Chapter 44
Trusted Cloud- and Femtocell-Based Biometric Authentication for Mobile Networks

Debashis De
West Bengal University of Technology, India

Anwesha Mukherjee
West Bengal University of Technology, India

Srimoyee Bhattacherjee
West Bengal University of Technology, India

Payel Gupta
West Bengal University of Technology, India

ABSTRACT

Authentication procedures are conducted in order to control and stop illegitimate access of such valuable data. This chapter discusses the biometric authentication inside the cloud. The authors describe how biometric information of a user can be securely transmitted and then stored inside the user database maintained in the trusted cloud. Femtocell, a recent development in mobile network using which secures biometric data transmission from the mobile device to the cloud, is discussed in this chapter.

INTRODUCTION

Frauds and fraudulent activities are social crimes that are increasing vigorously every day. They are million dollar businesses escalating every year. The PwC global economic crime survey of 2009 suggests that close to 30% of companies worldwide have reported being victims of fraud in the past year (PricewaterhouseCoopers LLP, 2009). The Oxford Dictionary defines fraud as the use of false representations to gain an unjust advantage. It involves people who purposely act in a secret manner to deprive someone from something of value which actually belongs to the victim.

DOI: 10.4018/978-1-5225-8176-5.ch044

Statistics says that in recent years, the development of new technologies has provided new avenues to criminals in which fraud can be committed (Bolton, 2002). With the maximum items of our daily lives gone electronic, the scope of performing such crimes has found a strong platform. Credit / debit card fraud, electronic fraud, identity theft etc. are few of the types of fraud that are encountered regularly. To combat such deceptive activities, it is very important to implement authentication techniques. It is the act of confirming the truth of an attribute of a datum or entity which might involve confirming the identity of a person or some software program. The process of authentication often involves verifying the validity of at least one form of identification which is unique in nature. Biometric authentication is an important authentication method which refers to the identification of humans by their characteristics or traits. In Computer Science, it is used for identification and secured access control. Different aspects of human physiology, chemistry or behavior are used for biometric authentication. Biometrics refers to the use of unique physiological characteristics to identify an individual. It uses human traits like finger prints, tongue impressions, iris and face recognitions (Pugazhenthi, 2013). These are unique to each individual and thus differentiate users. A human physiological or behavioral biometric should possess the following desirable properties (Jain, 1999):

1. **Universality:** Every person should possess the characteristic;
2. **Uniqueness:** No two persons should be the same in terms of the characteristic;
3. **Permanence:** The characteristic should not vary with time;
4. **Collectability:** The characteristic should be measurable quantitatively.

Biometric techniques and cloud computing are combined for the purpose of a secure cloud computation. As cloud is nothing but a remote server, hence, the operations carried out are beyond trusted boundaries and is much more vulnerable to hacking and security breaches (Pugazhenthi, 2013).

As we all know, worldwide adoption of mobile products and cloud computing services is not only continuing, but is accelerating. Biometric security technology seems promising inaddressing the issue of authenticating genuine user that is a fundamental flaw inconventional cryptography. Conventional biometric applications, specifically verification and identification, have been extensively investigated over the past decades,leading to a significant improvement.

BIOMETRIC AUTHENTICATION IN CLOUD ENVIRONMENT

Cloud computing is a promising field in the world of technology. It provides cost effective secure framework and allows software, platforms and infrastructures to be used as a service (Li-qin, 2010). Securing user privacy and data or application from frauds is a task of concern for the cloud service providers. Biometric based authentication is dependent on analyses of human characteristics or traits. It is used for user identification and access control (Wang, 2014). Implementation of biometric based authentication in cloud based storage and at the client end would provide immunity against security attacks (Li-qin, 2010). For enabling biometric authentication in the cloud, the biometric infrastructure including the databases, network connectivity and all the processing required for the authentication must be available to the cloud. Biometric infrastructures are characterized by ease of set up, affordability, scalability and on-demand service provisioning (Armbrust, 2010).