

## Chapter 22

# Enterprise Cloud Adoption: A Quantitative Exploratory Research

**Omondi John Opala**

*Devry University, USA & Cisco Systems, USA*

**Shawon S. M. Rahman**

*University of Hawaii-Hilo, USA & King Saud University, Saudi Arabia*

**Abdulhameed A. Alelaiwi**

*King Saud University, Saudi Arabia*

### ABSTRACT

*Cloud computing is synonymous with outsourced data center management and agile solution architecture that improves the scalability for delivery of services for enterprises. It has the capability to revolutionize how data is delivered from commodity to Information Technology as a service. At its core, Cloud computing is a new approach to distributed computing and shared pooling of IT infrastructure linked together to offer centralized IT services on demand. Companies that provide Cloud computing services manage multiple virtualized computation systems that allow for dynamic on-demand provisioning of IT delivery as services. This chapter presents a study of the factors that influence the adoption of Cloud computing in enterprises based on managements' perception of security, cost-effectiveness, and IT compliance. The results of a linear regression analysis testing are presented, which indicate that managers' perceptions of cost-effectiveness and IT compliance are more significantly correlated to the enterprise adoption of Cloud computing than security.*

## **INTRODUCTION**

The traditional network delivery of IT services requires rigid capacity planning and limiting the ability to offer on-demand software management and related IT functionality. However, the *Cloud computing model* improves IT service delivery, but adds complexities in security and IT compliance integration with the organization's procedures (Lombardi & Di Pierto, 2011). The elastic nature of Cloud computing provides customers with resources such as CPU and storage space on demand, thereby, creating an illusion of unlimited computing and network capacity and availability (Armbrust et al., 2010).

The need for Cloud computing arises from the deluge of raw data, demand for high compute intensive applications, requirement of high availability of systems, and the desire for cost-effective IT delivery solutions. Such applications include particle physics, biology, chemistry, knowledge base databases, big data requirements, enterprise resource planning, customer resource management, and financial research that mandate the use of large computer infrastructures to achieve performance gains for organizations (Ekanayake et al., 2010), among others. The adoption of Cloud computing provides benefits to organizations that include pay-as-you-go billing, on-demand capabilities, and reduction in IT operational expenses (Anderson & Swager, 2004).

This study was intended to provide data on *security, cost-effectiveness, and IT compliance* factors influencing adoption of Cloud computing (Truong, 2010) in enterprises. The security risks associated with the existing Cloud adoption model involve issues of determining data ownership, confidentiality, integrity, privacy, and virtualization (Subashini & Kavitha, 2010). Compliance requirement exists in every facet of IT, requiring rigorous enforcement of policies to encourage organizations to maintain acceptable processes

to protect customer and personal identifiable data from unlawful access (Luthy & Forcht, 2006). For instance, violation of the Health Insurance Portability and Accountability Act and Sarbanes Oxley Act of 2002 compliance requirements, carries penalties ranging from fines to imprisonment (Hoffman & Podgurski, 2007).

In Cloud computing, however, the compliance assurance process is not clear when data ownership and storage locations are not under the control of the enterprise organization. IT compliance for Cloud-enabled networks includes internal IT processes such as system logging, log analysis, authentication, and authorization; as well as data archiving, image back-ups, and physical security of servers in the Cloud (Jarrell, Welker, Silsbee, & Tucker, 2008). Compliance risks associated with IT have been prevalent in outsourced services (Ahmed, 2011; Blaskovich & Mintchik, 2011) and the recent increase in the number of data security breaches has made security requirements a priority consideration for Cloud adoption (Burns & Peterson, 2010).

The shared resources nature of Cloud computing delivery hinders security processes such as data confidentiality and data integrity, as well as data availability requirements, because multiple customers use the same resources to access their data (Chakraborty, Ramireddy, Raghu, & Rao, 2010). Reliability can be a serious problem for Cloud users. Salesforce.com, for example, left customers without service for six hours in February 2008. Amazon's Simple Storage Service (S3) and Elastic Compute Cloud (EC2) suffered a three hour outage in the same month. In early 2009, Google's Gmail went down for three hours, thereby preventing its 113 million users from accessing their emails or the documents that they store online on Google Docs.

This chapter is structured as follows. The background section provides general information on Cloud computing adoption and delivery models.

33 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/enterprise-cloud-adoption/115444](http://www.igi-global.com/chapter/enterprise-cloud-adoption/115444)

## Related Content

---

### **MADES FP7 EU Project: Effective High Level SysML/MARTE Methodology for Real-Time and Embedded Avionics Systems**

Alessandra Bagnato, Imran Quadri, Etienne Brosse, Andrey Sadovykh, Leandro Soares Indrusiak, Richard Paige, Neil Audsley, Ian Gray, Dimitrios S. Kolovos, Nicholas Matragkas, Matteo Rossi, Luciano Baresi, Matteo Carlo Crippa, Stefano Genolini, Scott Hansen and Gundula Meisel-Blohm (2014). *Handbook of Research on Embedded Systems Design* (pp. 181-208).

[www.irma-international.org/chapter/mades-fp7-eu-project/116110](http://www.irma-international.org/chapter/mades-fp7-eu-project/116110)

### **A Taxonomy Built on Layers of Abstraction for Time and State Vulnerabilities**

Horia V. Corcalciuc (2013). *International Journal of Secure Software Engineering* (pp. 40-66).

[www.irma-international.org/article/taxonomy-built-layers-abstraction-time/77916](http://www.irma-international.org/article/taxonomy-built-layers-abstraction-time/77916)

### **Comparative Analysis of Texture Classification Using Local Binary Pattern and Its Variants**

Richa Sharma and Madan Lal (2017). *International Journal of Information System Modeling and Design* (pp. 45-56).

[www.irma-international.org/article/comparative-analysis-of-texture-classification-using-local-binary-pattern-and-its-variants/199002](http://www.irma-international.org/article/comparative-analysis-of-texture-classification-using-local-binary-pattern-and-its-variants/199002)

### **Software Asset Re-Use: Migration of Data-Intensive Legacy System to the Cloud Computing Paradigm**

Richard Millham (2012). *Software Reuse in the Emerging Cloud Computing Era* (pp. 1-27).

[www.irma-international.org/chapter/software-asset-use/65165](http://www.irma-international.org/chapter/software-asset-use/65165)

### **Agile Software Development: The Straight and Narrow Path to Secure Software?**

Torstein Nicolaysen, Richard Sassoon, Maria B. Line and Martin Gilje Jaatun (2010). *International Journal of Secure Software Engineering* (pp. 71-85).

[www.irma-international.org/article/agile-software-development/46153](http://www.irma-international.org/article/agile-software-development/46153)