# Chapter 67
# Security in Cloud Computing

**Alpana M. Desai**
*University of Alaska Anchorage, USA*

**Kenrick Mock**
*University of Alaska Anchorage, USA*

## ABSTRACT

*Cloud computing has recently emerged in prominence and is being rapidly adopted by organizations because of its potential and perceived benefits of flexibility and affordability. According to surveys conducted in 2008 and 2009 by International Data Corporation (IDC) of IT executives and CIOs, security was cited as the top concern for the adoption of cloud computing. Enterprises that plan to utilize cloud services for their infrastructure, platform, and/or software needs must understand the security risks and privacy issues related to cloud computing. This chapter discusses the technical, legal, and policy/organizational security risks of cloud computing, and reviews recommendations/strategies for managing and mitigating security threats in cloud computing. It also presents vendor-specific solutions and strategies that cloud service providers are implementing for mitigating security risks in cloud computing.*

## INTRODUCTION

The benefits of cloud computing include easy and fast deployment, pay-as-you-go model, benefits of scale, and less in-house IT staff and costs. According to a 2008 survey conducted by International Data Corporation (IDC), a global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets, security and performance were the top two challenges of cloud computing that were cited by senior IT executives and CIOs, (IDC, 2008b). IDC conducted another survey in 2009 and the top concern was still security but availability was the second top concern and performance moved from the second top concern in 2008 to the third top concern in 2009 (IDC, 2009). The projected increase of spending on public IT cloud services is expected to increase from $16.5billion in 2009 to $55 billion in 2014, (IDC, 2010).

Cloud computing is rapidly being adopted not just domestically but also globally. The European Network and Information Security Agency (ENISA), an EU agency, launched a survey of the actual needs, requirements and expectations of

DOI: 10.4018/978-1-4666-6539-2.ch067

Small and Medium Enterprises (SMEs) for cloud computing services. As per this survey the top two concerns of SMEs were information security and liability. In particular the major concerns of SMEs were confidentiality of their information and liability for incidents involving the infrastructure, (ENISA, 2009).

Thus it is important to understand risks associated with adoption of cloud computing. Enterprises utilize cloud services for their infrastructure, platform, and/or software needs. In this chapter, security risks and security benefits of cloud computing are discussed. Technical, legal, and organizational security risks of cloud computing are also presented as are security risks in the traditional context and as related to cloud computing in particular. Some of the security issues that are discussed in this chapter are insecure interfaces and APIs; risks associated with multi-tenancy; data leakage; malicious insider; data protection risks; data ownership and accountability; compliance risks; and customer lock-in issues.

Several strategies exist and are being proposed by vendors and groups to mitigate security risks in cloud computing. Solutions and strategies that cloud service providers are implementing for mitigating security risks in cloud computing are presented. To convey reliability and security of their cloud services, vendors seek and maintain compliance with existing security standards. Some of these security standards that are already in place and are in development stages are discussed in this chapter.

## DEFINITION OF CLOUD COMPUTING

Cloud computing has been defined differently by various groups (comprising of industry, academia, and government). Armbrust, et al. (2009) state that "cloud computing is a new term for a long-held dream of computing as a utility" due to its pay-as-you-go characteristic. They refer to cloud computing as "both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services."

IDC (2008a) makes a distinction between cloud services and cloud computing by first defining cloud services with eight specific attributes (off-site/third party provider; accessed via the internet; minimal/mo IT skills required to implement; provisioning; pricing model; user interface; system interface; and shared resources/common versions) and then defining cloud computing as consisting of "a growing list of technologies and IT offerings that enable cloud services as defined by its eight characteristics."

In this article, we use NIST's (National Institute of Standards and Technology) definition of cloud computing. NIST defines cloud computing as a model for enabling 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 & Grance, 2009)

This cloud model promotes availability and it is composed of five essential characteristics, three service models, and four deployment models.

The five essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. A sixth characteristic that is not considered essential but is often discussed as such and is identified as an important element of cloud computing by the Cloud Security Alliance (CSA) is multi-tenancy (Cloud Security Alliance, 2009). A tenant refers to a user's application that runs on the cloud and requires some degree of security or exclusivity. Multi-tenancy refers to multiple tenants running on some shared infrastructure within the cloud. Such sharing could occur at different levels, for example, tenants could share the same hardware separated via virtualization, or tenants could share