# Chapter 10
# Cloud Security Engineering:
## Avoiding Security Threats the Right Way

**Shadi Aljawarneh**
*Isra University, Jordan*

## ABSTRACT

*Information security is a key challenge in the Cloud because the data will be virtualized across different host machines, hosted on the Web. Cloud provides a channel to the service or platform in which it operates. However, the owners of data will be worried because their data and software are not under their control. In addition, the data owner may not recognize where data is geographically located at any particular time. So there is still a question mark over how data will be more secure if the owner does not control its data and software. Indeed, due to shortage of control over the Cloud infrastructure, use of ad-hoc security tools is not sufficient to protect the data in the Cloud; this paper discusses this security. Furthermore, a vision and strategy is proposed to mitigate or avoid the security threats in the Cloud. This broad vision is based on software engineering principles to secure the Cloud applications and services. In this vision, security is built into all phases of Service Development Life Cycle (SDLC), Platform Development Life Cycle (PDLC) or Infrastructure Development Life Cycle (IDLC).*

## INTRODUCTION

Due to lack of control over the Cloud software, platform and/or infrastructure, several researchers stated that a security is a major challenge in the Cloud. In Cloud computing, the data will be virtualized across different distributed machines, hosted on the Web (Taylor, 2010; Marchany, 2010). In business respective, the cloud introduces a channel to the service or platform in which it could operate (Taylor, 2010).

Thus, the security issue is the main risk that Cloud environment might be faced. This risk comes from the shortage of control over the Cloud environment. A number of practitioners described this point. For example, Stallman (Arthur, 2010) from the Free Software Foundation re-called the Cloud computing with Careless Computing be-

DOI: 10.4018/978-1-4666-1879-4.ch010

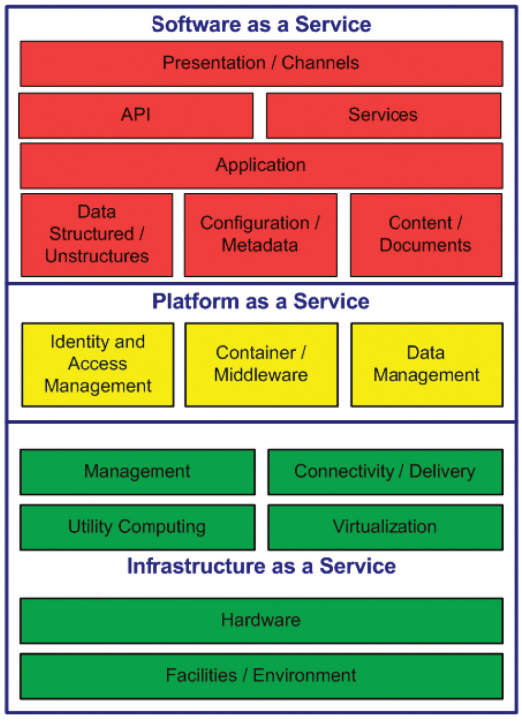
cause the Cloud customers will not control their own data and software and then there is no monitoring over the Cloud providers and subsequently the data owner may not recognize where data is geographically located at any particular time.

Threats in the Cloud computing might be resulted from the generic Cloud infrastructure which is available to the public; while it is possessed by organization selling Cloud services (Marchany, 2010; Chow et al.,2009).

In Cloud computing, software and its data is created and managed virtually from its users and might only accessible via a certian cloud's software, platform or infrastructure. As shown in Figure 1, there are three Cloud models that describe the Cloud architecture for applications and services (Taylor, 2010; Marchany, 2010):

1. The Software as a Service (SaaS) model: The Cloud user rents/uses software for use on a paid subscription (Pay-As-You-Go).

*Figure 1. Models of Cloud environment-taken from (Taylor, 2010)*




2. The Platform as a Service (PaaS) model: The user rents a development environment for application developers.
3. The Infrastructure as a Service (IaaS) model: The user uses the hardware infrastructure on pay-per-use model, and the service can be expanded in relation to demands from customers.

In spite of this significant growth, a little attention has been given to the issue of Cloud security both in research and in practice. Today, academia requires sharing, distributing, merging, changing information, linking applications and other resources within and among organizations. Due to openness, virtualization, distribution interconnection, security becomes critical challenge in order to ensure the integrity and authenticity of digitized data (Cárdenas et al., 2005; Wang et al., 2005).

Cloud opts to use scalable architecture. Scalability means that hardware units that are added bringing more resources to the Cloud architecture (Taylor, 2010). However, this feature is in tradeoff with the security. Therefore, scalability eases to expose the Cloud environment and it will increase the criminals who would access illegally to the Cloud storage and Cloud Datacenters as illustrated in Figure 2.

Availability is another characteristic for Cloud. So the services, platform, data can be accessible at any time and place. Cloud is candidate to expose to greater security threats, particularly when the cloud is based on the Internet rather than an organization's own platform (Taylor, 2010).

Although the security is a risk in the Cloud environment, several companies are offering now Cloud services including Microsoft Azure Services Platform, Amazon Web Services, Google and open source Cloud systems such as Sun Open Cloud Platform for academic, customers and administrative purposes (Taylor, 2010). Yet, some organizations have not realized the importance of security for the Cloud systems. These organiza-