand Pawan Kumar Singh (2021). *Research Anthology on Privatizing and Securing Data* (pp. 15-41).

www.irma-international.org/chapter/security-and-privacy-challenges-in-big-data/280168

Taxonomies of User-Authentication Methods in Computer Networks

Göran Pulkkis, Kaj J. Grahnd Jonny Karlsson (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 737-760).

www.irma-international.org/chapter/taxonomies-user-authentication-methods-computer/23125