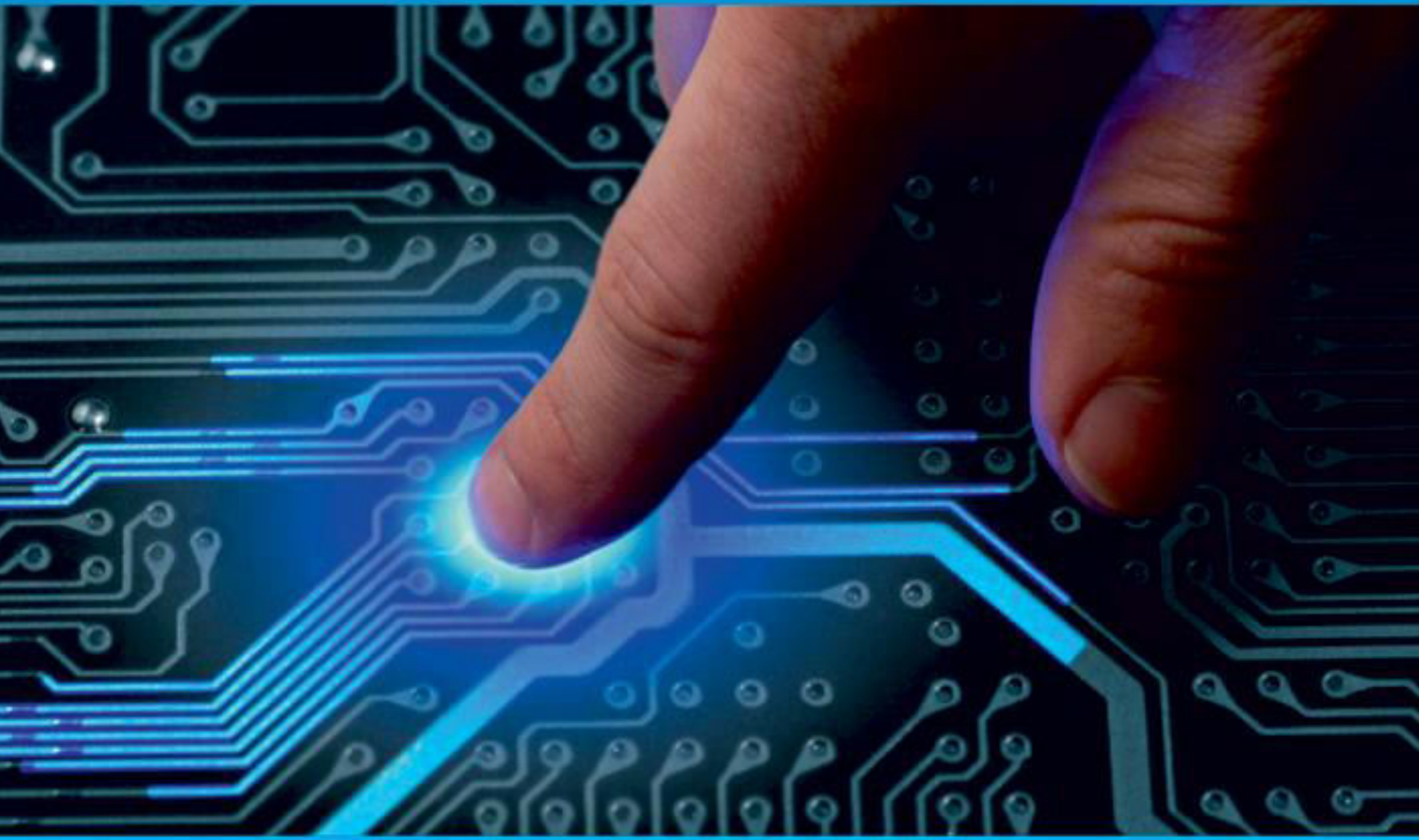
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006081 |

Secured Health Monitoring System Using AES

Dr. M. V. Karthikeyan, D. S. Sandhiya, M. Shanmuga Priya

Department of Electronics and Communication Engineering, St. Joseph's Institute of Technology, Chennai, India

UG Student, Department of Electronics and Communication Engineering, St. Joseph's Institute of Technology, Chennai, India

UG Student, Department of Electronics and Communication Engineering, St. Joseph's Institute of Technology, Chennai, India

ABSTRACT: Wireless medical sensor network is used in healthcare applications that have the collections of biosensors connected to a human body or emergency care unit to monitor the patient's physiological vital status. The real-time medical data collected using wearable medical sensors are transmitted to a diagnostic centre. The data generated from the sensors are aggregated at this centre and transmitted further to the doctor's personal digital assistant for diagnosis. The unauthorised access of one's health data may lead to misuse and legal complications while unreliable data transmission or storage may lead to life threatening risk to patients. So, this system uses Advanced Encryption Standard (AES) algorithm to encrypt the data to make it secured transmission and access control system for medical sensor network. Further the data is sent to a centralised server through a wireless network. In this case this server can be a Personal Computer (PC) connected to the same network, for this transmission User Datagram Protocol (UDP) can be used. This data can be accessed at the receiver side only.

KEYWORDS: Advanced encryption standard algorithm; healthcare applications; program microcontrollers

I. INTRODUCTION

The recent progress in WSNs has given rise to its numerous application areas in healthcare. It has created a new field of Wireless Medical Sensor Networks(WMSNs). Using any of the wearable and non-wearable biosensor devices, human health can be tracked and monitored. The data collected through biosensors are transmitted over wireless network to the diagnostic center. The transmission of health data through wireless networks is susceptible to attacks. During transmission, the person's data may be misused by others and it may create a danger to the person's life. Therefore, security is a principal requirement of healthcare applications.

This system collects the data and encrypts the data using AES, this process makes the data transmission very secure. Further the data is sent to a centralised server through a wireless network. In this case this server can be a PC connected to the same network, for this transmission UDP protocol can be used.

II. RELATED WORK

In recent years mostly all the health centers and hospitals use the wireless networks and internet for biomedical information exchanging, the secure of this information in not verified and cannot be grantee in such environment, the personality of patient and for security concerns inside such institutions there is a need for encryption system that can easily encrypt the biomedical data and it can be shared with other centers via internet without and concerns about privacy. Our system based on modified advanced encryption standard (AES), with encryption and decryption in real time taking to consideration the criticality of data that been encrypted. This scheme is composed of algorithms that authenticate and measure the trust level of devices in three situations, i.e., when only LT (local trust) level, or only GT(global trust), or both levels are used for the trust measurement, and has been partially used for the construction of our trust mechanism. However, the development of a trust scheme for the D2D m-health environment has not been considered. It also involves local data collecting system.

III. ALGORITHM USED

Advanced encryption standard (AES) is consider one of the popular block ciphers worldwide, many attacks is formed in AES, none of these attacks can totally cryptanalysis this algorithm, the modification suggested to this algorithm goal is to improve the security offered by it and add randomness to original algorithm. It is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

AES instruction set is now integrated into the CPU (offers throughput of several GB/s)to improve the speed and security of applications that use AES for encryption and decryption. Even though its been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.

IV. PROPOSED SYSTEM

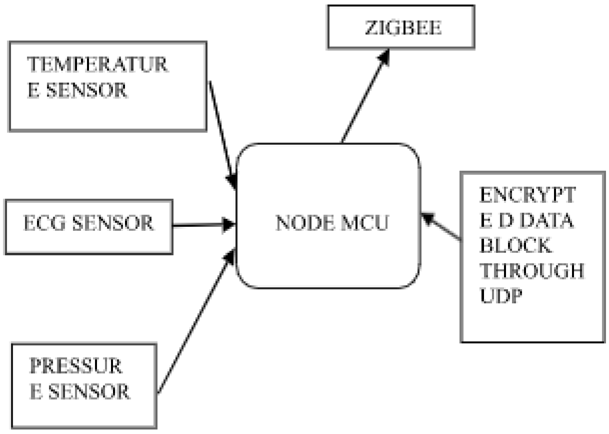


Fig 3.1 Block diagram of Transmitter

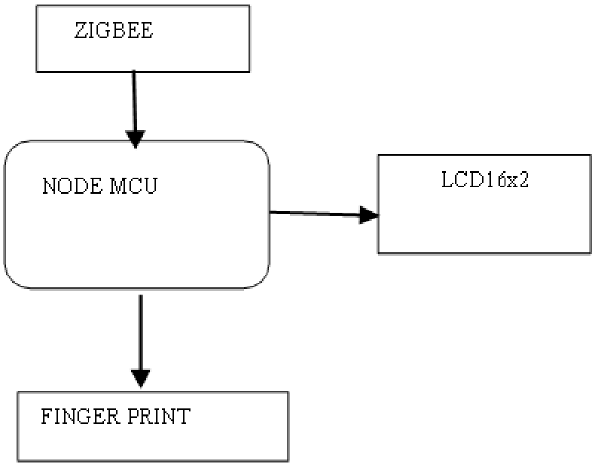


Fig 3.2 Block diagram of Receiver

IV. CONCLUSION AND RESULT

As an outcome of the pursued research work, the real time secured health monitoring system is depicted in this thesis. This prototype of Real time secured health monitoring system was designed and built to monitor the people's health wirelessly at any time and make precautionary measures to avoid death or illness. The wearable technology is implemented with this system for the people to feel comfortable without any add-ons to there daily wear that would not make them feel conscious. A trust evaluation indicated the close devices suitable for the relay of data to guarantee the delivery of data from the source device to the health center. The protocol has proven the safest, because it has fulfilled

| DOI: 10.15680/IJIRCCE.2022.1006081 |

all security objectives and achieved better performance. Therefore, no intruder can discover confidential and critical parameters and information.

Thus, the data generated from the sensors are aggregated at this centre. The transmitted encrypted data is received and using authentication factor the data is decrypted in secured manner.

REFERENCES

1. Dr. M V Karthikeyan.: 'Secure IR Communication Design for pre-cardiac arrest detection in wireless body area network'
2. Dr. M V Karthikeyan., J Manickam.: 'ECG-signal based secret key generation (ESKG) scheme for WBAN and hardware implementation', Wireless Personal Communications., 106 (4), 2037-2052.
3. Wang H., Peng D., Wang W., et al.: 'Resource- aware secure ECG healthcare monitoring through body sensor networks', *IEEE Wirel. Commun.*, 2010, 17, (1), pp. 12–19.
4. Alemdar H., Ersoy C.: 'Wireless sensor networks for healthcare: a survey', *Comput. Netw.*, 2010, 54, pp. 2688–2710.
5. Knight PH, Maheshwari N, Hussain J, Scholl M, Hughes M, Papadimos TJ, et al. Complications during intrahospital transport of critically ill patients: Focus on risk identification and prevention. *Int J Crit Illn Ini Sci*. 2015; 5:256-64.
6. He D., Chan S., Tang S.: 'A novel and lightweight system to secure wireless medical sensor networks', *IEEE J. Biomed. Health Inf.*, 2014, 18, (1), pp. 23–32.
7. Alonso J.V., Matencio P.L., Castano F.J.G., et al.: 'Ambient intelligence systems for personalized sport training', *Sensors*, 2010, 10, pp. 2359–2385.
8. Kumar P., Lee H.J.: 'Security issues in healthcare applications using wireless medical sensor networks: a survey', *Sensors*, 2012, 12, (1), pp. 55–91.

BIOGRAPHY

Dr. M V Karthikeyan is an Assistant Professor in the Electronics and Communication Engineering Department, St.Joseph's Institute of Technology, Chennai. He received his doctrate (Ph.D) in Information and Communication in 2020 from Anna University, Chennai, TamilNadu, India. His research interests are medical devices, Cybersecurity.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ✆ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details