Chapter 7
CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1. CONCLUSION

A Wireless Body Area Network (WBAN) is the network of low-powered, short-ranged devices for measuring and monitoring physiological parameters such as Electrocardiogram (ECG), Blood Pressure, Electromyography (EMG) etc. These devices could be wearable or could be implanted inside the body that communicates wirelessly to a monitoring station known as the Base Station. Body Area Networks, predominantly in the field of individual health monitoring, are emerging as one of the major research areas. In view of the fact that health data are secretive and sensitive, the security of data transmission inside a BAN turns out to be a significant issue that needs utmost attention. This piece of research proposed novel cryptographic algorithms for the secured data transmission in the BANs.

In the first phase of the research work, Elliptic Curve-based Signcryption method proposed for safe and authenticated message delivery, which fulfils the functions of digital signature and encryption simultaneously. This method’s cost requirement is below that of the standard signature-then-encryption method. And also the fuzzy ontology is used for improving the semantic interoperability. The authentication procedure and group key generation are very simple and efficient.

In the second phase of the research work, Attribute-based Ring Signcryption Scheme (ARSS) is tested. The patient’s dataset is pre-processed using Independent Component Analysis (ICA). Then interoperability among body area sensor networks is tested with Ant Colony Optimization based Fuzzy Ontology (ACO-FO). Then the proposed ARSS is simultaneously provides the attributes of message confidentiality, authentication, integrity, unforgeability, non-repudiation, public verifiability, and forward secrecy of message confidentiality.

In the third phase of the research, the proposed versatile cryptosystem was submitted to Cipher Text-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS) in order to ensure the much needed security for the BANs. The initial process of proposed
system is pre-processed the patient’s dataset using Enhanced Independent Component Analysis (EICA). Then ACO-FO is used to improve the interoperability of BAN system. A CP-HARS scheme is constructed with short cipher texts. The scheme is proven to have security in the standard model under non-interactive assumptions. In this subsection, the security strength of the proposed scheme is analyzed by examining how it can counter possible major attacks.

Compared with the previous works in BANs, proposed method has attained only lesser computational and communication cost for the authentication and key derivation. The studies conducted showed that the novel scheme is light in weight and energy efficient too. And a detailed discussion on privacy and security aspects needed for health care applications was also provided.

The experimental output provided unforgeability, authenticity, non-repudiation and confidentiality to achieve higher security, lower energy consumption, lesser computational cost and communication overhead.

7.2. FUTURE WORK

Innovative health-oriented networking and wireless communication technologies have become an intrinsic part of many modern medical services. Body Area Networking is a key enabler and technique for e-healthcare systems. This will make real-time health-related information accessible to medical specialists, who are then enabled to cast appropriate and timely medical treatment to the patients. A BAN deals with more sensitive and important patient information that has significant security, privacy, and safety concerns, which may prevent the wide adoption of this technology. Our analysis indicates that the proposed scheme is feasible, can provide message authenticity, and can counter possible major attacks such as collusion attacks and battery-draining attacks.

To overcome the challenges, this research work resorted to the Ciphertext-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS), which was proposed as a new means of providing role-based access control on encrypted data. The future works in this domain shall contribute to the designing of efficient signcryption schemes to achieve reduced storage costs, meet the design necessities of the BANs and computational cost. Based on attribute encryption and a lightweight signcryption scheme, the designing of
efficient signcryption approach to meet the stringent security concerns is the prime consideration. Our future research lies in the following direction: design a more efficient encryption approach with less computational and storage requirement, which could be better suitable for practical BAN applications.