ABSTRACT

Wireless Local Area Networks are becoming more and more popular as they are fast, cost effective, flexible and easy to use. Networks carry the risk of security in transmitting information. There are several users in the networks who access networks remotely, transmit data through internet. Hence, providing security to the users of the network becomes a primary concern.

There are various techniques available in the literatures which make use of passwords, smart cards and so on, to provide network related security. But these conventional authentication systems have several limitations such as unreliability, vulnerability to attacks, stealing of passwords and so on. Thus, a novel authentication system becomes relevant to circumvent the above mentioned drawbacks. Biometrics is the technique of evaluating and statistically analyzing biological data that can be used to recognize various biometric features. Biometric features like fingerprint, retina and iris are used to provide security to the network users. These biometric features are more reliable when compared to the traditional methods. Thus, the biometrics based authentication system provides better security and authentication.

Bio-cryptosystems are seen to produce better authentication and security to the network users. This technique integrates the unique characteristic features of both biometrics and cryptography and has the advantages of both the technologies. Hence, this research proposes an approach for network security using a novel bio-cryptosystem technique for personal authentication, where a combination of biometric features like
fingerprint, iris and retina are used for authentication. This novel key authentication protocol is found to provide better security to the users. This key authentication protocol is integrated with the biometric features like fingerprint, iris and retina.

The first proposed approach uses the fingerprint biometric features and key authentication protocol. This approach uses an image processing approach to extract the biometric measurement called “minutiae” from the user’s fingerprint. The fingerprint image of the user is converted and stored as encrypted binary template, which is used for authentication by the server of the network. Then, Lipmaa’s PIR Authentication Protocol is incorporated into the feature points of the fingerprint.

The second proposed approach uses the iris and retina biometric features which are observed to provide better results than the fingerprint biometric features. The different phases included in the iris based approach are user registration, extraction of minutiae points and secret key, iris localization and normalization. The implementation of the proposed approach is through the operations such as transformation, encoding and finally decoding. A user applies a password in this stage for the encoding and decoding purposes which provides revocability which is absent in the fingerprint based authentication system. Then, the Iris authentication protocol is used in this approach for enhancing the biometric authentication security.

Retina biometric feature is also used in this research which is observed to provide better security when compared with the fingerprint and iris biometric features. The same process carried out for iris biometric feature extraction is used in this process. In order to enhance the performance and security in the biometric authentication
system, multimodal biometric is used in this research. The above mentioned biometric features are combined using multi-modal biometric techniques and are used for authentication purposes.

Feature level fusion is used in this approach which refers to combining different feature sets that are extracted from multiple biometric sources. Multi-modal biometrics provides better security and authentication. In this proposed technique, fingerprint-iris, fingerprint-retina and retina-iris are used as the multi-modal biometrics features. Using the feature level fusion technique, the two biometric features like fingerprint and iris are fused to obtain a single feature points. Then this feature points is given to the mapping function and authentication protocol as described earlier.