JCSE Journal of Computing Science and Engineering

Regular Paper

Journal of Computing Science and Engineering,
Vol. 14, No. 2, June 2020, pp. 66-75

Enhancement of Security and QoS in Wireless Medical Sensor Networks

Sathya Duraisamy* **and Pranavi Krishnasamy**
Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India
sathy.spj@gmail.com, pranavi.18mcs@kct.ac.in

Jeena Jacaob Israel
Department of Computer Science and Engineering, GITAM School of Technology, GITAM University, Bengaluru, Karnataka, India
jeni.neha@gmail.com

Jagadeesan Duraisamy
Department of Management Studies, Rathinam College of Arts and Science, Coimbatore, Tamilnadu, India
kirthikjaga@gmail.com

Abstract

Wireless medical sensor networks (WMSN) collect the data of a patient's vital body parameters using wearable or non-wearable biosensors. Since WMSN is wireless in nature there occur numerous issues like a false alarm, lack of robustness, and low processor speed, which reduce the system's effectiveness. One of the major issues is the security and privacy protection of the collected data and providing a greater Quality of Service (QoS) for the network in terms of energy efficiency, standardization, etc. Targeting these problems, we introduced a hybrid secure and fuzzy fusion system to achieve efficient secure transmission and data fusion in WMSN. The basic idea of the proposed method is to generate a private key from specific features of the digital color image; the generated key is encrypted by the Advanced Encryption Standards (AES) mechanism. The proposed system handles the vague and imprecise data to reduce energy consumption and increases the network lifetime. The inference results verify the efficiency of the proposed method in terms of security and energy consumption of the network.

Category: Privacy and Security

Keywords: Fuzzy logic; Private key; Data encryption; Digital image; Image feature

I. INTRODUCTION

Wireless medical sensor networks (WMSN) consist of distributed sensors, which sense human physiological signs and monitor the health conditions of the patient. Providing privacy to the patient's data is an important issue and a challenging task. Since the information passes through the public channel in WMSN, sensitive information of the patients can be easily obtained by an eavesdropper or by unauthorized users. Therefore, there exists an essential need of controlling unauthorized access to the patient's medical information. Symmetric encryption uses a single key that is shared among the people who are necessitated to receive the message whereas asymmetrical encryption

Open Access http://dx.doi.org/10.5626/JCSE.2020.14.2.66 http://jcse.kiise.org

Received 18 May 2020; **Accepted** 15 June 2020

*Corresponding Author

pISSN: 1976-4677 eISSN: 2093-8020

uses a pair of the public key and a private key to encrypt and decrypt the messages. Asymmetric encryption takes a relatively longer time than symmetric encryption.

Sensors are used in embedded medical equipment to convert various forms of stimuli into electrical signals for analysis. Sensors can increase the intelligence of medical equipment, such as life-supporting implants and support remote monitoring of patients. Despite the benefits of WMSN, there is a major concern to provide security for healthcare data. A lot of existing systems contribute to providing data privacy. Previously, a novel and lightweight secure system have been proposed to address the security challenges in WMSN [1]. During the digitalization of the medical records, there is a possibility of eavesdropping the health data [2]. To provide security and privacy, the improved IBE-Lite cryptographic method provides additional security provisioning to other cryptographic algorithms [3]. A novel key agreement scheme has been employed for message authentication [4]. The results are effective in terms of security performance as well as energy consumption for body area network (BAN). The effectiveness of the system could be higher not only by providing security services but also assuring Quality of Service (QoS) parameters. Reducing the amount of data transmission ultimately reduces the energy consumption of the network [5]. Therefore, the network lifetime can be increased and the battery life can be extended. Data fusion from various biosensors helps to achieve high flexibility in telemonitoring of patients [6].

Even though various cryptographic and data fusion approaches have been proposed to overcome the security and QoS challenges in wireless networks, they cannot be applied to the sensor network since the lifetime of sensors is quite less. If the security requirements are not met successfully then the data could be eavesdropped easily. To ensure security while maintaining data privacy and enhance the performance of the energy consumption, the proposed methods are hypothesized to be helpful. Various encryption methods like ElGamal algorithm, elliptic curve cryptography, block ciphers, etc., have been reported to provide security for health data. Implementation of the data fusion approach ensures that the energy consumption can be reduced and the network lifetime can be increased efficiently.

To secure sensitive data, particularly on an insecure network, RSA can be used [7]. RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer. It requires the involvement of a third party to verify the reliability of public keys. Data transferred through the RSA algorithm could be compromised through middlemen who might temper with the public key system.

To overcome this drawback, the Advanced Encryption Standards (AES) algorithm is used which not only reduces the code size but also reduces the overall energy consumption of wireless networks [8]. Despite its use in sensor networks as the fastest encryption method, it is breakable and prone to attacks. Thus, it fails to meet the security requirements of medical data [9]. Consequently, an improved AES algorithm is proposed to handle the inefficiencies. The private key could be generated from features of the digital color image and combined with AES to provide security as well as efficiency to the medical sensor network [10]. In this paper, health data from various sensors were filtered using a fuzzy logic approach and the data were encrypted using three cryptographic algorithms like RSA, AES, and hybrid AES. The computation time of all the three algorithms was compared and the performance of the hybrid AES algorithm was found to be good. The goal of the proposed method is to protect data against different types of attacks by unauthorized parties and the outcomes were positive.

In this article, Section I states the outline of wireless medical sensor networks employed in healthcare and their security issues. Both security and QoS parameters are discussed in detail. Section II describes the related work accounting for the security and privacy issues as well as the energy efficiency mechanisms. Section III demonstrates the data filtration and fusion approaches and the comparison of various cryptographic techniques and their advantages for security provisions. Section IV explains the results of the proposed techniques. The conclusion is explained in Section V.

II. RELATED WORK

Fusion technique is a major information supporting tool for system analysis and health management which possibly associates and fuses the data from different sensors, thereby reducing target perception uncertainty and improving target system integrated information processing and response capabilities. Fusing the heterogeneous data for efficient user authentication and access control are achieved in many real-time applications.

A. Cryptographic Techniques to Secure Health Data

Despite the performance, the issues of battery protection and resource usage, small sensor nodes and network life are essential aspects to be considered while developing a network. The framework used the AES and the proxy-protected signature to ensure safe data transmission and control of data access [1]. The approach thus provides confidentiality and backward secrecy. However, as the system does not deal with energy consumption, it is only suitable for low-power sensor nodes.

Privacy is a serious problem for clinicians as the medical records contain confidential information. A patient's health record may be lost when digitally scanned. In certain cases, attackers can obtain personal data. First, if the encryption or decryption is not strong enough, there may be a DoS attack. Second, the program must satisfy the security requirements. Third, if the size of the sensors is small, the sensor nodes will lose out.

In order to solve these security issues and to provide privacy, protected certificates, pseudo-random number generator, and proof of knowledge are used in the system [2].

IBE-Lite is lightweight identity-based encryption designed to achieve body sensor network (BSN) protection and privacy [3]. IBE-Lite was built upon elliptic curve cryptography, which is a BSN-suitable public key system. The machine, however, experiences a constraint that can only unlock "n" hidden keys. If more than "n" secret keys are released, the vulnerabilities are exposed by the master secret key (X). Conventional IBE is effective but cannot be used in the case of BSN devices.

B. Biometric Techniques to Secure Health Data

The demanding task is to protect health data over the wireless environment with reduced power consumption. The architecture allows the sharing of a common key produced by electrocardiogram (ECG) signals by neighboring nodes in BSN [4]. The improved Jules-Sudan (IJS) algorithm is used to set up key agreement to authenticate the messages. The experimental results demonstrate better credibility conservation and privacy than other traditional algorithms. In terms of false acceptance rate (FAR), power consumption analysis, false rejection rate (FRR), and energy efficiency for BANs, the proposed ECG-IJS scheme leads to better security results.

Developing infrastructure is a significant obstacle to be addressed when ensuring security and privacy. Using the wireless channel characteristics, the authors suggested a physical layer protection algorithm based on fingerprint behavior [5]. This offers an efficient and energy-friendly usability environment compared to traditional authentication algorithms. The proposed framework deploys three levels of protection called a region of non-trust, a region of restricted trust, and a region of trust. Therefore, during the authentication process, no additional packages can be produced thereby ensuring battery life.

Even a mild health issue transforms into an immense problem due to the massive population increase and inadequate treatment centers and personnel. The security plan would not only fix the issues but also protect personal data privacy [6]. The solution developed includes a mobile emergency system (MES) that could work both in the regular and emergency phases. A secure MES (SMES) has been deployed to ensure privacy and authentication. Based on the warning, the rescue team will take responsibility.

Resource limitations and health safeguards are the main concerns in biomedical applications. A conventional approach offers credibility and privacy about substantial memory and computing resources. Lightweight encryption and compressed sensing are implemented in the process of protection of wireless physical layers [11]. Securing of information is based on the use of measurement matrix as a key to the encryption thereby ensuring protection when compressing the analog signals at the time of sampling. With ECG, the signals can be analyzed and stimulated.

Implantable medical device (IMD) wireless transmissions should be protected against eavesdroppers and unauthorized users [12]. The proposed approach allows the use of full-duplex protected communication with a modern protector of wireless IMD systems. The jacket is responsible for the extraction of jams and the reception of maximum ratio combining (MRC). Spoofing based beamforming technique called as multi input single output (MIMO) technology is used when reception is done. The experimental results indicate that the protector is highly efficient to control eavesdroppers.

C. Biosensors Data Fusion

Protection and privacy can be obtained in various implementations regardless of the QoS parameters. One of the key reasons is to reduce energy usage and increase the service life of the network. A method is introduced to fuse the data collected from the sensors before transmission to the wireless sensor network [13]. The proposed fuzzy fusion logic incorporates the input data into each sensor and measures the percentage of similarity to define the packet size to be sent. The experiment was applied in MATLAB, and the result suggests a decrease in energy consumption and an improvement in network life.

The fusion of collected sensor data is not only helpful in developing QoS but also helps to ensure privacy in the telemonitoring system. Telemonitoring has been introduced to safeguard the privately living older population. The developers suggested a multi-modal data fusion approach to combine psychological, behavioral, and acoustic environmental factors using fuzzy systems [14]. Works were introduced in the EMUTUM platform to deal with circumstances of distress. The fuzzy classifier uses the fuzzy logic to fuzzify the inputs, the membership functions to categorize input levels, and the fuzzy IF-THEN rules to defuzzify the inputs. The multi-modal data integration approach thus improves the efficiency of the entire network and ensures the omnipresence of smart home health monitoring.

The contributions of wireless body sensor networks (WBSNs) have recently been widely used in the healthcare field. In an emergency situation, the processing of massive amounts of data collected by biosensors and the proper decision-making are the major challenges. To make the right decisions, fuzzy set theory and decision matrices are used [15]. The authors proposed Improved Local Emergency Detection with Adaptive Sampling Rate (Updated LED*) algorithm to optimize data transmission, energy usage and increasing the lifetime of the biosensors.

Computing, networking, and physical processes are built into cyber-physical systems. The medical sensor generates many false alarms which decrease the effectiveness of the system. Using fuzzy IF-THEN rules, medical fuzzy alarm (MFA) filter is designed to solve the problem [16]. Fuzzy logic handles the vague and imprecise data. The training of data sets and the analysis of simulation results is performed using the Weka tool. The experimental results demonstrate that the use of fuzzy rules improves accuracy and makes the system more effective.

The devices on the Internet of Things (IoT) have less computing power and less storage. The need to have data privacy in e-healthcare is a major issue. While several hard-security approaches have been proposed, the authors aim to include soft means of confidence management methods. The suggested approach is evaluated concerning RFID where more security services are primitive [17]. The approaches provided are ideal for the low cost and off-the-shelves commercial (COTS) environments. The trust management techniques are used as a lightweight protocol for handling privacy using ND-PEPS and generalized metrics such as subjective logic. This research leads to the development of cost-efficient and non-invasive WMBANs for healthcare services.

Health monitoring is commonly used nowadays to handle conditions of distress. A solution was built for mobile data acquisition (DAQ) based on Android [18]. The smart mobile app collects, analyzes, and sends data from different wireless or wired sensors for further processing. The proposed solution uses the cloud and the smart information system where the sensors are used in real-time. Advanced RISC (ARM7TDMI) computers are used as microcontrollers. RFID tags are attached for identification and tracking of patients and continuous monitoring of the information at the health centers. Many wireless medical sensors collect health data and combine with Android-based smartphones to offer large functionality [19]. The physiological data is transferred through the Bluetooth HC-05 module to the smartphone. ECG module using LM355 is used for signal processing. To take action at an emergency level, the alert system has been introduced in terms of both SMS and Email. Hence, the solution handles the emergency situation effectively.

The embedded and IoT devices are emerging faster in the healthcare industry. The wireless medical sensors and IoT contribute more feasibility to patients in health care centers. A new framework called SYNDROME is introduced to monitor embedded medical devices [20]. The malware detector uses electromagnetic (EM) signals to run even in the absence of malware. Syringe Pump, an embedded IoT device, is used to test SYNDROME. It is used to identify and stop the attacks.

The study of techniques to secure the process of communication between the sender and receiver in the presence of third parties is known as cryptography. Basically, it includes the design of protocols based on the fields of mathematics, computer science, and electrical engineering to encrypt as well as decrypt the information in the form of data and images. To overcome this ever-growing problem, the modified encryption and decryption of images using the RSA algorithm and its subsequent application on an image file is proposed [7]. It involves splitting of the image to procure encryptable split files, and finally retrieval of the original image by applying decryption mechanisms. As a result, an efficient approach is established for keeping the image safe.

As a faster encryption method, the simplified AES (S-AES) algorithm is used in ZigBee and sensor networks, but it is easily breakable and not secure. Thus, it does not meet the security requirements of medical applications. The modified S-AES algorithm is enough for data encryption in ZigBee networks and biomedical sensor networks, where both robustness and real-time are essential. A comparison between the enhanced algorithm and the original S-AES is presented about robustness [8]. IAR is used to simulate the improved AES algorithm and compares the standard AES algorithm to infer that the improved AES algorithm not only reduces the code size but also reduces the energy consumption [9]. The basic idea of the proposed method is to generate a private key from a specific feature of the digital color image (red, green, and blue) [21]. The hiding algorithm used is the least significant bit (LSB) [10]. The generated key is tested by the hiding process and changing the extension of the image, to detect changes in the generated key. MATLAB is used to design and implement this method.

III. PROPOSED SYSTEM

The outline of the proposed system is shown in Fig. 1. The data from wearable medical sensors use a fuzzy-based approach to filter the normal and duplicate values. Only the abnormal or highly critical values need to be sent to the doctors for medical diagnosis. So those critical values are encrypted using cryptographic algorithms to provide security and efficiency. We have used three cryptographic algorithms such as RSA, AES, and hybrid AES to provide security to the medical data. These algorithms are tested with respect to time complexity and vulnerability to attacks. RSA algorithm performs bulk encryption and decryption operations at much higher speed but takes a long time to calculate the key. To avoid such problems, the AES algorithm is used. Cracking of AES key is much difficult but the time to encrypt and decrypt the data is higher. The hybrid AES algorithm provides additional security to the data and takes relatively lesser time than AES. Hence the hybrid AES algorithm is used in the proposed system for encryption, which uses Aadhaar card as a digital color image for generating the key.

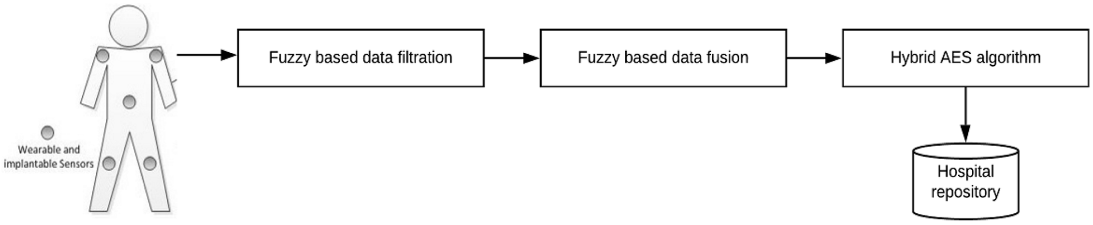


Fig. 1. Proposed system.

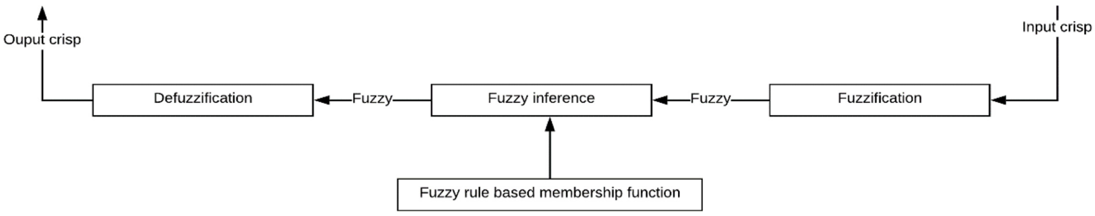


Fig. 2. Fuzzy system.

A. Fuzzy Logic

Fuzzy logic has a wide area of application in medicine. It can be used for classifying the disease or diseased patients or risk ratio of a disease. It is also used to construct a decision support system (DSS). The proposed algorithm has been built based on the normal and abnormal ranges of medical data. The input values were fuzzified in the fuzzification section as shown in Fig. 2. The input values are fed to the fuzzy inference system for filtering the data. Based on the membership function of the inputs as defined in the database and several rules defined in the rules database, the necessary inference has been made on the input data and, according to the interferences, it was found whether the output was normal or abnormal. The results were then defuzzified. After determining the normality, the test step was started and input values were fused to be fed into the hiding mechanism to provide security as well as efficiency. The input values are the attributes of cardiac disease. They are systolic pressure, serum cholesterol, ST depression, and maximum heart rate. The method of data filtration using fuzzy logic reduces the voluminous of data which should be transmitted to the hospital or the doctors, thereby reducing the energy consumption of sensors and increasing the network lifetime. Using fuzzy logic, accurate conclusions can be made. Fuzzy logic is designed to solve problems by considering all available information and making the best possible decision from the given input.

B. RSA Algorithm

RSA algorithm handles the bulk of data and provides security at a higher level. In such a cryptosystem, the encryption key is a public one and the decryption key which is different from the encryption key is kept private [7]. As two different keys are used in encryption and decryption, the RSA algorithm is also called as an asymmetric cryptographic algorithm. RSA uses prime factorization, which makes the process of deciphering the information difficult without using the right key.

The RSA algorithm consists of three major steps in encryption and decryption. The steps are as follows [7].

1) Key Generation

The RSA involves a public key and a private key. The public key is used for encrypting messages and can be known to everyone. The messages encrypted with the public key are decrypted using the private key. The process for key generation is as follows. First, choose two distinct prime numbers p and q and then compute $n=p\times q$ where n is the modulus for the public key and the private key. Next compute $\varphi(n) = (p-1)(q-1)$. Choose an integer e such that $1 < e < \varphi(n)$ and GCD $(e, \varphi(n)) = 1$. The pair (n, e) is the public key. The private key is a unique integer d obtained by solving the equation,

$$d\cdot e \equiv 1 \ (\mathrm{mod}\ \varphi(n)). \tag{1}$$

2) Encryption

The RSA algorithm is used here for encrypting an image. So the message text (m) is in the form of pixels lying in the range 0 to 255. The pixels are stored and operated upon in an array format. The text is encrypted using the public key (n, e) from the equation,

$$c = me \ \mathrm{mod}(n). \tag{2}$$

3) Decryption

The text is decrypted using the private key (n, d) from the equation,

$$m = cd \ \mathrm{mod}\ (n). \tag{3}$$

C. AES Algorithm

Since in RSA, the key is too large and calculation time is long, AES a new standard for symmetric encryption block established to change the old Data Encryption Standard (DES), which was published by the National Institute of Standards and Technology (NIST) of the United States as Federal Information Processing Standard Pub 197 (FIPS 197) on November 26, 2001. AES is an encryption algorithm that is applied to defend electronic data. Since AES has special features for wireless sensor network applications [7-9], the secure AES implementation can greatly affect very limited resources of network nodes. The benefit of using AES in healthcare data protection resides in cracking a 128-bit AES key with a state-of-the-art supercomputer, which takes longer than the presumed age of the universe.

The AES algorithm is implemented by three sections: encryption, decryption, and key generation [8].

The key expansion gives rise to a schedule key, which is derived from the secret key, that is used in the encryption and decryption procedures. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits operates. The number of revolutions depends on the cryptographic keys 10, 12, and 14, respectively. AES is based on a 4×4 bytes matrix (designated to as “state”). The algorithm is made to perform simple four different transformations that are applied consecutively on the bit data blocks, in several repetitions, as rounds. The transformations are: SubBytes, ShiftRows, MixColumns, and AddRoundKey, as shown in Fig. 3.

a) SubByte:

SubByte is a non-linear byte substitution function. Using a substitution table (S-box) replaces each byte of the state. S-box results from a multiplicative inverse of a finite field.

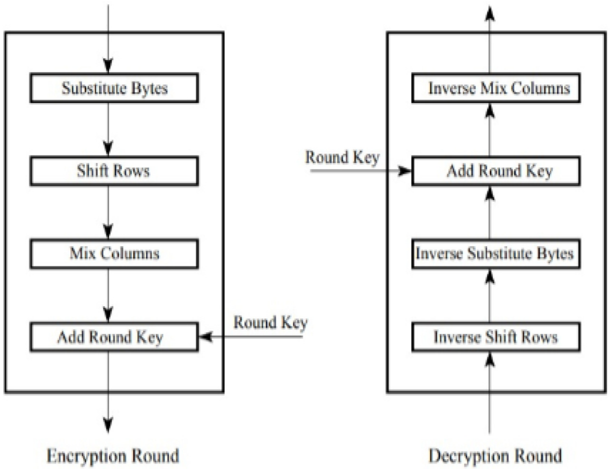


Fig. 3. AES structure.

b) ShiftRows:

ShiftRows is a permutation function. An offset identical to the line number shifts respectively row of the state to the left.

c) MixColumns:

MixColumns is a mixing function. This transformation functions on the state column by column; the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function is responsible for multiplying a constant matrix with the state.

d) AddRoundKey:

AddRoundKey is an XOR function. For each round, a subkey result from the leading key using Rijndael key schedule, XORed with state matrix.

For decryption, AES uses the inverse transformations. It applies the inverse of four process which converts 128 bit block of ciphertext into plaintext. AddRoundKey is similar for encryption and decryption. The other three use inverse functions in the decryption process: inverse SubBytes (InvSubBytes), inverse ShiftRows (InvShiftRows), and inverse MixColumns (InvMixColumns).

D. Hybrid AES Algorithm

The presented method generates a cryptographic key by using a digital color image which has extension JPEG via computing the number of frequencies for three colors of the image that are red, green, and blue by using the mathematic formula to compute frequencies for each one of them to construct the general frame for generating process [21]. The generated key is encrypted by the AES algorithm to provide security to the data. The authors used the specified features of the digital color image such as red, green, and blue to generate the key. In our work, the Aadhaar card images are used as a digital color image to generate the key and combines with AES to provide security.

The pre-processing steps for generating a cryptographic key are shown below:

i. Get the input image
ii. Calculate the colour frequency
Red Value = (Original Image(row,col,1)/ reduction_factor+1)
Green Value = (Original Image(row,col,2)/ reduction_factor+1)
Blue Value = (Original Image(row,col,3)/ reduction_factor+1)
Color_frequency = [Red Value Green Value Blue Value]
iii. Find the Maximum frequency
iv. Multiply Maximum frequency with the number of frequencies
v. Convert Numeric into String

In this work, the specified values in the pre-processing stage were hidden in an image as cover after applying XOR operation between the generated cryptographic key and value. Finally, recounting of colors frequencies of an image after decryption using AES was done to check the changes in the generated cryptographic key. Hybrid AES proves that increasing the complexity of generating a cryptographic key provides high-level security against unwanted threats or attacks.

IV. IMPLEMENTATION RESULTS

The evaluation of the following algorithms is given below:

The running time is a critical parameter in the development of an encryption algorithm. It is the overall time required to encrypt and decrypt the data. In this section, we will calculate the performance of our simulation results. MATLAB is used to implement the simulation. Aadhaar card images are encrypted and decrypted with a very short turnaround time of about 4.54 ms for encryption and 5.54 ms for decryption.

The simulation of fuzzy system is performed on the heart disease dataset [22]. The fuzzy system is implemented to categorize the normal and abnormal values of systolic pressure, serum cholesterol, ST depression, maximum heart rate, which is shown in Figs. 4–7. The normal range for systolic pressure is 80–130 mm Hg, serum cholesterol is 150–200 mg/dL, ST depression is 0.1–0.3 mV, respectively. The normal range for heart beats per minute is between 60–110. The Fig. 8 shows the output of heart disease in

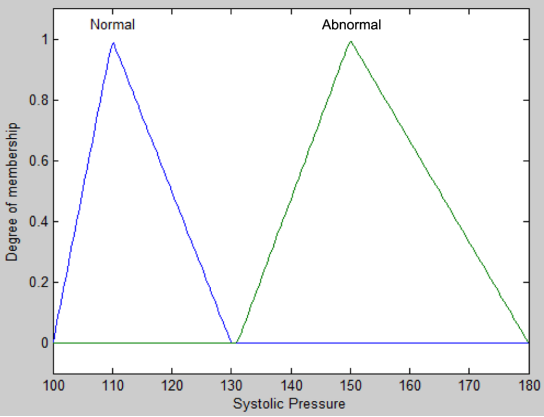


Fig. 4. Systolic pressure.

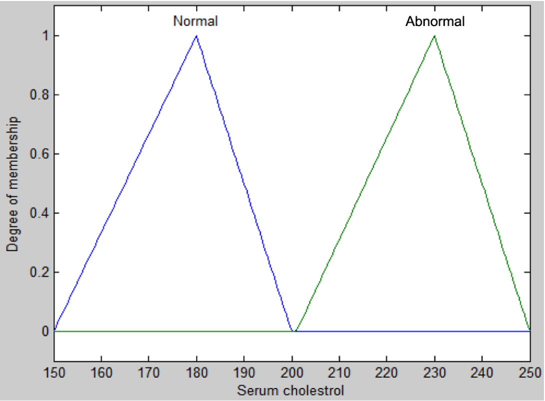


Fig. 5. Serum cholesterol.

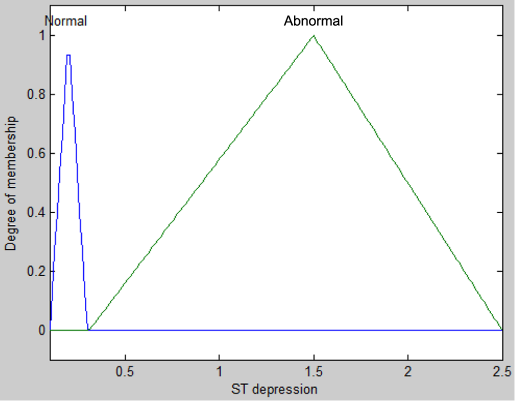


Fig. 6. ST depression.

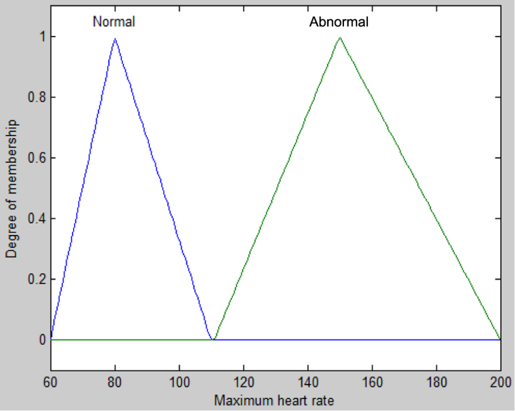


Fig. 7. Maximum heart rate.

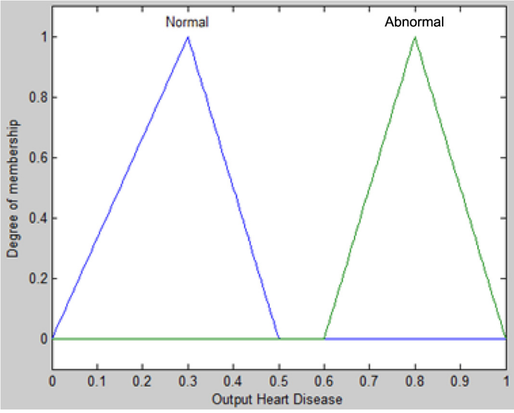
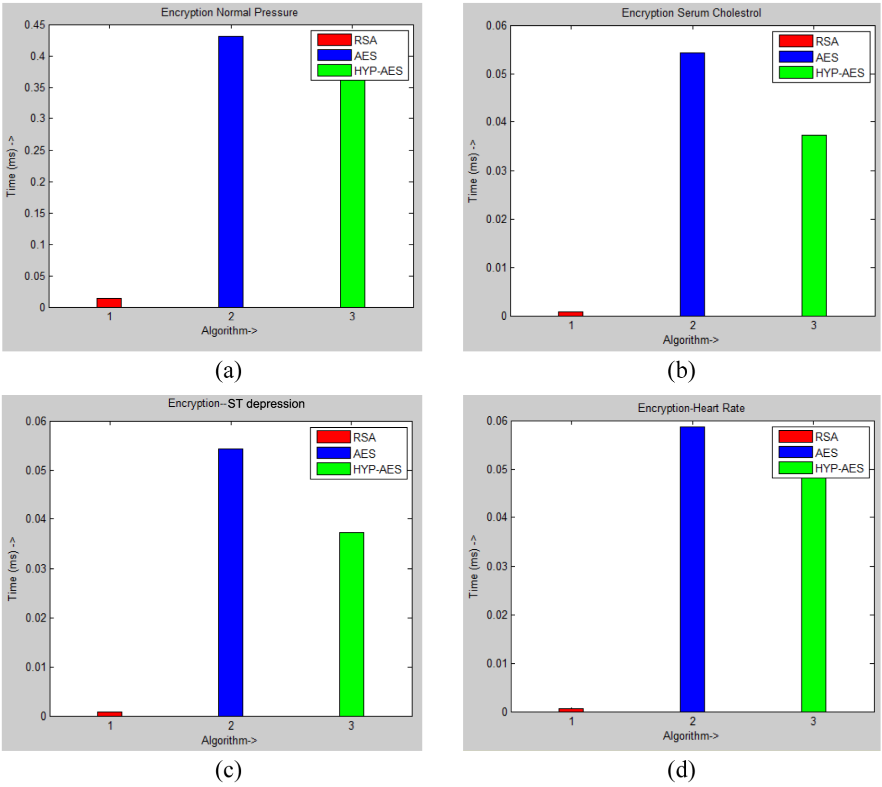


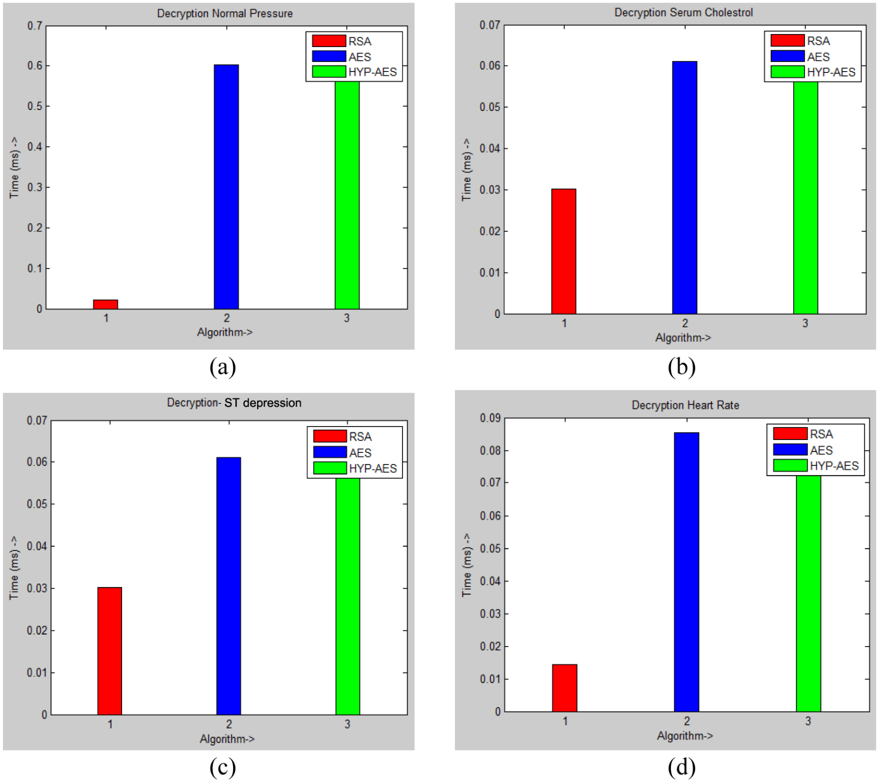
Fig. 8. Output heart disease.



(a) (b)

(c) (d)

Fig. 9. Simulation results for the encryption: (a) systolic pressure, (b) serum cholesterol, (c) ST depression, and (d) the maximum heart rate.



(a) (b)

(c) (d)

Fig. 10. Simulation results for the decryption: (a) systolic pressure, (b) serum cholesterol, (c) ST depression, and (d) the maximum heart rate.

which the range beyond the boundary value is taken as the abnormal state.

The simulation results of using the above-mentioned algorithms are shown below as a comparative analysis. Fig. 9 shows the time complexity to encrypt the systolic pressure, serum cholesterol, ST depression, and the maximum heart rate. Fig. 10 shows the time complexity to decrypt systolic pressure, serum cholesterol, ST depression, and the maximum heart rate.

Since the key generation using RSA takes much time, deciphering the ciphertext is very difficult due to the minimum number of steps and it takes very little time for the encryption and decryption. In the case of using AES, the key generation is simple but it involves many steps to both encrypt and decrypt, thereby taking much time for the encryption as well as decryption, but provides higher security at the same time. Comparatively, the hybrid AES algorithm is stable in terms of providing higher security as well as takes reasonable time to encrypt and decrypt.

V. CONCLUSION

Sensor networks are the standard technology in wireless communications. Due to the wide range of sensor distribution, a massive amount of data is produced. From experiments of the proposed method, we can articulate that combining the data fusion approach with the enhanced hiding mechanism results in reducing energy consumption and increasing the network lifetime. In future work, the proposed method can be used under conditions of different protocols and different scenarios.

REFERENCES

1. D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 316-326, 2013.
2. J. Sun, Y. Fang, and X. Zhu, "Privacy and emergency response in e-healthcare leveraging wireless body sensor networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 66-73, 2010.
3. C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-Lite: a lightweight identity-based cryptography for body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926-932, 2009.
4. Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070-1078, 2012.
5. N. Zhao, A. Ren, M. U. Rehman, Z. Zhang, X. Yang, and F. Hu, "Biometric behavior authentication exploiting propagation characteristics of wireless channel," *IEEE Access*, vol. 4, pp. 4789-4796, 2016.
6. S. Y. Chiou and Z. Y. Liao, "A real-time, automated and privacy-preserving mobile emergency-medical-service network for informing the closest rescuer to rapidly support mobile-emergency-call victims," *IEEE Access*, vol. 6, pp. 35787-35800, 2018.
7. S. Mukherjee, S. Sinha, S. Chakrabarti, and T. Mukhopadhyay, "A meticulous implementation of RSA algorithm using MATLAB for image encryption," in *Proceedings of 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech)*, Kolkata, India, 2017, pp. 1-6.
8. N. Challita and B. Bakhache, "Enhancement of S-AES using chaos for the support of biomedical applications," in *Proceedings of 2013 2nd International Conference on Advances in Biomedical Engineering*, Tripoli, Lebanon, 2013, pp. 175-178.
9. F. Rao and J. Tan, "Energy consumption research of AES encryption algorithm in ZigBee," in *Proceedings of International Conference on Cyberspace Technology (CCT 2014)*, Beijing, China, 2014, pp. 1-6.
10. A. Msolli, A. Helali, and H. Maaref, "Image encryption with the AES algorithm in wireless sensor network," in *Proceedings of 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Monastir, Tunisia, 2016, pp. 41-45.
11. R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 1, pp. 135-142, 2016.
12. S. Kulac, "A new externally worn proxy-based protector for non-secure wireless implantable medical devices: security jacket," *IEEE Access*, vol. 7, pp. 55358-55366, 2019.
13. A. Mandeh, K. Khamforoosh, and V. Maihami, "Data fusion in wireless sensor networks using fuzzy systems," *International Journal of Computer Applications*, vol. 125, no. 12, pp. 31-36, 2015.
14. H. Medjahed, D. Istrate, J. Boudy, J. L. Baldinger, and B. Dorizzi, "A pervasive multi-sensor data fusion for smart home healthcare monitoring," in *Proceedings of 2011 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE 2011)*, Taipei, Taiwan, 2011, pp. 1466-1473.
15. C. Habib, A. Makhoul, R. Darazi, and C. Salim, "Self-adaptive data collection and fusion for health monitoring based on body sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2342-2352, 2016.
16. W. Li, W. Meng, C. Su, and L. F. Kwok, "Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems," *IEEE Access*, vol. 6, pp. 6530-6539, 2018.
17. D. Trcek and A. Brodnik, "Hard and soft security provisioning for computationally weak pervasive computing systems in e-health," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 22-29, 2013.
18. S. Lakshmanachari, C. Srihari, A. Sudhakar, and P. Nalajala, "Design and implementation of cloud based patient health care monitoring systems using IoT," in *Proceedings of 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, China, 2017, pp. 3713-3717.
19. N. Sehatbakhsh, M. Alam, A. Nazari, A. Zajic, and M. Prvulovic, "SYNDROME: spectral analysis for anomaly

detection on medical IoT and embedded devices," in *Proceedings of 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, DC, 2018, pp. 1-8.

20. Y. K. Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 456-467, 2019.
21. W. A. Shukur, "A proposed method for generating a private key using digital color image," *International Journal of Applied Engineering Research*, vol. 12, no. 16, pp. 6235-6240, 2017.
22. UCI Machine Learning Repository, "Heart Disease Data Set," https://archive.ics.uci.edu/ml/datasets/Heart+Disease.

Sathya Duraisamy

Sathya Duraisamy is presently working as Assistant professor II, Department of Computer Science and Engineering, at Kumaraguru College of Technology, Coimbatore. She received the B.E. Computer Science and Engineering degree from Bharathiar University in 2004 and M.E. Computer Science and Engineering degree from Anna University, Coimbatore in 2010, and completed her doctorate degree in Anna University, Chennai in the year 2019. She has overall experience of 15 years in teaching field. Her research interests include sensor network and security. She has published 30 papers in international journal and conferences.

Pranavi Krishnasamy

Pranavi Krishnasamy completed Bachelor of Engineering in Computer Science and Engineering Department at Kumaraguru College of Technology, Coimbatore in the years 2014-2018 and is doing her Master of Engineering in Computer Science and Engineering at Kumaraguru college of Technology, Coimbatore.

Jeena Jacaob Israel

Jeena Jacaob Israel has completed her B.E. (Computer Science and Engineering) in 2004 from St. Xavier's College of Engineering, Chunkanakadai, M.E. (Computer Science and Engineering) in 2006 from Karunya Institute of Technology and Sciences (Deemed to be University), Coimbatore and Ph.D. (Information and Communication Engineering) in 2015 from Anna University, Chennai. Her areas of research are image processing, deep learning, etc.

Jagadeesan Duraisamy

Jagadeesan Duraisamy works as assistant professor in the Department of Management Studies in Rathinam College of Arts and Science, Coimbatore. He received his Bachelor of Science in Electronics at SNR Sons College, Bharathiar University, Coimbatore, in the year 1994. He completed his Master of Business Administration at RVS College, Bharathiar University, Coimbatore, in the year 2000. He completed his Master of Philosophy in Management at SNR Sons College, Bharathiar University, Coimbatore, in the year 2011. He published many papers in international journals and conferences.