Chapter 78
Cloud Computing Security and Risk Management

Yoshito Kanamori
University of Alaska Anchorage, USA

Minnie Yi-Miin Yen
University of Alaska Anchorage, USA

ABSTRACT

Cloud computing is changing the way corporate computing operates and forcing the rapid evolution of computing service delivery. It is being facilitated by numerous technological approaches and a variety of business models. Although utilizing the infrastructure of existing computing and networking technologies, different cloud service providers (CSPs) are able to unite their efforts and address a much broader business space. As a result, confusion has emerged and questions have risen from both Information Technology (IT) and business communities. How cloud environments differ from traditional models, and how these differences affect their adoption are of major importance. In this chapter, the authors first clarify misperceptions by introducing the new threats and challenges involved in cloud environments. Specifically, security issues and concerns will be depicted in three practical scenarios designed to illuminate the different security problems in each cloud deployment model. The chapter also further discusses how to assess and control the concerns and issues pertaining to the security and risk management implementations.

INTRODUCTION

Cloud computing is a new, rapidly evolving model of computing service delivery and has been receiving more and more attention from the IT industry. Although cloud computing integrates the latest computing and networking technologies – which are also used in non-cloud (or traditional) IT infrastructures – it has the potential to deliver more cost-effective and flexible management mechanisms to the IT industry, especially when compared to the traditional, dedicated server hosting model. One of the major characteristics of cloud computing is "Resource Pooling," where a cloud service provider (CSP) pools resources (e.g., computational power, storage space) in a server farm, or datacenter, to run on-demand virtual instances of their customers' servers. Companies can

DOI: 10.4018/978-1-4666-6539-2.ch078

purchase software, platforms, or infrastructures from the CSP through the Internet only when they need it, while the CSP charges the companies based on the amount of services used. Companies can reduce their hardware and software needs, which in turn can reduce their IT staffing requirements. However, this promising technology also brings security and privacy challenges, to not only IT and auditing professionals, but to the business leaders who need to make decisions on whether to adopt a cloud computing model (Armbrust, et al., 2009; Takabi, Joshi, & Ahn, 2010).

In this chapter, security and privacy challenges in the cloud computing environment are discussed. Instead of simply listing the challenges, specific security issues and concerns are depicted in three practical scenarios designed to illuminate the different security problems in each cloud deployment model in the next section. In the third section, the common security issues are discussed in all cloud models. Security and risk management implementation issues will be briefly introduced in the fourth section. Finally, our conclusion and recommendation are given in the last section.

THREATS AND SECURITY CHALLENGES

One of the primary challenges cloud computing faces is data security. When users store their sensitive data on public cloud servers, security will always be a great concern. The major problem behind the data security issue is that cloud servers and data owners are not within the same trusted domain (Yu, Wang, Ren, & Lou, 2010). So, it is difficult for customers to assess the security measures existing in the public cloud service provider (CSP) environment (Choudhary, 2007). For example, when a customer uses a web application provided by a third party to process data, the processed data may be temporarily stored on the third party's server. The customer expects the third party to be in compliance with the regulations required for the customer's business (e.g., HIPAA (HHS, 1996).) However, there is no easy way to verify how the third party actually processes and stores its customer data. The more third party applications a customer uses, the more threats and challenges that customer will face in the cloud environment.

In the following three scenarios, the security issues and challenges in cloud environments are illustrated based on three key cloud deployment models – private, public, and hybrid clouds – using three distinct delivery models – Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Mather, Kumaraswamy, & Latif, 2009; Krutz & Vines, 2010).

Three Cloud Computing Scenarios

In all scenarios, a company provides users with two web applications: (1) an Audio Editor (AE); and (2) a Movie Editor (ME), which uses the AE as an external component to edit the movie's audio track. Since movie editing in general requires a large amount of computations, the ME application copies the user's data as the input and returns edited data to the user. The company has internal users who use the applications, developers who develop the applications, and administrators who manage the company's IT infrastructure. These web applications are also available to customers (i.e. external users). A database is used to manage user account information, including the internal users, and customer or external user information. Customers in the scenarios use the web applications over the Internet. Cloud Service Providers (CSPs) deliver cloud services (i.e., SaaS, PaaS, and IaaS) to the company.

The first company, Company X, uses the private cloud model for its internal users while making the applications available through the public cloud for customers (see Figure 1). The second company, Company Y, utilizes the public cloud for both its internal users and development, as well as for its external users (see Figure 2). The