Abstract

Biometric technology has been successfully applied to solve automatic user identification and verification problems. Of late, there is a trend to apply biometric traits of a user in cryptography for data storage security, secure message communication through an insecure network channels and user authentication in a distributed environment. This dissertation attempts to explore the possibilities of the aforementioned applications. More specifically, this thesis aims three objectives: to secure a users' remote data storage, to authenticate a user for a secure access to services and group authentication in a multiparty system.

We propose biometric-based cryptographic mechanism (we call it *BioKEY*) to protect users' data. In *BioKEY*, we consider a fingerprint biometric data of a user from which we extract statistical features. These feature vectors are then used to generate a cryptographic key. We encrypt user's data with this cryptographic key. Ciphertexts are stored as a combination of encrypted text and a codeword. Codeword is a secret piece of component to encode the user's biometric data. We propose the codeword generation using Reed-Solomon coding scheme. Prior to the decryption, a user is validated with a newly captured feature and the codeword. For the verification, we propose SVM ranking mechanism. A successful verification follows the regeneration of cryptographic key from the codeword and hence the decryption.

In our second work, we develop a user authentication scheme (we call it as *BioCAP*) for a secure access to Cloud services located in remote locations. In *BioCAP*, we derive a unique and revocable user identity from a user's biometric data, which is used to generate user's private key and session keys. These keys are used for a secure message transmission and access to services remotely. Further, with the proposed session key, we lay down an approach to mutually authenticate two communicating parties for a secure communication.

Our third work is to address the issues and challenges to develop a multy-party authentication system (we call our proposed approach as *BioMAS*). In this work, we investigate the generation of group permits for each user belongs to a group using his biometric data. A member can access the system using his fingerprint data as a secret credential. A number of issues in the multiparty authentication system namely adding a new member, revoking a member, revocable member id generation, etc. have been addressed in this work.

Keywords: *Bio-Crypto System, Remote Data Storage Security, Cloud Service Security, Authentication Protocol, Multi-party Authentication*