Chapter 66
Different Perspectives of Cloud Security

M. Sundaresan
Bharathiar University, India

D. Boopathy
Bharathiar University, India

ABSTRACT

Cloud storage systems can be considered to be a network of distributed datacenters that typically use cloud computing technology like virtualization and offer some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations. Basic cloud storage is generally not designed to be accessed directly by users but rather incorporated into custom software using API. Cloud computing involves other processes besides storage. In this chapter, the authors discuss different viewpoints for cloud computing from the user, legal, security, and service provider perspectives. From the user viewpoint, the stored data creates a mirror of currently available local data. The backup feature allows users to recover any version of a previously stored data. Synchronization is the process of establishing consistency among the stored data. From the legal viewpoint, provisions regulating the user processing and storage of the data must have to be constant from when the data is stored in the cloud. The security viewpoint requires interaction with the Web application, data storage, and transmission. The service provider viewpoint requires the maximum level of cloud storage service at the minimum cost.

CLOUD SECURITY

New computing models are always facing the problems like security, controllability, accessibility, portability, operability. Cloud computing model is not an exceptional from this list. The security problem is vital issue in cloud computing. The Cloud Service Providers (CSP), Cloud Service Vendors (CSV) and Cloud Service Users (CSU) are facing real time problems and still they are trying to come out from the issues. The security issues differ and vary based on the following perspectives and they are:

1. Service Provider perspective
2. User Perspective
3. Security Perspective
4. Legal Perspective

DOI: 10.4018/978-1-4666-6539-2.ch066

1. Service Provider Perspective

The Cloud Service Providers are classified into three types, based on the kind of service they provide. Here the consumer plays a major role.

Software as a Service Provider (SaaS): The consumer is provided the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (for example, web-based email). The consumer does not manage or control the underlying cloud infrastructure that includes network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a service Provider (PaaS): The consumer is provided the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure that includes network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configuration.

Infrastructure as a service Provider (IaaS): The consumer is provided the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of some of the networking components (for example, host firewalls).

The cloud computing is an umbrella term. The cloud service providers are interlinked between them with the certain limitations and conditions. According to that some important and mandatory things are discussed.

1.1 Connectivity

The Connectivity between the service providers is the most important aspect. So to avoid the confusion and misleading, some important things are framed and followed by them. This may help them to provide the secured services to their clients.

1.1.1 SSL

The Secure Socket Layer is used to provide a secure communication channel. When the application is independent, it is optimized for Hyper Text Transfer Protocol (HTTP) and usually used for secure communication with a web server. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. The complexities of the SSL protocol remain invisible to your customers.

1.1.2 Virtual Private Networks

A VPN securely transports IP packets across the Internet backbone by establishing tunnel endpoints that negotiate a common encryption and authentication scheme prior to transport. Virtual private network enables a computer to send and receive data across shared or group or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites

1.1.3 Firewalls

Firewalls are standards for every Cloud Service Provider (CSP). A usual setup is having an outer firewall, a Demilitarized Zone (DMZ) with web servers and an inner firewall (may be from a different vendor) that protects the applications, databases etc. Of course an Application Service Provider (ASP) could have a much more compli-