Chapter 65
Cloud Security Using 2-Factor Image Authentication Technique

Ratish Agarwal
UIT-RGPV, India

Anjana Pandey
UIT-RGPV, India

Mahesh Pawar
UIT-RGPV, India

ABSTRACT

Cloud computing is being anticipated as the infrastructural basis of tomorrow's IT industry and continues to be a topic of interest of many new emerging IT firms. Cloud can deliver resources and services to computers and devices through internet. Since Cloud Computing involves outsourcing of sensitive data and critical information the security aspects of cloud need to be dealt carefully. Strong authentication, focusing mainly on user-authentication, acts as a pre-requisite for access control in the cloud environment. In this paper we discuss an efficient authentication mechanism to deal with the security threats that are faced by cloud. The method proposed in this paper prevents the confidential data and information of end users stored in a private cloud from unauthorized access by using a two-factor authentication involving shared image concept in addition with encrypted key authentication.MD5 hashing technique is used which takes binary pixel value of image as input and convert it into a 128-bit hash value. The overall process of authentication has been shown through experimental result and implementation which shows a series of snapshots taken from the chapter.

INTRODUCTION

Cloud computing is a type of computing that uses the internet to allow the sharing of resources and data to other computers and devices as per the demands of clients. This technology provides users and enterprises with various capabilities to store and process their data in third-party data centers. It has become a highly demanded utility as it provides high computing power, cheap cost of services, high

DOI: 10.4018/978-1-5225-8176-5.ch065

performance, scalability, accessibility as well as availability. The technology which is responsible for cloud computing is termed as virtualization, which divides a single physical computing device into multiple "virtual" devices, which are independent of each other and can be used and managed easily for performing computations on different tasks. A cloud can be deployed into three main types Public Cloud, Private Cloud and Hybrid Cloud, according to the types of its user.

There are a number of security concerns associated with cloud computing. These issues fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. The security issues faced by end users can be reduced by using authentication mechanisms at their end. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. Two-factor authentication mechanisms are more robust as compared to traditional password authentication.

- **Cloud Computing:** We will also concentrate on fundamental concepts of Cloud Computing and its related technologies. Computing phenomenon itself, to be considered totally virtualized, must let the computers to be built from physically distributed components like storage, processing, data, and software resources. Technologies like cluster, grid and recently cloud computing, have altogether allowed accessing to huge amounts of computing resources by integrating computing and physical resources in a fully virtualized way and have offered in single system view to the end user. The end users use the computing and physical resources in Utility manner which describes a business framework for delivering the services and computing power on-demand basis. And according to the need of the user, Cloud Service Providers (CSPs) have aimed to deliver the services and cloud users have to pay the service providers based on their usage that means "pay-per-use" or "pay-as-you-go". As we discussed in the previous chapter that in electric grid, the users just use the electricity which is coming from the power stations and users have to pay how much they have used the electricity. Likewise in Cloud Computing environment, users need not to know the underlying architecture for getting the services; they just have to pay according to their usage. Cloud is basically an infrastructure which is maintained by some Cloud Service Providers and end-users are getting the services on-demand from the service provider and they have to pay the required money for their usage. Service Provider giants like Amazon, Microsoft, Google, IBM offer on-demand resource and computing services to the user commercially.
- **Evolution of Cloud Computing:** Cloud computing evolved when we started thinking about what we actually need. Cloud computing is not a new technology. In fact, it is the most used technology whenever we work on our computers. The difference that has occurred now is the way we see and utilize cloud computing. The beginning of what we call the concept of cloud computing can be traced back to the mainframe days of the 1960s when the idea of "Utility Computing" was coined by MIT computer scientist and Turing award winner John McCarthy. He remarked that "Computation may someday be organized as public utility". In 1961, while speaking at the MIT Centennial he suggested.

Utility computing concept is very simple. Utility computing can be defined as a service provisioning model where a service provider makes computing resources and infrastructure management available to the customer as needed. This approach is like pay-per-use or metered service that means customer can pay as their usage for internet service, file sharing, web site access and other applications. In 1966,