Chapter 62
Cloud Security:
Implementing Biometrics to Help Secure the Cloud

Natasha Csicsmann
Pennsylvania State University – Altoona, USA

Patrick Shea
Pennsylvania State University – Altoona, USA

Victoria McIntyre
Pennsylvania State University – Altoona, USA

Syed S. Rizvi
Pennsylvania State University – Altoona, USA

ABSTRACT

Strong authentication and encryption schemes help cloud stakeholders in performing the robust and accurate cloud auditing of a potential service provider. All security-related issues and challenges, therefore, need to be addressed before a ubiquitous adoption of cloud computing. In this chapter, the authors provide an overview of existing biometrics-based security technologies and discuss some of the open research issues that need to be addressed for making biometric technology an effective tool for cloud computing security. Finally, this chapter provides a performance analysis on the use of large-scale biometrics-based authentication systems for different cloud computing platforms.

INTRODUCTION

For decades, businesses had their own way of storing data and information for clients. Today, with technology constantly changing, researchers and computer engineers are developing new ideas to store data and adapting to new ways of doing so. The most recent and popular innovation is cloud computing. Cloud computing was first introduced in the sixties by J.C.R Licklider. In 2006, the term cloud computing was formally established. Cloud computing is a new concept in the technology field and is still being developed and changed. Thousands of people use the cloud to store their personal and public information.

Many people have heard of this term before, but many are not familiar with what the "cloud" actually is. Cloud computing is an infrastructure that uses a network of remote servers hosted on the Internet to store, manage, and process data rather than store it on a local server or personal computer (Das, 2013). This makes it easier and more convenient for clients and other users to access their stored data anytime,

DOI: 10.4018/978-1-5225-0983-7.ch062

anywhere. People can store pictures, music, videos, documents, and other files in the cloud. Many corporations, such as Google, Apple, Microsoft, and IBM have switched from using their local servers to using the cloud (Shaikh & Haider, 2011).

The characteristics of cloud computing include demanding self service, broad-based network access, resource pooling, and rapid elasticity (Stojmenovic, 2012). There are also other advantages of using the cloud for storing information. The cost of cloud computing is significantly cheaper than running local servers because the cost of cloud computing is fixed and predictable. Businesses no longer have to rely on constantly updating from service providers and monitoring infrastructures around the clock. Some companies allow unlimited usage and space for their customers on the cloud. For example, Google has an unlimited free space for Gmail and other services (Čandrlić, 2013). This allows clients and customers to add anything they want.

Although it is an advantage to have everything on the cloud at easy and quick access, this could cause a major security concern. Since the cloud is fairly new, many security measures have not been implemented. If a hacker or a virus infiltrated the cloud and gained access to service provider's networks, a customer's or client's information can be compromised. Not only could unclassified information (music, games, platform applications, or pictures) be stolen, but also classified information, such as government information will be at high risk. If classified information is compromised or the cloud faces a security breach, this could cost the company millions of dollars in damages and could cost the government billions of dollars worth of knowledge, information, and resources. This would be catastrophic to the intelligence community, national security and can cause potential risk and attacks from outside invaders.

In order to help better secure the cloud, sensitive and important information for customers and clients, software engineers and developers need to establish a stronger safeguard against future hackers and viruses from breaking into the cloud. To achieve this goal, biometrics is considered as a promising solution that can be implemented before accessing the cloud.

PROBLEM IDENTIFICATION

There are many concerns associated with cloud computing (Almorsy, Grundy & Ibrahim, 2011). One of the major issues is that the cloud users are not familiar with what the cloud actually is, leaving them making irrational decisions when choosing a service provider. Because the cloud is fairly new, there are several vulnerabilities and faults associated with the system. Large amounts of sensitive data, from PIN numbers to passwords, are submitted across the cloud. Therefore, there must be a solution to increase the security for cloud computing while minimizing the number of vulnerabilities and threats that the cloud currently faces (Hutchings, Smith & James 2013).

A development that would greatly supplement the use of the cloud is biometrics. Biometrics is a system of verification that uses biological identification for access. Some examples include fingerprint scan, retinal scan, facial recognition, or signature. An increasing number of improvements are being made for biometrics, and with that, biometrics is being implemented in a variety of ways. If more users become familiar with cloud computing and learn about the importance of implementing biometrics as a part of a security measure, this system will have an increased level of security with minimal risks and threats.