Chapter 40
Web Services Gateway:
Taking Advantage of the Cloud

Jide Aniyikaiye
Sullivan University, USA

Emmanuel Udoh
Sullivan University, USA

ABSTRACT

Cloud computing has many advantages and is being used increasingly as an efficient and safe solution for web based services. This on-demnd self-service provides network access to a shared pooi of redundant computing resources. Software applications are being developed in the cloud and there are demands for the interoperability of these applications. A common way to meet this demand is the development of Web services (applications), taking advantage of Service-oriented architecture principles. These loosely coupled Web base components pose some security challenges. This paper examines Security as a Service (SECaaS) solutions, as well to propose a new approach to security management in the cloud.

1. INTRODUCTION

Cloud computing is the most efficient model for enabling convenient, mobile, network access to a shared pool of redundant computing resources, including public and private networks, servers, storage, applications, and services, capable of rapid provisioning and effortless access (Mell & Grance, 2009). Cloud Computing is defined as shared hosting and applications delivered as services over the Internet to end-users (Armbrust et al., 2010).

Cloud computing is a large-scale distributed computing paradigm (Foster et al., 2008) that refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services (Armbrust et al., 2010). The diagram shown in Figure 1 depicts several hardware having access to shared computing resources and services, made available over the internet. Cloud Computing is rapidly being deployed as an efficient and safe solution for Web services applications (Mell & Grance, 2009).

DOI: 10.4018/978-1-5225-5634-3.ch040

A significant advantage of Cloud Computing is an on-demand self-service solution, which provides dynamic scalability, or *elasticity*. It enables Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), and reduces per unit costs by spreading fixed costs over a large number of users. Also, the cost can be significantly cheaper because it eliminates support related expenses associated with maintaining the in-house data center (Saleem, 2011). In other words, each level (Application, Platform, and Infrastructure) referenced in Figure 1 are offered on as-service basis. Cloud architecture prevents web applications from failing during peak loads, effectively supporting nearly unlimited end users. "Much like plugging in a microwave in order to power it doesn't require any knowledge of electricity, one should be able to plug in an application to the Cloud in order to receive the power it needs to run, just like a utility" (Varia, 2010, p. 4).

With the proliferation of cloud computing, comes different security challenges in its adoption. Also, with the different service delivery models (PaaS, SaaS & IaaS), there are different levels of security requirements in the cloud environment (Subashini & Kavitha, 2011). According to the result from a survey done by the Cloud Security Alliance and IEEE, there are numerous enterprises eager to adopt cloud computing but lack the security measures to accelerate the adoption of cloud on a wide scale so as to respond to trending regulatory drivers.

This paper presents a fresh approach to security management based on a Security-as-a-Service (SECaaS) paradigm (service model). The proposed service concept facilitates securing cloud based Web services developed on a service-oriented architecture.

Figure 1. Cloud computing [https://en.wikipedia.org/wiki/Cloud_computing]