Chapter 38
Security Architecture for Cloud Computing

Robin Singh Bhadoria
Indian Institute of Technology Indore, India

ABSTRACT

Clouds need to address three security issues: confidentiality, integrity, and availability. Security architecture for cloud computing is designed based on the functional architecture. The approach is to enhance the components of a functional architecture with additional components providing various security services. This is an extension of SaaS concept to have several security components that are common to all application and services. Various cloud security issues are discussed in this chapter.

INTRODUCTION

The of data can be problematic because of a number of ways it can be achieved since Cloud computing relies on security supported by any Cloud service Provider. As Cloud computing is constantly evolving, new threats are surfacing. An enterprise-wide understanding of the responsibilities, threats and risks should be created to take adequate security measures, establish security organization and instil the security culture. The cloud service provider's (CSP) interface provides access to the logical endpoints, including the security manager, service manager and the service catalog. These endpoints provide various services to interact with service entities such as VMs, volumes, networks, and composite applications, get audit reports and perform a host of other activities required to fulfil and maintain a cloud service requirement.

The two categories of actors interacting with the CSP interface are:

- Users;
- Application programs such as management, automatic provisioning, billing, or audit applications.

The user might also interact through a portal interface using a web browser. The portal interface will be developed using the cloud service provider interfaces. Both actors would be authenticated at the CSP interface by the security manager or present an identity token to the security manager. The following table summarizes the common authentication mechanisms used:

DOI: 10.4018/978-1-5225-5634-3.ch038

Table 1. Authentication techniques

Traditional authentication	"User name" and "Password"
Application program	Certificates or Kerberos tickets
Stronger mechanisms	"Identity Federation" and "assertion provisioning"
Cloud user	Authentication tokens

However, it is deemed insecure to embed user names and passwords in application programs. In this case tokenized identity can be profitably used to provide a higher standard of security.

In case of cloud user appropriate mechanisms may vary in different environments. Trust relationships may be employed to strengthen the authentication and authorization mechanisms. There should be clear business leadership for infrastructure and technology services to set priorities, approve plans, agree investments and monitor progress, as well as to lead the introduction and awareness of new IT infrastructure technology with a specific emphasis on information or data security into cloud services (The ISO 17799 Information Security Portal, 2014).

The Alliance of Cloud Security, a group of industry which promotes the cloud computing security best practices and standards, identified total seven areas of security risk. Five of them directly focus on protecting data and platform i.e.

1. Unauthorized and nefarious use of cloud services;
2. Multitenancy and shared technology issues;
3. Data loss;
4. Account hijacks;
5. Unknown risk.

Several Infrastructure as a Service (IaaS) providers make it easy to take advantage of their services. The requirement is only a valid credit card for user's registration. Once registered, anybody can start using cloud services right away. Exploiters and hackers actively target cloud service providers taking the advantage of their relatively crackable registration system. Since most of the providers have limited fraud-detection capabilities this helps vague identities.

Rigorous initial registration and validation processes, credit card fraud monitoring, and subsequent authentication can be some kind of remedy to heal this type of threat (Trend Micro, Incorporated, 2009).

Clouds deliver countable services which provide computing power for multiple users such as business groups from the same company or independent organizations. That means shared infrastructure-CPU caches, graphics processing units (GPUs), disk partitions, memory, and other components-that was never architected for strong compartmentalization. Even with a Virtualization software to make a user interface for better access between guest operating systems and physical resources, there is problem that attackers can gain unauthorized access and control of underlying platform with software-only isolation mechanisms. Potential compromise of the virtualization software layer can in turn lead to a potential compromise of all the shared physical resources of the server that it controls, which includes memory and data and other virtual machines (VMs) on that server. Experience at Intel found that Virtualization brings with it a log of risks to the enterprise when strong application components and services of varying risk profiles onto a single physical server platform. This is a key limiter faced by most IT organizations