Chapter 15
Biometrics in Cloud Computing

Mainak Adhikari
IMPS College of Engineering and Technology, India

ABSTRACT

Biometric-based authentication is automatic identity verification, based on individual physiological or behavioural characteristics, such as fingerprints, voice, face, iris, etc. Over the next few years, the amount of biological data will increase rapidly and require enormous amounts of storage space and huge processing power. To face those challenges, the Service Providers are looking towards a distributed approach, Cloud Computing, which can improve the Quality of Service (QoS) of overall systems and handle the challenges quite efficiently with its unlimited storage space, and parallel processing power, using the help of virtualization technology and rapid data distribution capacity. This chapter presents the important standards and recommendation of Biometric Services in Cloud Platform and elaborates the potential value of Cloud-Based Biometric Services by presenting two important case studies.

INTRODUCTION

Authentication is the act of confirming the truth of attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artefact or ensuring that a product is what it's packaging and labelling claim to be. In case of authenticated people still use what he/she has (email-id, ph. No., ATM), what he/she knows (password, PIN) and he/she is (Face, Iris). Nevertheless, the main problem of these approaches is that each user may have more than one account, and each account has a unique password, which may be forgettable by the user, or different users may use same username and password for the multiple sites. To achieve verification that is more reliable or identification a possible solution can be found in the use of Biometrics.

The term Biometrics comes from Greek words "Bio" means "life and "Metric" means "to measure". Biometrics is the science and technology of measuring and analysing biological data. Biometric-based authentication is an automated method for recognizing individuals based on measurable biological and behavioural characteristics. To determine or verify a person, biometric identification system uses physiological characteristics (Face, Hand Geometry, Iris, retina recognition) or behavioural characteristics (Voice, Keystroke on keyboard, digital Signature) of the person. Since biometric is not possible to forge and it cannot be forgotten or stolen by anyone. Biometric authentication offers a convenient, accurate,

DOI: 10.4018/978-1-5225-0983-7.ch015

irreplaceable and high secure alternative for an individual, which makes it, has advantages over traditional cryptography-based authentication schemes. Biometric data is the private information, which has no need to be remembered all the time and cannot be replaced like password. Biometric information is uniquely and permanently associated with a person. A biometric system can be either an 'identification' system or a 'verification' (authentication) system. The main issue of Biometric technology is to handle huge amount of biological data, which, required sufficient storage space and significant processing power in the system.

The main solution is to move the existing Biometric technology to a Cloud platform that ensure appropriate scalability, sufficient amount of storage, use virtualization, parallel processing capabilities and widespread availability of devices that provides an accessible entry point for various applications and services that rely on the three types of clients- Thin clients, Thick clients and Mobile clients. Hence, Cloud computing is capable of addressing issues related to the Biometric technology, but at the same time, offers new application possibilities for the existing generation of Biometric systems.

However, Biometric technology in Cloud is a nontrivial task. Developer attempt to tackle this task must be aware of the following challenges:

1. The most common challenges and obstacles encountered when moving the technology to a Cloud platform.
2. Standard and recommendations pertaining to both Cloud-based services as well as Biometrics in general.
3. Existing solutions that can be analysed for examples of good practices.

This chapter provides some basic guidelines on how to move the Biometric technology in Cloud platform. This chapter also describe some basic about Biometric technology and Cloud computing. Additionally it presents two case studies on some important Biometric technologies in the Cloud platform. Sufficient references are given for the benefit of readers.

BIOMETRIC SERVICE

Biometric recognition systems represent pattern recognition systems, capable of recognizing individuals based on their physiological or behavioural traits. These traits are considered to be unique to each individual and unlike knowledge or token-based security mechanisms cannot be forgotten, lost or stolen. Biometric system is categorising into two parts: Identification system and Verification ('Authentication') system.

- **Identification:** One to Many: Biometric system can be used to identify a person without his/her knowledge or consent about the data. For example, scanning a crowd with a camera using face recognition technology, one can identify a person using a known database.
- **Verification:** One to One: Biometrics can also be used to verify the identity of a person. For example, one can grant to access a secure area of a building by using the finger scans or one can grant to access a bank account at an ATM by using retinal scan method.

Biometric authentication requires a registered or enrolled Biometric sample, which is stored in a database, which will be compared with a newly captured Biometric sample (Balfanz et al. 2012). Dur-