Chapter 45
Secure Architecture for Cloud Environment

Kashif Munir
Malaysia University of Science and Technology, Malaysia

Sellapan Palaniappan
Malaysia University of Science and Technology, Malaysia

ABSTRACT

Cloud computing is set of resources and services offered through the internet. Cloud services are delivered from data centers located throughout the world. Enterprises are rapidly adopting cloud services for their businesses, measures need to be developed so that organizations can be assured of security in their businesses and can choose a suitable vendor for their computing needs. In this chapter we identify the most vulnerable security threats/attacks in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing and propose relevant solution directives to strengthen security in the cloud environment. This chapter also discusses secure cloud architecture for organizations to strengthen the security.

INTRODUCTION

With Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has become important issues to highlight. There are a number of security issues/ concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers.[1] In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information(Philip Wik, 2011).

Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software.

DOI: 10.4018/978-1-5225-5634-3.ch045

NIST defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction"(Mell P, Grance T, 2011) . It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use. It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues. According to (Ponemon, 2011), 91% of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment.

As shown in Figure 1, Cloud services are offered in terms of Infrastructure-as-a- service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS). It follows a bottom-up approach wherein at the infrastructure level; machine power is de- livered in terms of CPU consumption to memory allocation. On top of it, lies the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level resides the application layer, delivering software outsourced through the Internet, eliminating the need for in-house maintenance of sophisticated software [6]. At the application layer, the end users can utilize software running at a remote site by Application Service Providers (ASPs). Here, customers need not buy and install costly software. They can pay for the usage and their concerns for maintenance are removed (Kashif & Sellapan, 2012).

SECURITY CONCERNS OF CLOUD COMPUTING

While the benefits of the cloud increase with experience, the challenges of cloud show a sharp decrease as organizations gain expertise with cloud.

Figure 1. Cloud Computing represented as a stack of service (Kashif & Sellapan, 2012)