BAES Token in Wireless Body Area Network for Real Time Healthcare Ecosystem

Reza Khalilian[1], Abdalhossein Rezai*[2], Farhad Mesrinejad[3]

[1] Department Electrical and Computer Engineering, Islamic Azad University of Majlesi Isfahan, Iran

[2] Department of Electrical Engineering, Unicersity of Science and Culture, Tehran, Iran

[3] Department of Communication Engineering, Islamic Azad University of Majlesi, Isfahan, Iran

Abstract:

Wireless Body Area Network (WBAN) is an important kind of wireless networks that has many applications such as telemedicine and monitoring healthcare. Hence, the secure communication is very important issue in this network. A common used method for secure communication is encryption. Symmetric encryption systems are one of the most widely used encryption systems that used to secure communication. Researchers have used Data Encryption Standard (DES), 3-DES, Advanced Encryption Standard (AES) to improve security. In this chapter, implementation of a security system for the WBAN is presented. The developed security system is Biosignal AES (BAES), which is hybride of biosignal encryption and AES-256 with a new key management scheme. In the implemented method, a random function is used to generate varible output from fixed input. In the first step of implementation, the C# program is used to evalute the operation of the security system. In the next step, the BAES is implemented in AVR especially for Real Time WBAN in Ubiquitous Telemedicine system. In addition, simulation results in MATLAB are presented and compared. The results demonestrate that this method has many advantages compared to other methods.

K W: WBANs, Cyber Space, Coding and Information Theory, Prevention Cybernetic Attacks, Energy Efficiency, Encryption and Decryption Algorithms (BAES), Media Access Control (MAC), Message Authentication Code (MAC), SecurityInformation Security Management System (ISMS).