Chapter 90
Cloud Risk Resilience:
Investigation of Audit Practices and Technology Advances – A Technical Report

Akhilesh Mahesh
University at Buffalo School of Management, Amherst, USA

Niranjali Suresh
Pricewaterhouse Coopers, Atlanta, USA

Manish Gupta
University at Buffalo School of Management, Amherst, USA

Raj Sharman
University at Buffalo School of Management, Amherst, USA

ABSTRACT

Cloud computing has been instrumental in transforming the way we store, access and process data. With mobility being the primary objective of the current market, cloud computing offers exactly that. Cloud offers convenient access to a shared pool of computing resources that can be configured and deployed with minimal effort which is used to deliver computing services over the internet. Exercising these advantages come with a plethora of security risks that need to be addressed. The security issues in cloud are complex due to the nature of implementation and regulations that govern them. In this article, we examine existing research on cloud risk and the various frameworks to manage risk. The objective is to map the risk with the audit control and technology that will help in mitigating the risk. We analysed the various cloud security solutions and came up with a list that best help in the effective management of the cloud risk and security issues.

DOI: 10.4018/978-1-7998-2466-4.ch090

1. INTRODUCTION

Cloud computing is transforming and redefining the design and procurement of IT infrastructure and software thereby providing attractive services to its users across the globe. The US National Institute of Standards and Technology (NIST) defines cloud computing as "…a model for enabling ubiquitous, convenient, on - demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction…" (Mell and Grance, 2011). The technology allows individuals and enterprises to avoid committing large capital outlays when purchasing and managing or operating software and hardware. Cloud reduces strain on developers by allowing them to focus their efforts on coding business logic rather than concerning about over or under provisioning resources for a service based on the market for a service. Large batch-oriented tasks can be efficiently executed with minima1 resources simply through scalable programming. In cloud, 1000 servers for one hour costs no more than using one server for 1,000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. As Heiser and Nicolett (2008) of Gartner mention that cloud computing lacks transparency because it is, for most part, provided by an external entity and is a method for "storing and processing your data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from multiple customers." In the same vein, companies are also advised they consider all the involved risks in moving to cloud and also evaluate all the required controls around the protection of data and processes before migrating to cloud.

One of the main contributions of the chapter is reviewing recent innovations in cloud computing in security space and how they are aligned to manage risks from specific areas of cloud implementation. The discussions on extant literature on cloud, auditing focus areas and risk assessment frameworks help the chapter highlight how recent innovations are poised to manage risks. The primary tenet of the research is innovation in cloud computing. Innovation in IT is one of the widely studied topics (Baregheh et al., 2009) with many acceptable definitions. We use Rogers' (1998) definition as "introduction of a new product or a 'qualitative change' in a product, a process…" Not all innovations have the same impact and vary based on type of innovation (Grover et al., 1997; Adomavicius et al., 2007; Christensen et al., 2007; Carlo et al., 2011). Innovation has been linked to higher productivity, growth, and development. (Fagerberg, 2005; Kaplinsky et al., 2009). In recent years, with increasing adoption of IT, the impact of innovations is on rise as well and has been of high interest to researchers (Avgerou, 2008; Xiao et al., 2013).

This chapter is organized in six sections that delve deep into cloud security and innovations. Having introduced cloud computing as a technology platform in the first section, we move on to discuss key risks in cloud, their impact on environmental security and customer's business processes. The third section elaborates on significant aspects of cloud that require additional attention through continuous auditing. Audit challenges and suggested approaches have been delineated in line with industry best practices. This is followed by a description of some of the most prominent cloud computing frameworks and working groups that are widely used accepted across industries and geographies as enablers and benchmarks while setting up cloud systems. The following section briefly examines additional challenges specific to particular cloud computing domains such as banking, medical, and government sectors. The final section discusses recent innovations in cloud computing and its impact on transforming enterprise cloud implementations and managing cloud computing risks. Figure 1 shows how different sections and approach for the study.