Chapter 42
Biometric:
Authentication and Service to Cloud

Ajay Rawat
University of Petroleum and Energy Studies, India

Shivani Gambhir
University of Petroleum and Energy Studies, India

ABSTRACT

Cloud computing lacks control over physical and logical aspects of the system, which imposes profound changes in security and privacy procedure; hence, it needs a high level of security. Currently, many researchers and developments are being done to provide client service-level agreements regarding security issues. These researchers are attracted towards biometrics and its security applications, since it is based on biometric traits, thus providing a high level of security. Due to biometrics' benefits and cloud advantages, the collaboration of cloud and biometrics have open up wide areas this field. This chapter discusses some case studies of integration of biometrics and cloud computing.

BIOMETRICS AND ITS WORK PROCESS

The word '*Biometrics*' is derived from Greek word '*Bio*' means life and '*Metrikos*' means measure. Thus, identification of humans through their characteristics and traits is referred as biometrics. It is used in the area where authentication of individual or to have supervision upon individuals in a group. Each and every individual have unique biometric characteristic which cannot be forgotten, stolen or lost. But in token based or knowledge based security mechanism there are chances that it can be lost or stolen. The following the most commonly used biometric authentication and recognition trait: faces, fingerprints, irises, palm-prints, speech etc.

Biometrics system is essentially a pattern recognition system. In spite of the design being used to deploy biometric system it contains four basic components.

- **Sensor Module:** It is a data procuring module (or sensor) that captures image and/or video sequences of an individual who is either registering into the biometric system or using it for verification/identification purposes.

DOI: 10.4018/978-1-5225-7501-6.ch042

- **Feature Module:** It is a template generation module which develops a biometric template pattern from the input data using machine learning, computer vision and pattern recognition techniques.
- **System Database Module:** It is a repository of registered/enrolled biometric patterns of users.
- **Matcher Module:** It is a matching module which compares the biometric pattern of 'live' image of the users to the respective biometric patterns stored in the System Database Module. Based on the matching results, it makes a decision with respect to the identity of the current user presented to the system.

It provides two functions i.e. identification and authentication/verification.

In *Identification process,* system identifies the individual by the matching it with all the templates available in the biometric database. While performing this operation it does one-to-many comparisons to ascertain the identity of an unknown individual. If the comparison of the biometric sample to actual template matches with the database; identifying of individual is succeed. The system will fail is the individual is not enrolled in the system database. Identification process is significant element in both in 'positive recognition' and 'negative recognition'. In positive recognition user does not have to provide any information about the template to claim its identity, and in 'negative recognition' is used to obstruct a single user form multiple identities. The tradition methods such as PIN, key, tokens can be used in former approach. The latter approach can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

In *verification* process, system performs comparison of his captured biometric characteristics sample with the registered templates stored in a biometric database. There are three steps involved in person verification.

Step 1: During this process, biometric templates are captured using sensing devices that generate reference models for all users and stores in model database.

Step 2: To generate the genuine and impostor scores, some samples are matched with reference model and thus calculate threshold.

Step 3: In this step biometric template testing is accomplish. It is done to indicate which template should be used for either comparison of smart card, username or ID number (e.g. PIN). 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity".

WHY BIOMETRIC IS SECURE?

- **Unique:** The biometrics systems are developed upon traits of each individual. Thus, there is virtually nil probability that two individuals have same biometric pattern, hence providing the uniqueness of data in database.
- **Cannot Be Shared:** It is extremely difficult to duplicate or share these properties as biometric properties are inborn feature of an individual. Hence, it cannot be shared by anyone.
- **Cannot Be Copied:** It is impossible to spoof the biometric characteristics even with new technologies, safeguarding that the biometric identified is from a live person.
- **Cannot Be Lost:** Even in case of serious accident, biometric property which people possess cannot be lost.