

Security and Privacy Issues in IoT Devices and Sensor Networks




Advances in ubiquitous sensing applications for healthcare

2021, Pages 43-59

Chapter 3 - Security and privacy in wireless body sensor networks using lightweight cryptography scheme

A.Sivasangari^aA.Ananthi^aD.Deepa^aG.Rajesh^bX.Mercilin Raajini^c

Show more 

 Outline |  Share  Cite

<https://doi.org/10.1016/B978-0-12-821255-4.00003-1>

[Get rights and content](#)

Abstract

Security and privacy must be ensured for WBAN. Various key management and distribution schemes are developed to provide the security in WBAN. The key distribution methods distribute the keys for secure communication in WBAN. However, these methods are not suitable for the body sensors, owing to the limited sensor resources. The proposed chapter introduces the wavelet transform a frequency time domain technique for separating pertinent signals, and these signals will be compressed by the lossless compression algorithm. Thus the compressed data will be encrypted using proposed SPECG encryption algorithm. Attribute-based encryption is applied for secure data access in cloud for accessing the medical data. Security and privacy are maintained in three levels of communication. The proposed algorithm is evaluated in terms of false acceptance rate (FAR), false rejection rate (FRR), and half total error rate (HTER). The system is evaluated with varying level of tolerance. The simulation results show that the proposed work is secured than the existing system. Analysis of the experimental results leads to the conclusion that the proposed work requires the least time for carrying out encryption compared with any other algorithms.