A Novel Secure Patient Data Transmission through Wireless Body Area Network: Health Tele-Monitoring

A. Basnet[1], Abeer Alsadoon[1], P.W.C. Prasad[1], Omar Hisham Alsadoon[2], Linh Pham[1], Amr Elchouemi[3]

[1]Charles Sturt University Study Centre, Sydney, Australia
[2]Al Iraqia University, Baghdad, Iraq
[3]Colorado State University Global Campus, USA

***Abstract*:** The security of sensitive data obtained from a patient has not been implemented properly because of energy issues of sensor nodes in Wireless Body Area Network (WBAN) and constrained resources such as computational power and low battery life. The main of this paper is to enhance the security level of data transmission between patient and health service provider by considering the availability of energy at sensor nodes. The proposed system consists of a hybrid Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), which provides simple, fast and high cryptographic strength of data security. ECC is used for securing AES encryption keys, and AES algorithm is used for encrypting/decrypting text. A scenario where sensor nodes are continuously supplied energy from solar power is considered and based upon the energy availability; respective encryption technique is implemented. The result shows that the proposed EEHEE algorithm increases the encryption of the data file by more than 19% compared to the State of Art's solution. The proposed EEHEE system is 11% faster in encrypting data file and reduces the energy consumption by 34 % compared to the current best solution. The proposed system concentrates on reducing the energy consumption in WBAN and increasing cryptographic strength to the system by using the hybrid symmetric and asymmetric algorithm. Thus, this study provides an efficient scheme to enhance security for real-time data transmission in telemedicine.

Keywords: *Data encryption, Advanced Encryption Standard, Elliptic Curve Cryptography, energy consumption, wireless body area network*

1. Introduction

Telemedicine is the process of use of telecommunication technology for remote diagnosis and treatment of patients. It allows health professionals to diagnose, evaluate and treat health patients without visiting them. Traditionally, both doctor and patient need to be physically present in clinic or hospital in the treatment. However, the limitation of the traditional system is the cost of time and money required to visit the clinic. In the present context, small wearable devices like fitness wristbands, heart-rate monitors, smart watches, and glasses have been invented, which send data to health service providers and accordingly are treated [1][2]. The emergence of the wireless body area network has a huge possibility of bringing revolution in future remote health technologies.

WBAN comprises of small, non-invasive sensors with low voltage and computational power and limited energy capacitors. These devices are either wearable or implanted in the human body which helps in early detection of diseases by continuously monitoring and transmitting health data to a health professional. In the telemedicine field, these devices connect health service provider and patient all the time and proper treatment are provided in case of any alarming cases. However, there are concerns raising about safe data transmission between patient and medical staff and energy limitation of the sensor node of WBAN. Kim et al. [3] stated that there is a trade-off relation between lifetime and data security level in wireless sensor nodes. Furthermore, the sensor nodes have very limited memory spaces and limited bandwidth available. Therefore, the algorithm which can provide better security, fewer computations, lower power consumption, and small-sized output should be selected for WBAN [4][5].

In the present context, many authors have contributed to the field of data transmission security. The current studies of hybrid encryption technique in data transmission use AES as symmetric and RSA as asymmetric encryption technique to prevent unauthorized access, to protect data integrity and confidentiality [6]. However, this system is slow and energy consumption in the case of WBAN. Asymmetric encryption (RSA) is a slow process which can consume more energy and can decrease the lifetime of the battery of WBAN. Such blackout of the node can lead to failure within the WBAN system and make the system vulnerable to attack. Priya et al. [7] proposed ECC algorithms to secure the data communications between wearable sensors and data sink. However, ECC encryption system consumes more processing time for encryption and decryption process if implemented alone, which is not preferred in WBAN.

The purpose of this study is to increase the cryptographic strength in WBAN sensor nodes by utilizing the least amount of energy available in sensor nodes. The hybrid AES, RSA and HMAC encryption scheme can lead to black out of a node as RSA is a slow process and requires more energy for the key generation. The use of ECC alone can be time-consuming and requires more computational power. This study proposes a new hybrid encryption technique, i.e. AES and ECC to provide maximum strength by using lowest possible energy in WBAN sensor. This study aims at reducing the time needed for encrypting message and reduce the amount of energy required for sensor.

2. Literature Review

This research focuses upon the use of encryption algorithms

for securing data file exchange, the time required for encrypting and decrypting the data file and amount of energy consumed during the telecommunication process. The process of securing highly sensitive health information requires high encryption algorithm systems. However, it is challenging to use high encryption algorithm scheme in wireless sensor as it requires more computational power and resources, which are not available in wireless sensor nodes. Meanwhile, symmetric encryption techniques are efficient but sharing secret key is a problem. On the other hand, asymmetric technique offers a solution for key sharing problem but is a slow process and consumes more energy. These limitations on the encryption system can make the sensor node either vulnerable to attacks or drains energy of WBAN very quickly. Initially, this research identifies the strength and limitation of symmetric and asymmetric encryption techniques for real-time communication between health patient and medical professional. Then, this research proceeds with the selection of encryption technique considering throughput time and energy issues of WBAN. After then, this research selects the best current solution to analysis latest encryption system and its result. Further analysis is done to find the limitation of the current best solution. Then a new solution is proposed to overcome the limitations providing theoretical and mathematical justification. And finally, simulation is done to experimentally verify that the new proposed system can provide high network security and save more energy in sensor node over the current system.

Amin et al. [8] reviewed the importance of securing data transmitted on each node of wireless sensor network and made a conclusion that encryption system can protect against eavesdropping and other malicious cyber-attacks. The key management process is one of the most challenging issues in wireless sensor networks as they are very constrained in resources such as memory, power and processor. National Institute for Science and Technology (NIST) [8] presented Advanced Encryption Standard (AES) as the current standard in encryption, which is being widely used in low energy available networks because of its high speed and high data encryption rate. However, the key management process is very difficult in AES. Hercigonja et al. [9] made a comparison of different symmetric and asymmetric cryptographic algorithms based upon the architecture of algorithms, security aspects and limitation they possess. A conclusion was made that asymmetric algorithms, although being high secured, they use more memory and high time processing.

Salim and Herba [6] introduced a hybrid secure encryption system of AES, RSA and HMAC where RSA was used for protecting AES encryption keys, AES was used for encryption and decryption process, and HMAC was used to protect message integrity. Although, this system provided simple overall encryption run and high system security, but still RSA seemed more time consuming. In this work, the hybrid encryption idea will be used. Liu et al. [10] proposed two anonymous authentication protocols for WBAN. However, was criticized by Xiong et al. [11], He et al. [5] and Zhao et al. [12] for being prone to impersonation attack and lack of strength to provide real anonymity. Hussain et al. [13] proposed a physical-layer security approach for securing video communication by considering noise aggregation. Whenever the eavesdropper has high-bandwidth connection than the receiver, this method seemed to have limitation. No further improvement has been done in this model.

Later, Tiwari et al. [14] provided a secure authentication protocol to prevent unauthorized users to access. Biometric identity, password and smart were used to validate the genuine authorized user. The solution helps to secure from man-in-the-middle and replay attack but has a limitation such as loss of smart card, forgotten passwords and false positive or false-negative issues of biometrics. Kiah et al. [2] used real-time transport protocol and RSA and AES algorithm for encrypting video in a conferencing framework for telemedicine. Although threats such as eavesdropping, disruption of transmission, data interception have been reduced, however, the system proved to be slow and increased delays. However, AES as being strong and fast encryption technique is used in the proposed method. Hayajneh et al. [15] proposed a method for WLAN with high speed and throughput without affecting data security using the FPGA (Field-Programmable Gate Array) system. This improved the data transmission speed by 3.7 times but has the disadvantage of being a single point of failure. This technique is not used in the proposed solution.

Raja et al. [16] presented an energy efficient secured encryption system using a RelAODV routing protocol to provide a highly secure system by utilizing the low energy of sensor nodes. This system could achieve high performance and much lesser packet dropping rate as compared to other conventional systems. However, as RSA encryption algorithm is used for this system, it is a slow process and is avoided in this project. Kim et al. [3] have used ECC encryption algorithm in a power adaptive sensor scenario which can conserve energy but ECC alone takes more computational time for encryption and decryption process. The solar-powered environment will be considered for this project.. Kumar et al. [17] proposed a hybrid algorithm architecture where a plain text is encrypted first with AES and then with ECC algorithm and hashed by MD5. However, the execution time under this system as long as both AES and ECC need to encrypt and decrypt plain text sequentially. This paper focuses on providing high cryptographic strength and will be used for this project [18][2].

Furthermore, Omala et al. [19] introduced an efficient remote authentication scheme for WBAN, which provided security against mutual authentication, anonymity and impersonation attack. However, the use of timestamp authentication imposes several limitations such as issues of clock synchronization and to trust clocks. This method is not used in the proposed system [20-23]. Furthermore, Priya et al. [7] introduced a secure and efficient data communication in WBAN by using ECC algorithm. ECC uses fewer numbers of key bit length than RSA and can provide same cryptographic strength for message authenticity and collusion resistance. ECC is useful for devices with limited storage and low processing power and is faster than RSA. However, if ECC algorithm is used for key generation, encrypting and

decrypting data, then this can slow down the process, and more energy will be consumed. ECC will be used for generating keys in the proposed system.

Salim and Herba [6] presented a secured data encryption system through a combination of AES, RSA and HMAC which utilizes the maximum advantage of a feature of symmetric and asymmetric encryption algorithms. In this system, RSA (asymmetric algorithm) is used to protect AES encryption keys; AES (symmetric algorithm) is used to encrypt and decrypt data, and HMAC are used to protect the data identity and integrity. This combinational encryption run provides high system security with low computational requirements. Figure 1 reveals the current system features highlighted in blue and limitations highlighted in red. The above figure 2 shows the flowchart of the hybrid encryption algorithm used for the state of art solution. In the first stage, one private and one public key is generated using RSA algorithm. These two keys are used for encrypting and decrypting AES key. The plain text is encrypted using AES encryption, and the cipher text is decrypted to final text using AES decryption. Sender Site (Remote Site): At the data sender side, AES encryption session key is generated and is used to encrypt the plain text as shown in figure 1. Along with the receiver's public key, RSA algorithm is used to encrypt AES session key. SHA256 hashing is used to hash the plain text and final output file is transferred to receiver end. The use of RSA encryption technique poses a limitation with the State-of-the-Art current solution as this technique is a slower process and requires a larger number of keys for providing the same level of cryptographic strength as compared to other asymmetric algorithms, which means that more computing power, memory, and battery life are consumed by RSA.

Receiver Site (Local Site): On the receiver end, the output file is processed through three different components as Encrypted cipher text, encrypted AES session key and SHA256 hash in which encrypted AES session key is decrypted using RSA algorithm with receiver's private key. Similarly, encrypted cipher text is decrypted using AES algorithm using AES key and then is hashed with SHA256. Both the hashes at the sender and receiver side are matched and if matched the data is considered true and if not, data is either corrupted or tampered.

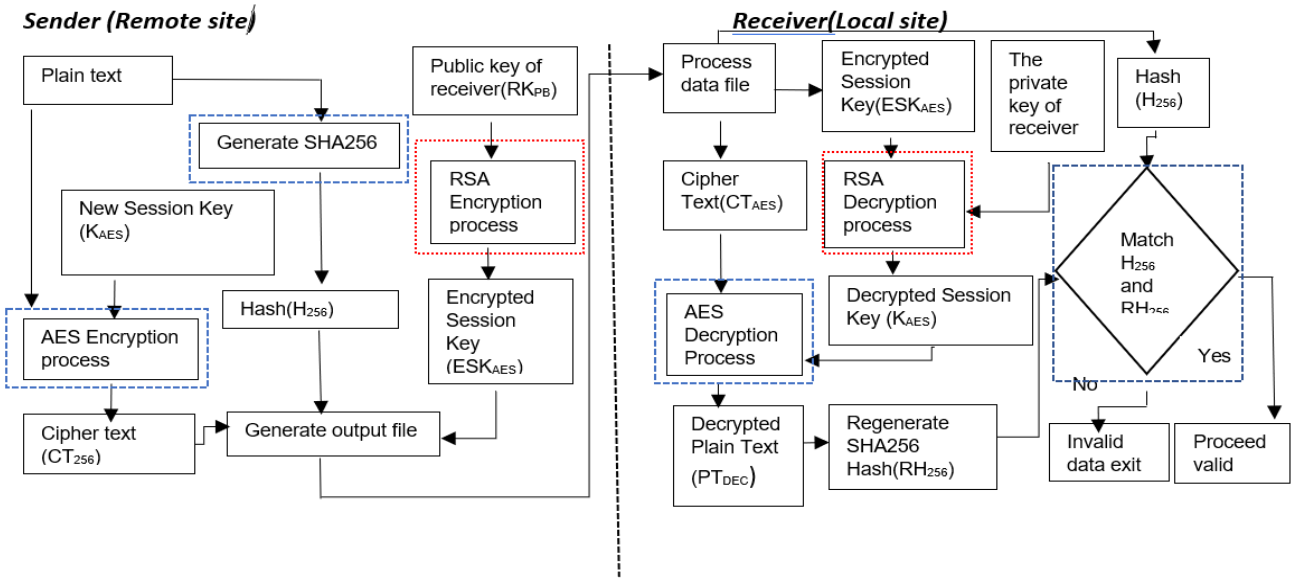

Figure 1. State of Art solution (Salim and Herba,2017)[6]; blue dotted border shows good features and red dotted border shows the limitations of this work

[This system considers data transmission between a patient at remote site and doctor at the local site.]

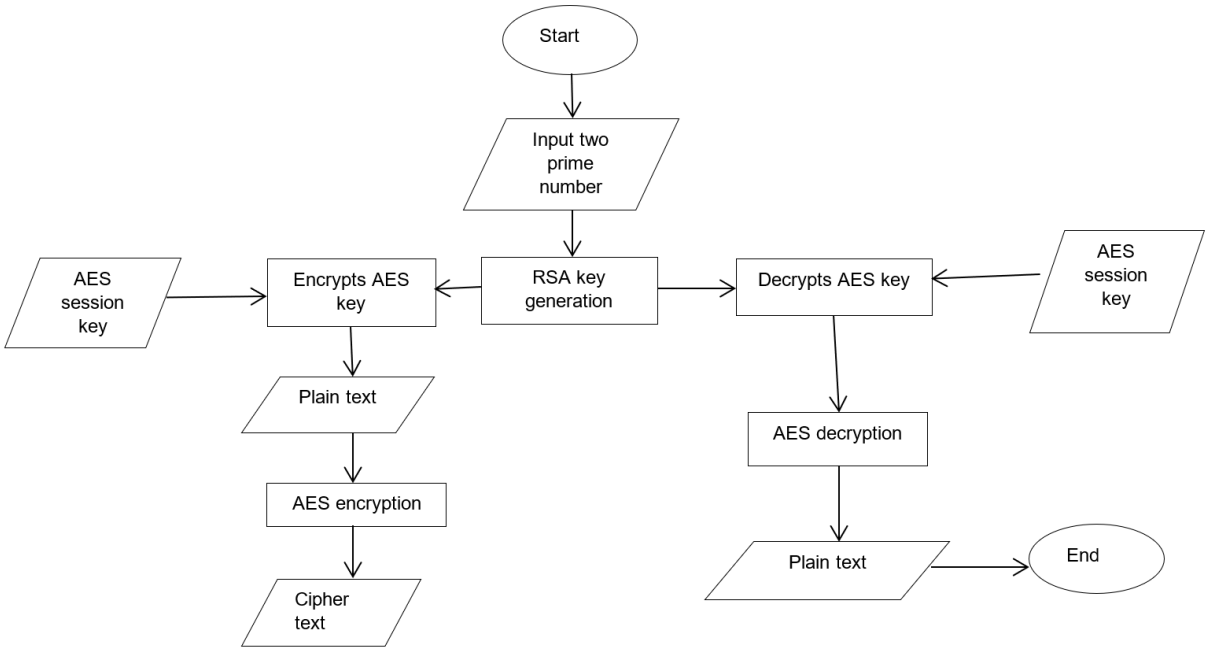

Figure 2. Flowchart of the hybrid encryption algorithm

The State of Art's solution has provided an increased level of text encryption from 144 bits to 784 bits under 1 second of encryption time. Furthermore, upon using a large text file of 136800 bytes, just a small change of size was seen because of adding 256bit AES and 256-bit HMAC encryption under same time request. This solution could provide high encryption speed with low processing time. However, the major issue with the current best solution is the RSA algorithm for the system which is a slow process and requires great computational resources for key generation. In the key generation process, RSA utilizes high memory power and also uses a large number of keys in order to provide the same level of cryptographic strength as of other encryption techniques.

The hybrid AES, RSA and HMAC encryption technique is presented in table 1 and the respective flowchart is shown in figure 2.

Two prime numbers p and q are generated, and modulus calculated from the product of p and q. The key generation process in RSA is given by equation 1 and 2 [24]

Public key (e)= (p-1) (q-1) (1)

Private key (d)= mod ((p-1) (q-1)) (2)

Where p and q are two random prime numbers.

If the values of p and q are small, then encryption processes becomes weak and the attacker can easily decrypt the data by using random probability theory and side channel attacks. If the values of p and q are large, then it will take a long time for a key generation, calculation and performance are degraded. RSA algorithms require similar lengths of p and q, which is a very difficult condition to satisfy practically as well.

Table 1. Hybrid Encryption Algorithm

Algorithm: RSA and AES algorithm encryption technique for encryption/decryption to protect data Input: two prime numbers and plain text Output: cipher text and original plain text
BEGIN Step 1: Input two prime numbers p and q Step 2: Compute n = p*q Step 3: Compute z= (p-1) (q-1) Step 4: Enter public key (e) Step 5: Input plain text Step 6: Compute cipher text Step 7: Input private key (d) Step 8: Compute original plain text Step 9: Encrypt plain text using AES algorithm Step 10: Generate cipher text Step 11: For decryption, the process step is reversed Step 12: Plain text

3. Proposed System

Medical professionals usually provide live instructions and feedback to patients via a telecommunication to save time and travel cost. The sensor nodes implanted on the human body transmit a message from the patient's body to doctors who alert them in case of an alarming situation. So, an internet connection and proper functioning of all devices are required for telecommunication. Furthermore, it is necessary that the data transmission is secured and trustworthy. Our proposed solution considers securing real-time data transmission between two parties in telemedicine where data related to the health condition to the patient (remote site) is automatically sent to doctors (local site) via wearable sensor devices. Additionally, it considers sending secured data encrypted with a fast and simple hybrid encryption technique of AES and ECC to trusted receivers. This feature will

increase the level of data security and decrease the overall encryption time as compared to the current best solution. Thus, our proposed solution considers two important parameters, which are encryption time and energy consumption for sensor nodes of WBAN. These two parameters along with the level of data encrypted and a number of keys used by the encryption system will provide an efficient hybrid encryption algorithm which can be used in resource-constrained WBAN. The proposed system provides an energy-efficient hybrid algorithm technique which can provide robust security against malicious attacks and, which solves energy issues of the wireless sensor. The algorithm of our proposed system is shown in table 4, and the flowchart of the process is presented in figure 3. At energy-rich mode, data transmission occurs from a patient at the remote site to doctor at the local site. ECC algorithm generates two keys, which protect AES encryption keys. AES algorithm is used for encrypting a file to cipher text and is sent to doctor at the remote site. At the remote site, the cipher file is decrypted by AES algorithm and is converted to original plain text.

3.1 Analysis of Energy Consumption at Sensor Node

At first stage, the energy consumption of a wireless sensor node is analyzed. As each of the sensor nodes in WBAN detects events, process and transmits data, energy consumption is divided into three parts, sensing, data processing, and transmission. The energy consumption from sensing depends on the applicant, types of sensor and complexity of detection. The consumption of energy in data processing depends on the clock frequency, average capacitance, Voltage supply and thermal voltage. As most of the energy is used in data transmission, the Energy used in data transmission is given by equation 3 [3].

$$ET=Eo+Etx+Erx, \quad (3)$$

where Eo is output transmit power and Etx and Erx are the power used in transmitter and receiver electronics.

The threshold value, i.e. energy consumption of entire network is calculated to determine two modes of the sensor. If the energy available in sensor node exceeds threshold energy, then sensor node operates in Energy-Rich mode and if energy available is less than threshold energy, then the sensor will operate in Energy-Saving mode. Another important aspect of classifying two nodes is to maximum utilization of energy in sensors. At some cases when threshold energy may be a high node will still operate in energy-saving mode and thus providing low-level security, which can waste energy available. On the other side, when the threshold is low, nodes may still operate in Energy-rich mode, which can lead to increase security level and hence blackout time of nodes.

As we are considering solar-powered sensor node, it is very important to consider energy harvesting rate of the solar cell and energy-consuming rate through the system. The main advantage of calculating is to find out the level of energy available at solar-powered sensor nodes. The amount of energy available in a battery is satisfied by equation 6 [3]:

$$Eresidual(i) \geq Psys(i).Tfull(Eresidual(i)) \quad (4)$$

Where, Psys is average power consumption rate of node i. and Tfull is time expected until battery becomes full.

After the verification of mode of the sensor node of WBAN, the nodes will operate accordingly to the type of energy available of mode. The strength of security level will then depend on the mode type.

3.2 Hybrid AES and ECC Encryption Algorithm

The next main contribution in our proposed system in the second stage is the application of hybrid encryption techniques. Following to the previous stage where we calculate threshold energy at nodes, in this stage, we apply AES encryption method when energy available is low because AES encryption requires the low amount of energy for encrypting and decrypting data and is also fast as compared to another symmetric encryption technique. If the energy available at nodes is greater than threshold energy, then the hybrid technique of AES and ECC will be used such that energy could be utilized properly. This will lead to a fast and high level of security. In this hybrid technique, using fewer numbers of key bit length, ECC will generate two keys, public and private. AES encryption will use the public key of ECC to encrypt data and the private key of ECC for data decryption at the receiver end. The main reason for using AEC and ECC together is because AES has a major issue in key exchange as it has the same shared key for both encryption and decryption.

The proposed power adaptive enhanced hybrid encryption technique is the combination of AES and ECC together in a rich energy available environment. By replacing the RSA algorithm with ECC, which is being used in the State of Art's solution, this new solution will be faster, more secured and will use less energy as ECC which is used as a key generation process requires fewer numbers of key length and the keys generated are very hard to get cracked.

According to the list provided by NIST for key size comparison, ECC requires the lesser number of keys than RSA and DSA. This makes ECC to utilize less energy for functioning and thus considered suitable for low power applications such as WBAN. Following table 2 shows the key comparison between ECC and RSA .

Table 2 . Key size comparison of ECC and RSA

ECC (key size in bits)	*RSA (key size in bits)*	*Ratio of key size*	*AES (key size in bits)*
160	*1024*	*1:6*	*..*
256	*3024*	*1:12*	*128*
384	*7680*	*1:20*	*192*
512	*16,360*	*1:30*	*256*

In Elliptic Curve Cryptography, the equation of an elliptic curve is given by simple elliptic formula as in equation [7]:

$$y2 = x3 + ax + b \quad (5)$$

Fig. 4 A simple elliptic curve; P is a point on the curve and Q is a public key

The above figure 4 shows a simple elliptic curve which is used for generating a private key of ECC algorithm.

ECC uses scalar multiplication despite using multiplication or exponentiation in the finite field. For example, for a point P on an elliptic curve, a scalar multiple of P, say as k is k. P= P+P+P+P….+P(k times). Solving Q= k.P which is used by ECC is more difficult to break down than factorization used

by RSA and discrete logarithm used by Diffie-Hellman. This makes ECC stronger than public key and signature authentication methods. Also, implementing scalar multiplication in software and hardware is much more feasible than performing multiplications, which make ECC much more computationally efficient than RSA. In this proposed solution, we use a fast and improved algorithm for point multiplication of KP as shown in table 3.

Table 3. KP algorithm

Input: K (in binary form), P
Output: Q=KP
1. **n = i-1**
2. **while (n>1) do**
   - **2.1 If a_n= 1, then Q<= 2P+P; else Q <=2P**
   - **2.2 n <=n-1**
   - **2.3 p<=Q**
3. **Return Q**

3.3 Remote Site of Telemedicine

At the local site of telemedicine communication, i.e. patient, plain text is encrypted to cipher text by AES encryption algorithm. Before encryption process, AES encryption keys are protected by the public key of ECC algorithm. ECC algorithm generates a pair of keys, public and private key. Then, AES encrypted key is used in the encryption process. This cipher text is then sent to doctor at the local site.

3.4 Local Site of Telemedicine

At a remote site of telemedicine communication, i.e. doctor, the received cipher text is decrypted into original plain text by an AES decryption process. The private key of ECC is used for securing AES decrypting keys. After then, the decrypted AES keys are used for decrypting cipher into plain text. The doctor will receive original data file sent from a health patients (remote site) after being undergone through series of encryption and decryption process.

3.5 Area of Improvement

The proposed solution is a hybrid encryption AES and ECC algorithms, which can be used in the wireless sensor network. This work will help to secure highly sensitive health data and increase the lifespan of the wearable sensor device. Our proposed solution considers the use of ECC encryption technique for encrypting AES keys and AES are used for encryption and decryption process. The current best solution has used AES and RSA encryption algorithm where RSA was used for encrypting AES keys. As RSA uses a large number of key sizes as compared to ECC for providing the same level of cryptographic strength and RSA is a slow process, we have made an improvement in our proposed solution by replacing RSA with ECC. With our proposed system, high level of data encryption can be provided, and less energy of the node is used, which means that lifetime of the node is increased as well.

3.6 Proposed Equation

The final enhanced proposed equation for hybrid encryption will be given by equation 6 and 7. AES encryption algorithm is used to encrypt cipher text in which encryption key is generated from ECC as given by equation 8. To get an original plain text, AES decryption algorithms are used as given by equation 9.

Enhanced cipher text(EC)= (((((P ⊕ ky')Mr)Mc) ⊕ky') (6)

Plaintext(P)=(((((C⊕ky')Mc)Mr)⊕ky') (7)

Where,

EC= Enhanced cipher, P= plain text, ky' is secret key obtained from ECC key generation process, ⊕= XOR, Mr= Mixed rows and Mc= Mixed columns

ECC key can be generated by equation 8 [24]

Ky'=K*P (8)

Where,

Ky'= public key

K= random number within range of 1 to (n-1)

P= point of elliptic curve

Why hybrid encryption technique? A hybrid encryption technique is basically a combination of symmetric and asymmetric encryption techniques, which uses asymmetric encryption technique for key generation and symmetric encryption for protecting data. As AES is considered as a fast process but has got a limitation in its key generation phase because it has only one private key, which is very vulnerable to attack. Asymmetric encryption technique generates two keys, private and public key for encryption and decryption process but takes a longer time as compared to AES. Thus, in order to provide an asymmetric and symmetric technique is used together. As we are also looking forward to saving energy in WBAN sensor nodes, level of security should be considered while taking energy in order to account. The current best solution uses AES as symmetric encryption technique, RSA as asymmetric encryption and HMAC as a hash authentication system. Here, RSA is used for generating keys and protecting AES keys on both receiver and sender side. AES algorithm is used to encrypt and decrypt the message. HMAC ensures data integrity of the message by comparing the hash value of receiver and sender side. However, RSA is a slow process and requires a large number of keys as compared to another asymmetric cryptography, this technique will slow down the process and use more energy for generating keys. This will affect the availability of energy in sensor node of WBAN. The second-best solution solves this limitation by using ECC, which is a replacement to RSA, and it considers that power is supplied to sensor nodes via solar energy. The mode of the sensor node is divided into Energy Rich and Energy-Saving mode. The node will use AES encryption in Energy-Saving mode because it is essential to conserve energy to avoid a blackout at node and AES is considered as a fast process and uses less energy for encryption/decryption process than another technique. If the sensor node has sufficient energy, then they will operate in Energy-Rich mode and thus ECC will be used. The limitation of the second-best solution is not using a hybrid technique in Energy-Rich mode

With the combination of the current best and second-best solution, power adaptive hybrid data encryption for energy-efficient and secure communication in WBAN is proposed. It is accomplished by combining AES and ECC technique together in Energy-Rich mode. The major advantage of using ECC over RSA is ECC can provide same cryptographic

strength as RSA by using a much lesser number of key bit size and is much faster than RSA. This helps to build strong data security level and conserve energy as well.

The proposed enhanced hybrid algorithm goes through series of step as shown in the flowchart in figure 5. A random number is used for generating a key using ECC algorithm. If point P lies in a curve, data is sent for AES encryption. The add-round key operation is performed followed by bit wise XOR operation, sub-bytes operation, mix-columns and add around key operation. The same process is performed in a reverse way for AES decryption.

Table 2. Proposed hybrid AES and ECC encryption algorithm

Algorithm: Proposed hybrid AES and ECC encryption method Input: random numbers Output: decrypted text

BEGIN Step 1: select randomly an integer from 1 to n-1 Step 2: generate public key Ky' = K*P where d = random number selected between 1 to n-1 ,P is point on curve and d is private key Step 3: find if point P lies on the curve. If yes proceed further. If no error process Step 4: input data to be send of maximum size 16bytes as string s Step 5: perform add-round key operation on string s Step bitwise XOR operation is performed Step 6: perform sub-byte operation on string 16 byte data should be now converted to 4×4 matrix M Step 7: perform shift-rows operation on matrix M i^{th} row is shifted circular right by i columns step 8: perform Mix-columns operation on columns of matrix M. the values of i^{th} column should be added with i step 9: perform add-round key operation on matrix M step 10: encrypt data step 11: perform inv-shift -rows operation on matrix m step 12: perform sub-byte operation on string s step 13: perform add-round key operation on matrix M step 14: output final decrypted data

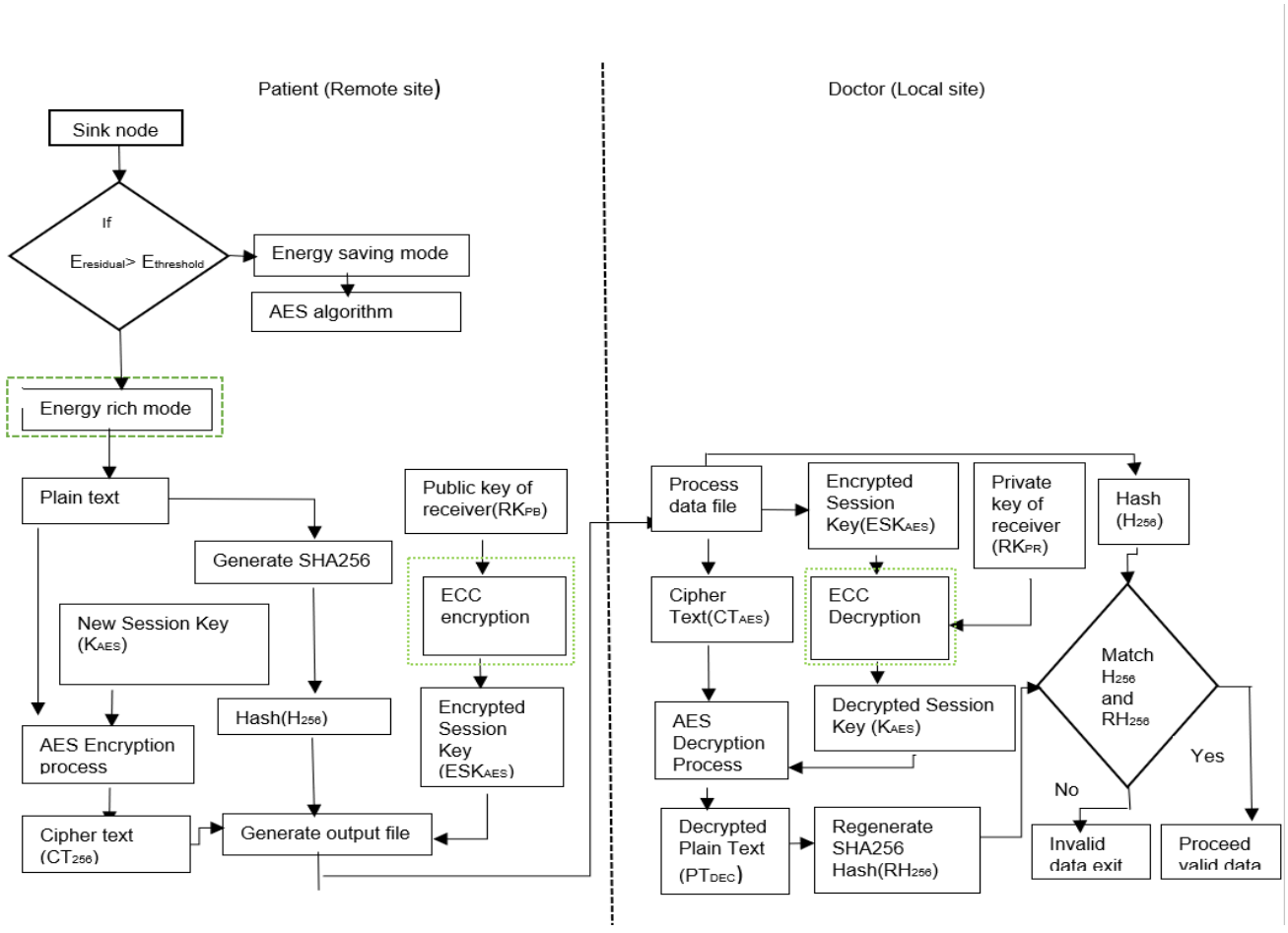

Figure 3. Proposed hybrid algorithm technique for secure data transmission; the contribution of this study is shown in green dotted border

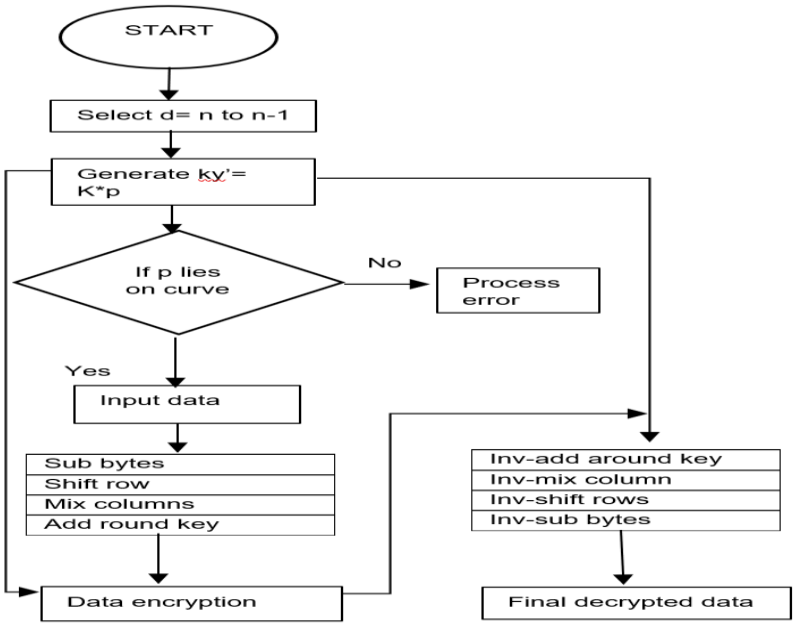

Figure 4. Flowchart of hybrid AES and ECC encryption technique

4. Results

The implementation and simulation of the proposed model were carried out in MATLABR2017b. Equation 6 was used for calculating the size of data encryption by proposed hybrid encryption .10 samples of different data size were used in this process. At first, each sample was encrypted with hybrid AES and ECC encryption technique. The time taken for encryption process was noted and total energy consumed by the algorithm was calculated. The results of the encryption were evaluated and compared to the base of encryption time and size of the file encrypted. As the simulations were carried in MATLAB installed on the personal computer, the processing time is expected to be higher. Also, the amount of energy consumed by each encryption process was measured by using the energy formula as stated in equation 3.

In a real-time scenario, the doctor at the local site receives health-related information from a patient at the remote site. As the connection is open, the sensitive data should be secured from malicious attack. The data is encrypted with AES encryption algorithm and sent to doctor. On the doctor sighed, the cipher text is decrypted to plain data. On-going through the secure transmission process, the doctor advises the patient on their health condition and required medication.

We have compared the result obtained from the encryption process with an existing current best solution for analysis. The size of the data file encrypted, and time required for encryption by our proposed solution was measured from the simulation process. The encryption time is the time used by an encryption process while encrypting the plain text to cipher text. Encryption time has been calculated in milliseconds(ms). The result from this comparison is shown in table 5. As shown on the table below, the data file of different sizes was passed through the state of art solution, i.e. hybrid AES and RSA encryption and size of the file encrypted, the time taken and energy consumed by the process was evaluated. Similarly, the same process was carried out through proposed hybrid AES and ECC algorithm process.

The below table 6 provides a quick and meaningful comparison between the current best solution and the proposed new solution. Both solutions are implemented in real-time data transmission, but the proposed solution provides much efficiency in WBAN. The state of art solution uses hybrid AES and RSA algorithm whereas, in the proposed solution, RSA has been replaced by ECC.

Table 3. Results of various comparison of State of art and proposed solution based on encrypted file size (bytes), time of encryption (ms) and energy consumed(mJ).

No of sample	Data size (Bytes)	State of Art			Proposed Solution		
		Encrypted file size	Time for encryption(ms)	Energy consumption(mJ)	Encrypted file size	Time for encryption(ms)	Energy consumption(mJ)
1	6050	6110	575	23.06994	7562.5	511.75	15.6382
2	8,250	8,263	756	47.66517	10312.5	672.84	38.4355
3	12,015	12,110	988	76.83625	15018.75	879.32	64.4283

4	25,615	25,868	1025	976.7546	32018.75	912.25	897.0571
5	30,184	30,482	1034	1150.98	37730	920.26	1023.3526
6	35,080	35,426	1059	1337.675	43850	942.51	1121.9595
7	45,645	46,095	1585	1740.541	57056.25	1410.65	1560.6371
8	61,386	61,991	3143	2340.779	76732.5	2797.27	2019.9008
9	75,986	76,735	3175	2897.508	94982.5	2825.75	2568.0994
10	92,768	93,450	3124	7022.49	115960	2780.36	6780.731
Average	392,979	39,653	1646.4	4202.63	49,122.38	1465.296	2,815.762

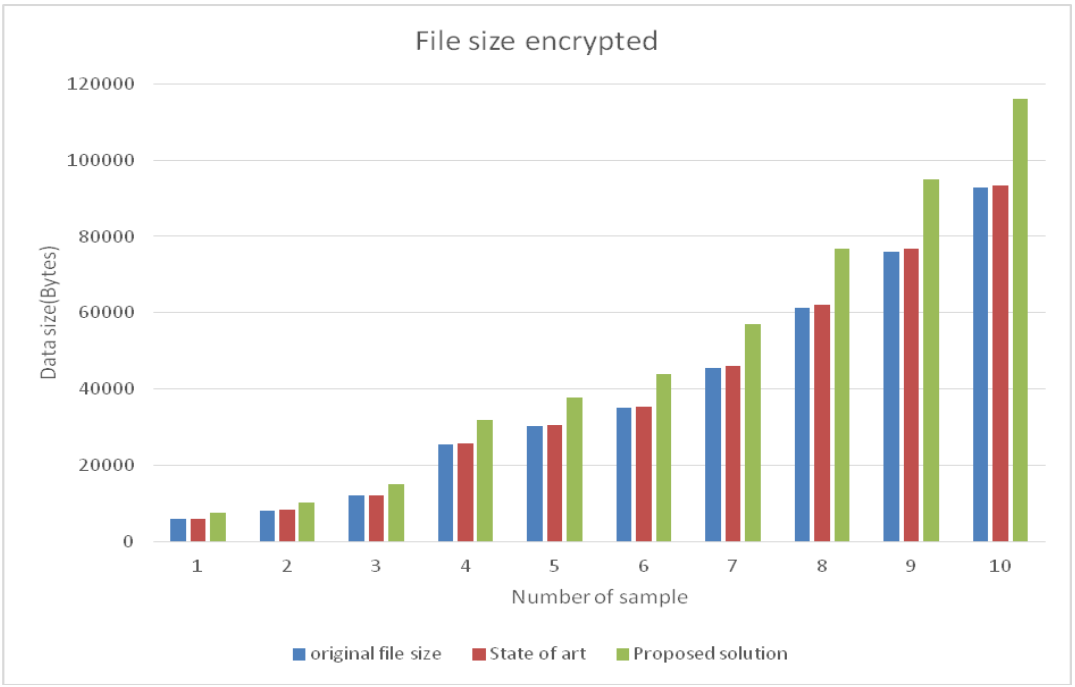

Figure 5. Results of file size encrypted for the State of Art and Proposed solution; blue colour shows original data file size; orange colour shows data file size encrypted by state of art and grey colour shows data file size encrypted by the proposed solution

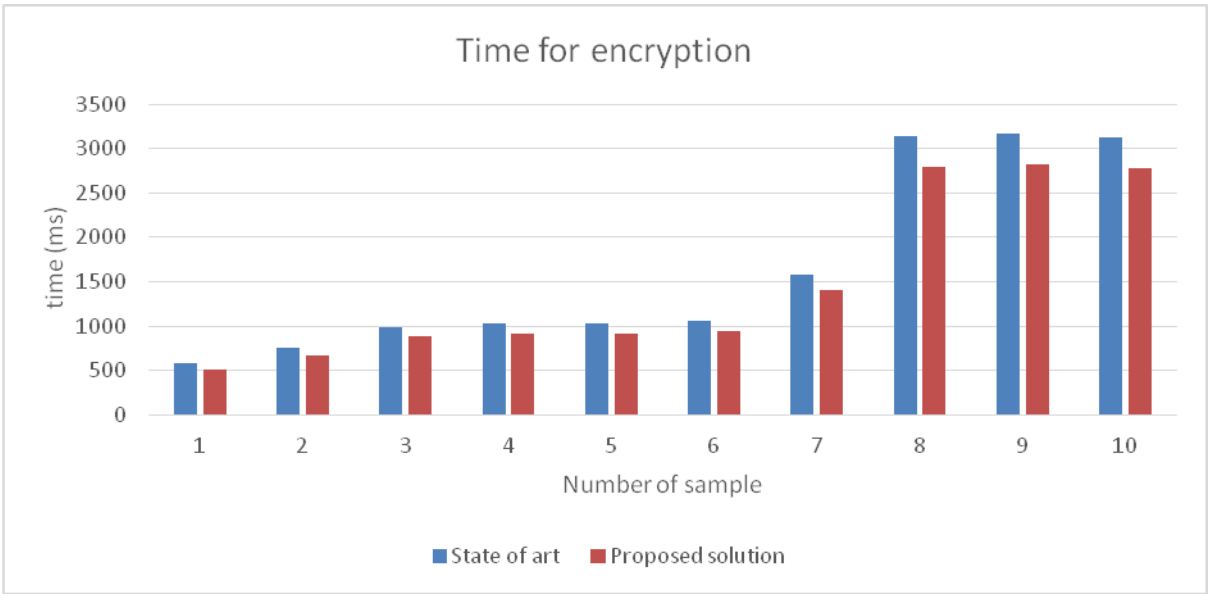

Figure. 6 Results of time taken for encryption of data file; blue colour shows time taken by the State of Art for encrypting original data file and orange colour shows time taken by the Proposed solution for encrypting the original data file

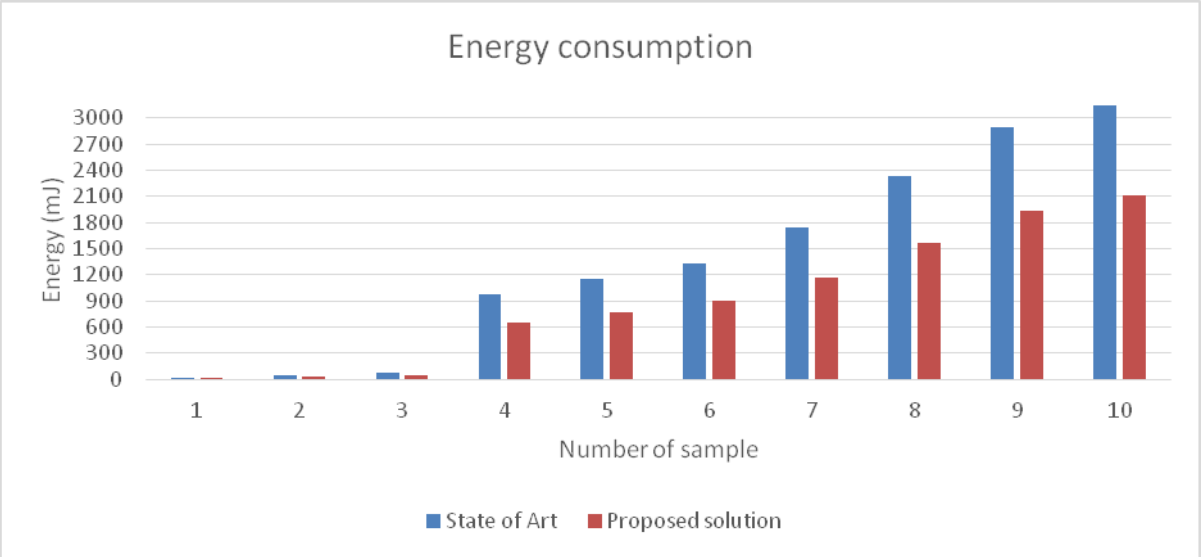

Figure. 7. Results of energy consumed by the State of Art and proposed solution for encrypting data file; blue colour shows energy consumed by state of art and orange colour shows energy consumed by the proposed solution

Table 4. Comparative results of state of art and proposed solution

	State of Art (hybrid AES and RSA algorithm)	The proposed solution (Enhanced hybrid AES and ECC algorithm)
Applied Area	Security of Real-time data transmission	Security of real-time data transmission in WBAN
Features	Provides simple and high-security encryption level	Fast, consumes less energy and provide high data encryption level
Algorithm	Hybrid AES and RSA algorithm	Enhances hybrid AES and ECC algorithm
Equation	Cipher text (C)= (((((P)Bs)Sr)Mc)ky	Enhanced cipher text(EC)= (((((P ⊕ ky')Mr)Mc) ⊕ky')

5. Discussion

The processed sample to the state of art was compared with a processed sample of the proposed solution. The samples were run through the proposed hybrid algorithm and the state of the art solution algorithm. The time run, size of file encrypted and energy consumed was noted. The results obtained from MATLAB will be analyzed from three points that include the size of cipher text, computational time, and energy consumption.

Size of Cipher text - Observing the values shown in table 5, the size of the cipher text created by the proposed hybrid AES and ECC encryption algorithm is more than the size of the cipher text created by the State of Art's solution. The data file sizes are presented in bytes. The proposed system increases the encryption of the data file by more than 19% compared to the State of Art's solution. This is because ECC is more efficient than RSA in securing keys for the encryption process. As the file encrypted is larger than current best solution, the encryption level will be high, which means a highly secured system is offered by the proposed EEHEE algorithm. The comparison of file encrypted size is made in figure 6 and the calculated value of files encrypted is shown in table

Computational Time - It can be observed from table 5 that the encryption time is different for various data file sizes. The reason behind this is the size of file, the cryptographic strength to the system and time taken for generating keys to the process. The average time required to encrypt data file size of 12,015 bytes is about 0.8 second whereas the time used by State of Art's solution is 0.9 seconds. The proposed hybrid AES and ECC are about 11% faster than the state of art solution. The reason behind this is more time is consumed by RSA in the key generation process which is used in State of Art's solution. This shows that the proposed EEHEE system can encryption data file in lesser time as compared to current best solution. This feature is very important in WBAN. The comparison of encryption time is shown in figure 7 and the value obtained is presented in table 5.

Energy Consumption - From table 5, it is seen that the amount of energy consumed is different for different file size, and the difference can be seen in energy consumed by two different systems. This variation is caused by the energy of wearable sensor is utilized by nodes for transmitting data, and the encryption technique uses energy for encrypting data as well. The average amount of energy consumed by the current best solution was 4202.63 mJ whereas our proposed EEHEE consumed only 2815.76 mJ energy during the encryption process. The proposed system has provided a higher level of cryptographic strength than State of art by consuming less energy which the main concern to this work is. The amount of energy consumed has been reduced by almost 34 % in the proposed solution. This is because the proposed encryption system uses ECC algorithm, which is very fast and requires less energy than RSA. This shows that the proposed EEHEE system can energy efficient compared to existing solution. If less energy is used by the algorithm process, the life span of sensor will increase as well. So our proposed system can offer highly secured data transmission system using fewer amounts of energy. The difference of energy consumption is shown in figure 8, and the values obtained are presented in table 5.

6. Conclusion

In this work, a robust hybrid encryption algorithm for WBAN is proposed. This technique is designed to solve various problems that arise in WBAN such as difficulty in practical implementation, high strength of crypto system, short response time and restrained resources such as computational power and energy. The proposed solution has used AES and ECC algorithms to utilize the advantage of dual symmetric and asymmetric encryption techniques. The proposed solution also focuses on reducing the level of energy used by crypto system to increase the battery life of WBAN. The performance of proposed hybrid AES and ECC algorithm is compared to the current best solution. It offers better security for shorter encryption time, which reduces processing overhead and energy consumption. The proposed system encrypts size of the file by more than 19%, are 11% faster and reduces energy consumption by 34% as compared to state of art solution. Therefore, it can be concluded that the proposed system is more energy efficient for securing data transmission between health patient and medical professional in telemedicine. On the future work, the data file sent from patient to doctor should be selected on the basis of criticality so that energy can be saved.

References

[1] K. Pavithradevi, "History and Applications in Body Area Network," *International Journal for Research in Applied Science and Engineering Technology*,167-170, 2017. Doi:10.22214/ijraset.2017.2027

[2] S. Kiah,. (, "Design and Develop a Video Conferencing Framework for Real-Time Telemedicine Applications Using Secure Group-Based Communication Architecture," *Journal of Medical Systems*, 38(133), 133-144, 2014. doi:10.1007/s10916-014-0133-y

[3] J. Kim, H. Lee, J. Yi, & M. Park, "Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks," *Journal of Sensors*, 1-9, 2016. doi:10.1155/2016/2678269

[4] S. Farooq, D. Prashar, & K. Jyoti, "Hybrid Encryption Algorithm in Wireless Body Area Networks (WBAN)," In *Intelligent Communication, Control and Devices* , pp. 401-410, 2018.

[5] D He, S Zeadally, N Kumar, JH Lee, " Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, PP(99):1–12, 2016. doi: 10.1109/JSYST.2016.2544805

[6] E. Salim, & I. Harba, "Secure Data Encryption Through a Combination of AES, RSA, and HMAC," *Engineering, Technology & Applied Science Research*, 7(4), 1781-1785, 2017. Retrieved from http://web.a.ebscohost.com.ezproxy.csu.edu.au/ehost/pdfviewer/pdfviewer?vid=5&sid=f721265d-6d29-48d6-ae94-d97cb1de8883%40sessionmgr4009

[7] C. L. Priya, & U. S. Visalakshi, ," Secure and Efficient Communication Using ECC Algorithm in Wireless Body Area Network," *International Journal of Engineering Science*, 10073, 2017.

[8] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, & X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems," *Journal of medical systems*, *39*(11), 140, 2015.

[9] Z. Hercigonja, " Comparative Analysis of Cryptographic Algorithms," *International Journal of Digital Technology & Economy*, *1*(2), 127-134, 2016.

[10] J. Liu, Z. Zhang, X. Chen, & K. S. Kwak, " Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, *25*(2), 332-342, 2014.

[11] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics and Security*, *9*(12), 2327-2339, 2014.

[12] Z. Zhao, " An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *Journal of medical systems*, *38*(2), 13, 2014.

[13] M. Hussain, Q. Du1, L. Sun, & P. Ren, " Security enhancement for video transmission via noise aggregation in immersive systems," *Multimedia Tools and Applications*, 75(9), 5345-5357, 2016. doi:10.1107/s11042-015-2936-3

[14] M. Tiwari, S. S. Panda, & G. Biswas, " An Improved Secure Remote Login Protocol with three-factor authentication," The Institute of Electrical and Electronics Engineers, 372-378, 2016. doi:978-1-4799-8579-1/16/$31.00

[15] T. Hayajneh, S. Ullah, B. J. Mohd, & K. S. Balagani, " An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications," *IEEE SYSTEMS JOURNAL*, 11(4), 2536- 2545, 2017. doi:10.1109/JSYST.2015.2424702

[16] K. S. Raja, & U. Kiruthika, "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks using RelAODV," *Wireless Personal Communications*, *83*(4), 2975-2997, 2015. doi: 10.1007/s11277-015-2577-x

[17] N., Kumar, ," A Secure Communication Wireless Sensor Networks Through Hybrid (AES+ECC) Algorithm," vol. 386, 2012. von LAP LAMBERTAcademic Publishing.

[18] R. A. Khan, K. H. Mohammadani, A. A. Soomro, J., Hussain, S., Khan, T. H. Arain, & H. Zafar, " An Energy Efficient Routing Protocol for Wireless Body Area Sensor Networks," *Wireless Personal Communications*, 99 (4),1443-1454, 2018. Doi: 10.1007/s11277-018-5285-5

[19] A. A. Omala, K. P. Kibiwott, & F. Li, " An efficient remote authentication scheme for wireless body area

network," *Journal of medical systems*, *41*(2), 25, 2017.doi 10.1007/s10916-016-0670-7

[20] Z. Adelani , G. Mirjalily , and M. H. Mirzaei, "Balanced Multi-Channel Data Collection in Wireless Sensor Networks," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No. 1, pp. 10-18, 2018

[21] J. Jusak , S. S. Mahmoud, "A Novel and Low Processing Time ECG Security Method Suitable for Sensor Node Platforms," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 10, No. 1, pp. 213-222, 2018

[22] Omar Achbarou, My Ahmed El Kiram, Outmane Bourkoukou, Salim Elbouanani, "A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment," Vol. 10, No. 3, pp. 526-533 , 2018.

[23] S. D. Putra, A. S. Ahmad, S. Sutikno, Y. Kurniawan, " Attacking AES-Masking Encryption Device with Correlation Power Analysis," Vol. 10, No. 2, pp. 397-402, 2018 .

[24] M. M. Rahman, T. K. Saha, & M. A. A. Bhuiyan, " Implementation of RSA algorithm for speech data encryption and decryption," *International Journal of Computer Science and Network Security (IJCSNS)*, *12*(3), 74, 2012.