East Asian Journal of Multidisciplinary Research (EAJMR)
Vol. 1, No. 6, 2022: 1175-1182

Secured Health Monitoring System Using AES

D. S. Sandhiya[1], M. V. Karthikeyan[2], M. Shanmuga Priya[3]
Electronics and CommunicationEngineering, 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 careunit 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. Furtherthe 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 : Health, Monitoring System, AES.

Submitted: ***02-07-2022****; Revised:* ***20-07-2022****; Accepted:* ***26-07-2022***

***Corresponding Author** : sruthimurugavel3111@gmail.com

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 andnon-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 casethis server can be a PC connected to the same network, for this transmission UDP protocol can be used.

RELATED WORKS

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, oronly 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.

PROPOSED SYSTEM

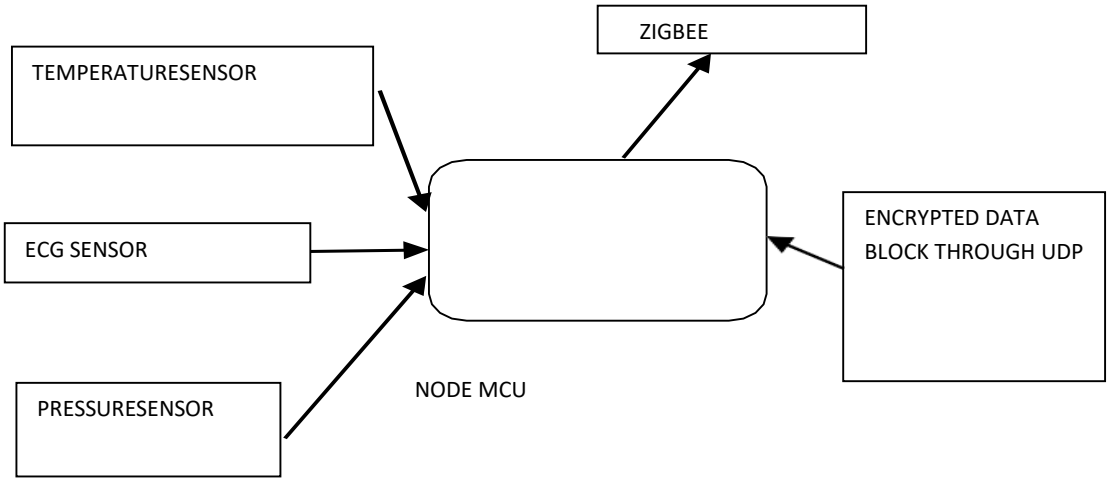


Figure 3.1 Block diagram of Transmitter

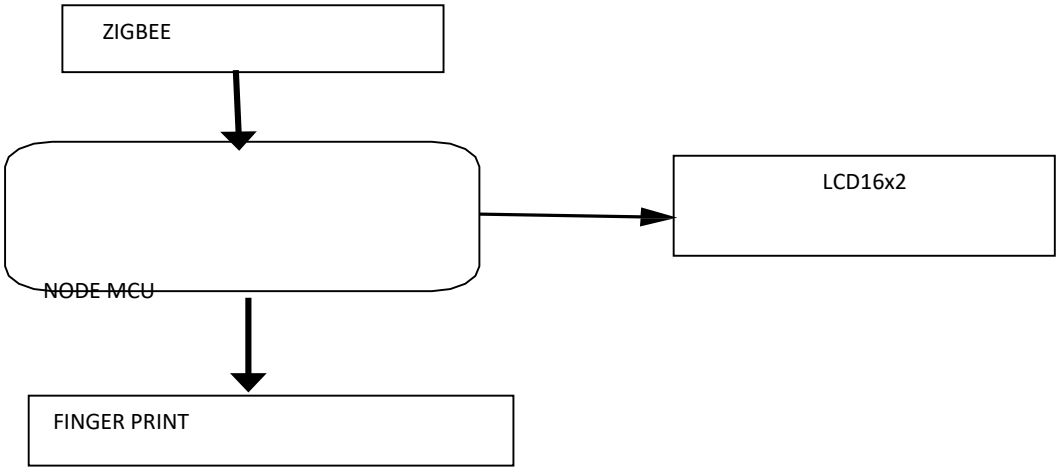


Figure 3.2 Block diagram of Receiver

ALGORITHM USED

Advanced encryption standard (AES) is considerone of the popular block ciphers worldwide, many attacksis 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 Instituteof Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES andtriple 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.

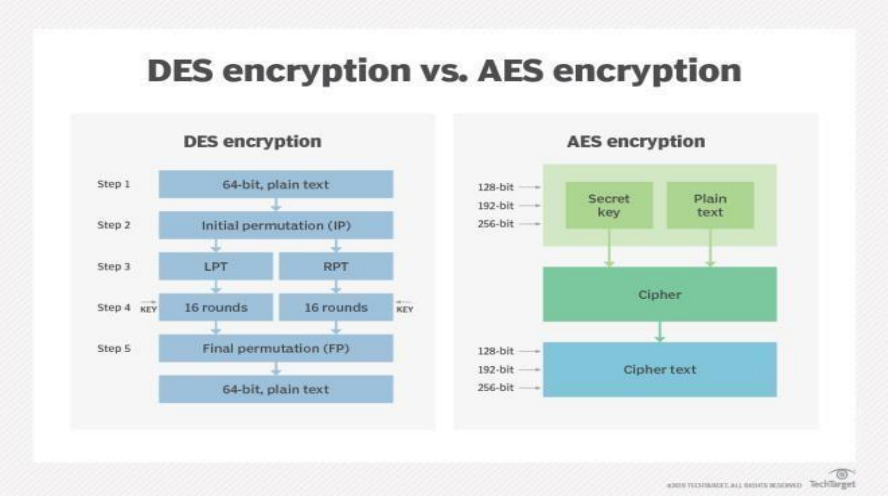


Figure 4.1 DES and AES encryption

HARDWARE REQUIREMWNTS

Node MCU

The Node MCU is a tiny and inexpensive Wi-Fi microcontroller, designed specifically for IOT projects. It can be programmed software, and it's the ideal platform for anyone interested in exploring the Internet of Things.

The ESP8266 chip uses a unique combination of capabilities: It is a Wi-Fi controller that can be programmed in the same way you program microcontrollers. It can connect directly to the Internet without needing a router or other intermediary device, soit has the potential to reduce in-home wiring requirements. And its small size and power consumptionmake it ideal for use in smart objects like sensors, actuators, and just about any type of electronics project you can imagine.

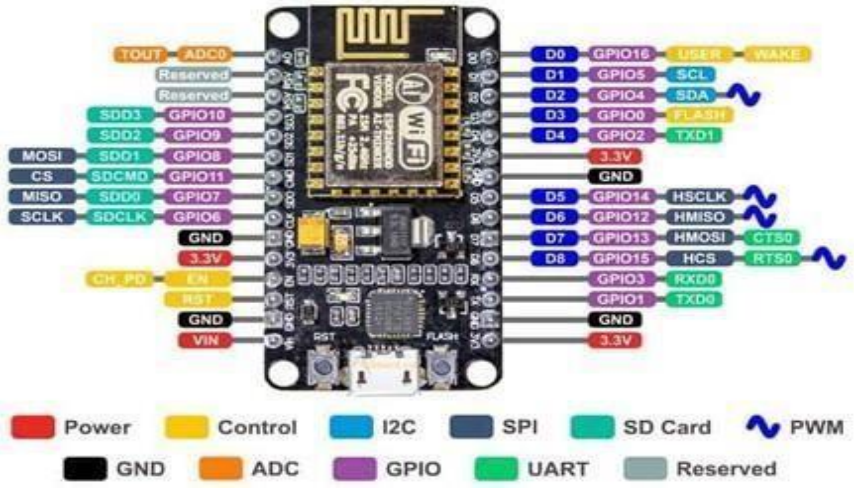


Figure 5.1 NodeMCU

Zigbee Module

The XBee/XBee-PRO RF Modules aredesigned to operate within the ZigBee protocol and support the unique needs of low-cost, low-power wireless sensor networks. The modules require minimal power and provide reliable delivery of data between remote devices.

The XBee/XBee-PRO ZB firmware release can be installed on XBee modules. This firmware is compatible with the ZigBee 2007 specification, while theZNet 2.5 firmware is based on Ember's proprietary "designed for ZigBee" mesh stack (EmberZNet 2.5). ZB and ZNet 2.5 firmware are similar in nature, but not over-the-air compatible. Devices running ZNet 2.5 firmware cannot talk to devices running the ZB firmware. It uses point-to-point and point-to-multipoint network topology. It is Self-routing, self-heating and fault-tolerant.

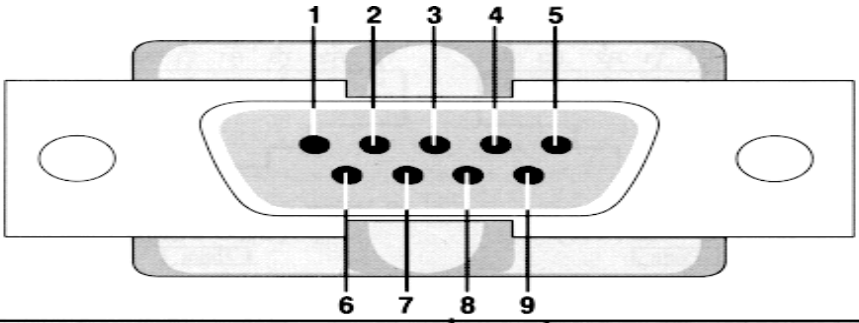
RF Module Operation

Data enters the module UART through the DIN (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted. Each data byte consists of a start bit (low), 8 data bits (least significantbit first) and a stop bit (high).

The module UART performs tasks, such as timing andparity checking, that are needed for data communications. Serial communications depend on the two UARTs to be configured with compatible settings.One of the advantages of a serial system is that it lends itself to transmission over telephone lines. The serial digital data can be converted by modem, placed onto a standard voice-grade telephone line.

It can also be converted back to serial digital data at the receiving end of the line by another modem. Officially, RS-232 is defined as the "Interface between data terminal equipment and data communications equipment using serial binary data exchange."

This definition defines data terminal equipment (DTE) as the computer, while data communications equipment (DCE) is the modem. A modem cable has pin-to-pin connections, and isdesigned to connect a DTE device to a DCE device. However, many interface products are not data communications equipment (DCE). Null modem cables are designed for this situation; rather than having the pin-to-pin connections of modem cables, null modem cables have different internal wiring to allow DTE devices to communicate with one another.



Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		

Figure 5.2 RF Module interference

RESULT

A trust evaluation indicated the close devices suitable for the relay of data to guarantee the delivery ofdata from the source device to the health center. The protocol has proven the safest, because it has fulfilled allsecurity 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.

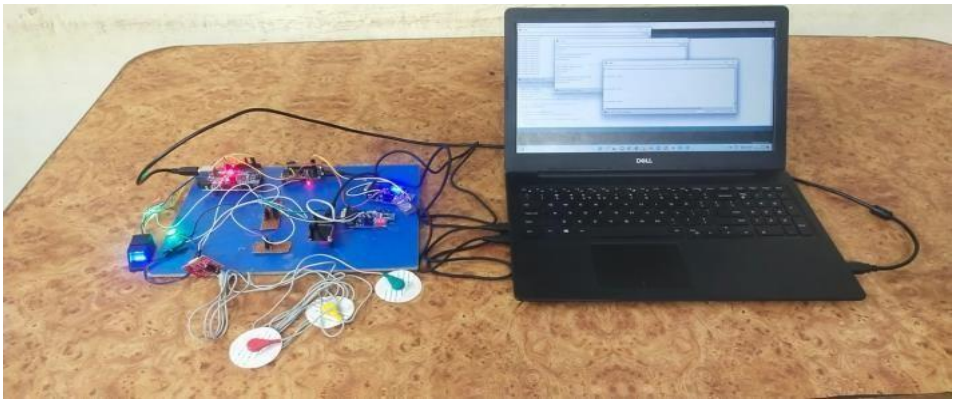


Figure 6.1 Output Response

CONCLUSION

As an outcome of the pursued research work, thereal time secured health monitoring system is depicted inthis thesis. This prototype of Real time secured health monitoring system was designed and built to monitor thepeople's health wirelessly at any time and make precautionary measures to avoid death or illness.

The wearable technology is implemented with this system forthe people to feel comfortable without any add-ons to there daily wear that would not make them feel conscious.

REFERENCE

Alonso J.V., Matencio P.L., Castano F.J.G., et al. : 'Ambient intelligence systems for personalized sporttraining', *Sensors*, 2010, 10, pp. 2359–2385 .

Kumar P., Lee H.J.: 'Security issues in healthcare applications using wireless medical sensor networks: a survey', *Sensors*, 2012, 12, (1), pp. 55–91.

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.

Alemdar H., Ersoy C.: 'Wireless sensor networks forhealthcare: a survey', *Comput. Netw.*, 2010, 54, pp. 2688–2710 .

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.

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.