Chapter 25
A Framework for Compliance and Security Coverage Estimation for Cloud Services: A Cloud Insurance Model

Dipankar Dasgupta
University of Memphis, USA

Durdana Naseem
University of Memphis, USA

ABSTRACT

Many organizations are adopting cloud services to reduce their computing cost and increase the flexibility of their IT infrastructure. As cloud services are moving to the mainstream to meet major computing needs, the issues of ownership and chain of custody of customer data are becoming primary responsibilities of providers. Therefore, security requirements are essential for all service models (while the degree of defensive measures may vary) along with satisfying industry standard compliances. The authors develop an insurance framework called MEGHNAD for estimating the security coverage based on the type of cloud service and the level of security assurance required. This security coverage estimator may be useful to cloud providers (offering Security as a Service), cloud adopters, and cloud insurers who want to incorporate or market cloud security insurance. This framework allows the user/operator to choose a cloud service (such as Saas, Paas, IaaS) and other pertinent information in order to determine the appropriate level of security insurance coverage. This chapter describes an extension to the MEGHNAD (version 2.0) framework by incorporating security-related compliances. The compliance for each sector requires specific protection for online data such as transparency, respect for context, security, focused collection, accountability, access, and accuracy. The MEGHNAD tool can also generate a SLA document that can be used for monitoring by a certified Third-Party Assessment Organization (3PAO).

DOI: 10.4018/978-1-4666-6539-2.ch025

1. INTRODUCTION

With rapidly changing computing and Information Technologies, it is becoming more expensive for companies and organizations to regularly update/ purchase hardware and software licenses and keep big IT departments with highly technical professionals. Cloud computing has evolved the concept of how we deploy, maintain, and access software, platforms, and infrastructure utilizing the high-speed Internet connectivity. Analysts forecasting a long-running trend where all types of business services will be virtualized, enabling massive interoperability, which will potentially lead to huge cost savings. So the cloud computing is becoming more attractive because of the possibilities in significant cost reduction in IT operations.

While some small and medium size companies are moving to cloud services for their IT need, they are very concerned about data privacy, security and compliance requirements (such as PCI DSS, HIPAA, GLBA, SOX, etc.). For example, HIPAA (Health Insurance Portability and Accountability Act) requires insurance portability, administrative simplification and fraud enforcement like privacy and security. Another example, PCI-DSS compliance, was set up to improve the Information Security of financial transactions related to credit and debit cards. GLBA (Gramm-Leach-Bliley Act) compliance requires analyzing the risks before moving customer information into emerging technology models. While security requirements are essential for all service models, as these three segments have differences and similarities, they vary in the degree of defensive measures and should be considered by organizations when selecting a cloud service. In any cloud service, satisfying compliance requirements will ensure the following:

- Best and improved protection of companies' critical data and its availability.
- Reduce the liability due to security breach.
- Timely audition to ensure full compliancy and reporting.
- Cost efficient service that meets the customer needs.

To guarantee the above-mentioned benefits, the cloud provider needs to be carefully assessed by each customer or 3PAO to assure that the key requirements of security and compliances are met (Dokras, 2009). Moving application and data to the cloud has many advantages but when it comes to sensitive data it is yet very risky. It is important to understand the cloud architecture, access control and network security and "know where your data is and know where your data is going." (Pennell, 2011).

2. CLOUD SERVICE MODELS AND COMPLIANCES

Cloud computing facilitates delivering services over the Internet are also known as cloud services. In this section we will describe different cloud service models, compliances and the necessity of SLA document with proper information on security coverage.

2.1. Cloud Service Models

Cloud computing has three main different service models which provide services at different levels (DoD, 2011), (Rackspace Hosting, 2011) as illustrated in Figure 1.

2.1.1 Software as a Service (SaaS)

In SaaS, the vendor uses the cloud service to host software applications for the customers. The vendor controls and maintains the physical computer hardware, servers, network, operating systems, and software applications. The customers have very limited control on settings specific to the user. Some SaaS vendors includes CRM,