IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 15, 2020, accepted September 26, 2020, date of publication October 5, 2020, date of current version October 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3028686

A Lightweight Genetic Based Algorithm for Data Security in Wireless Body Area Networks

TALLAT JABEEN[1], HUMAIRA ASHRAF[1], ASMA KHATOON[1], SHAHAB S. BAND[2,3], AND AMIR MOSAVI[4,5,6]

[1]Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan
[2]Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
[3]Future Technology Research Center, College of Future, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan, R.O.C.
[4]Kando Kalman Faculty of Electrical Engineering, Institute of Automation, Obuda University, 1034 Budapest, Hungary
[5]Faculty of Civil Engineering, Technische Universität Dresden, 01069 Dresden, Germany
[6]School of Economics and Business, Norwegian University of Life Sciences, 1430 As, Norway

Corresponding authors: Humaira Ashraf (humaira.ashraf@iiu.edu.pk), Shahab S. Band (shamshirbandshahaboddin@duytan.edu.vn), and Amir Mosavi (amir.mosavi@kvk.uni-obuda.hu)

This work was supported in part by the Hungarian-Mexican Bilateral Scientific and Technological Project under Grant 2019-2.1.11-TÉT-2019-00007, in part by the New Szechenyi Plan under Grant EFOP-3.6.2-16-2017-00016, and in part by the European Union and the European Social Fund.

ABSTRACT The new generation of wireless body area networks (WBAN) for the internet of things (IoT) is emerging in a fast-paced. Today patients can be tested using remote clinical nanosensors. WBAN involves small interconnected sensors for the collection of ongoing medical data and transmitted through the networks for further processing. However, the protection of healthcare data is very important and difficult because of the various active and passive numbers of attacks. Although there exist several literatures on data security techniques such as digital signatures, Elliptic curve cryptography, and Advanced Encryption Standards (AES) they contain stumbling blocks for the security methodologies. Thus, in this paper, a novel data protection genetic-based encryption scheme is proposed for higher performance.

INDEX TERMS Wireless body area networks, WBAN security, genetic-based algorithm, cryptography, healthcare data security, man-in-middle attack, Internet of Nano Things, IoT.

I. INTRODUCTION

The phenomenal success of information and communication technology has lifted human life [1]. WBAN is a powerful advancement in IoT. The Internet of nano things implies to the group of nanosensors that monitor and record the data from the environment [2]. WBAN comprise of small tiny sensors nodes that are placed in the human body to record patient's healthcare data. This data may relate to human ECG, body temperature, sugar level, or blood pressure [3]. There are two layers in WBAN, Intra WBAN and beyond WBAN. Intra layer consists of nanosensors that are wearable to the human body and record health data. Beyond WBAN contains a wireless channel that provides a connection between gateway and server [4]. Healthcare data further routed towards biomedical servers through a wireless channel as shown in figure 1.

The associate editor coordinating the review of this manuscript and approving it for publication was Lorenzo Mucchi.

Data security is very important while sharing the patient's data over a public wireless network where attackers can easily misuse or modify the readings [5]. Consequently, there is vastly needed a security plan for smooth transmission of data. Multiple encryption techniques are proposed in the literature for data security like digital signatures, AES, ECC etc. This paper proposed a novel lightweight genetic based encryption algorithm for the data security of patient's health. The genetic-based algorithm has less computational time complexity and cost-effective as compared to the literature techniques. This scheme also presents a new key generation algorithm that has fewer steps and very less computations [6]. Genetic based lightweight encryption algorithm implemented over the nano sensor devices after generating the patient's data. Then encrypted data is forwarded towards the collector which further transmits it over a wireless network [7]. The proposed encryption algorithm takes 8-bit plaintext and converts it into binary values. All other associated operations of algorithms are performed on the binary generated data.

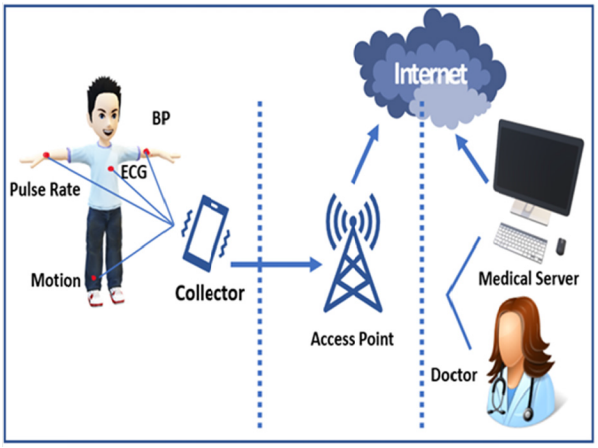

FIGURE 1. WBAN Architecture that collects data from nano sensors and transfers towards medical server through a wireless channel.

These operations involve Mutation T, crossovers substitution box, amino acid table, and string mapping that produces ciphertext. The complete procedure of performing these operations for encrypting data is given in section III.

This encrypted data is further processed towards the biomedical server through a wireless channel, and the protocol used in this paper is MQTT protocol. Message Queuing Telemetry Transfer (MQTT) protocol is very lightweight as compared to HTTP and ensures data availability. A combination of lightweight genetic-based algorithm and MQTT protocol is a very productive system as both have significantly less amount of energy consumption.

A. MOTIVATIONS

The motivation of this study can be summarized in several bullet points as follows.

- To elucidate current trends in the internet of nano things.
- Motivate to transfer secured encrypted data over the reliable lightweight channel.
- Motivate to encrypt WBAN's data efficiently concerning cost, time, and sensors' memory range.

B. CONTRIBUTIONS

This paper contributes by presenting the current state of augmenting data security in WBAN, focusing on the data security scheme in WBAN to investigate methodologies on avoiding various attacks. Accordingly, the contribution of this study can be described in several bullet points as follows.

- Developing a novel taxonomy that covers the security encryption techniques that are needed for WBAN. Existing research has been addressed in depth to support the proposed study.
- All state of the work art has
- To provide a lightweight encryption technique with a lightweight key generation process to maintain smooth data transmission over the WBAN network.
- Finally, a lightweight encryption scheme with the lightweight protocol is proposed for the efficient transmission.

C. NOVELTY

The unique points of the proposed paper are as follows,

- A novel genetic-based encryption algorithm is proposed with the lightweight key generation steps.
- A combination of lightweight genetic-based encryption with the lightweight protocol is implemented.
- To elucidate the recent trends in the data security of nano sensors in the WBAN environment.
- The goal is to provide a protocol, which is bandwidth-efficient and uses little battery power.

D. ORGANIZATION

The rest of the paper is organized as follows. Section I discuss the introduction; Section II explains the literature of the WBAN and protocol. Section III provides Methodologies, and Section IV, and V gives evaluations/Conclusion.

II. LITERATURE REVIEW

Security is currently one of the most important concerns for telecommunications due to the widespread of deployed wireless networks. One of the key problems in the field of ensuring the wireless exchange of information is the initially shared awareness between source and destination. So, various encryption techniques are used in literature to secure the data. Author Anwar *et al.* proposed safe hashing algorithms along with encryption techniques that are used to make data transmission more efficient and powerful. Digital signatures are created by a hash procedure to transport patient data more safely and authentically. This proposed algorithm used the Asymmetric key generation approach that requires pairs of public and private keys, making the algorithms slower and highly complex [1].

Advances in medical science and technology have brought together modern Patient Monitoring System (PMS) activated by the wireless body area network which provides a simple, effective, and unparalleled revolution health facilities. WBAN used nano sensors to collect patient's data and transmit it on the way to the hospital server through a wireless network. Privacy and protection of data is an important concern for the patients and doctor. Consequently, the author Fahim Shahriar Chowdhury et all used data encryption to secure from eavesdropper and authenticate to ensure the legitimate user [2].

The literature technique used end to end secured monitoring transportation system and encrypt data with lightweight version AES (Advanced Encryption Standards). Then encrypted data is transported over MQTT protocol in the direction of the hospital server. This scenario resulted into a simple and effective system. Various protocols were used in the literature for the transmission of data. The author Shahwar *et al.* used LEACH protocol in the proposed study and lightweight encryption algorithm which transfers data on wireless sensor networks efficiently [3] and Savita Sindhu *et al.* used CSMA/CA and TDMA protocol for routing [10].

Wearable sensor nodes are mostly implemented inside a wearable body area network (WBAN) to record data of

physiological signals, such as the heart rate (HR), respiration rate (RR), electrocardiography (ECG), body temperature, body position, and blood pressure (BP). Security and privacy are the most important issue over a public wireless channel. Therefore, author Fan Wu et all, used a hybrid wearable sensor network system to upgrade the health safety of workers in the construction industry [4]. There are mainly two networks are proposed in the paper to make system hybrid, one is local environment LPWAN and WBAN second cloud connecting IoT network. IoT network system used MQTT protocol for the transmission of data towards the biomedical server.

The internet of things (IoT) is gaining rapid prominence due to its ability to bring about a global digital transition and is increasingly being used in manufacturing, transportation, digital health, and farming. IoT brings several research challenges with various implementations, including the appropriate infrastructure for control and communication between devices. WBAN field communicates sensors with a medical server via a wireless channel. The author Adil Bashir et all used a lightweight encryption algorithm with MQTT protocol [5]. There are used three phases for security schemes which are key generation, encryption, and publish through MQTT and decryption. Publisher sensed data is encrypted by the generated key and will transfer towards MQTT broker. Publishers must have to send a ping message request to the broker, indicating that it has some data to be forwarded towards the medical server and the broker will respond with the system ID to the publisher for transmission of data. Then the encrypted data packet will be transferred from the publisher to the broker towards subscriber or medical server in the WBAN environment.

Author Marva BOUMAIZ *et al.* intends to investigate the impact of an adjacent BAN 's existence, when it transmits power differs, on a reference BAN's output through simulation. Both the CM3A path loss model, defined in the IEEE 802.15.6 standard for the 2.4 GHz on-body medium, and the temporal variation phenomenon, are being considered. Evaluation of output is performed in terms of the rate of packet loss (PLR) [6]. The author Saiyma Fatima Raza *et al.* suggests a new approach to data protection especially during emergencies in a wireless network.

WBAN uses passive Encryption Standard-128 (AES-128) cipher requiring considerable time for encryption which can be fatal in emergencies. Due to the region and resource constraints, the sensor node protection mechanism should be lightweight. The suggested approach uses chaos-based scrambling in emergencies, which is Lightweight concerning AES, and much less processing time is needed in emergencies [7]. Many security standards are inevitable in WBAN, such as data confidentiality, data quality, data accessibility, data authentication, accessibility, access control, transparency, non-repudiation, etc. [8]. Two security suits are presented in the proposed study in the study of Agha *et al.* [9]. The first security suit focused on KBS key management with Hashing and the second called KAISC suit for communication between sensors as key management scheme. The requirement to have two separate procedures, one for transmission of data to the base station and one for intersensory communication, is to improve safety. WBAN is an advanced technology that employed nano sensors into the human body and accumulates health-related data. The transportation of data needs security schemes to avoids attackers. Such cryptographic mechanisms are based on the use of well-managed cryptographic keys (generation and distribution) to make security robust enough [11]. The author Marko Kompara *et al.* used efficient mutual authentication and key agreement technique for security in the proposed study of WBAN [12]. Two new protocols have been proposed by author Peyman Dodangeh to exchange the key between the sensor nodes with the watch and the mobile node in a two-tier WBAN topology and to achieve mutual authentication. The proposed protocols for inter and intra BAN sections require secure authentication of other nodes by one node, biosensors, the watch, the mobile node, and the medical server.

The two protocols suggested using operations for a hash function, concatenation, XOR, and cryptography [13]. WBAN is not only used in medical applications but also switched into military uses, sports, education, and for the safety of human lives. WBAN has become a leading research field and development which offers enormous potential for improvement in health services [14]. Another quantized stream encryption scheme for WBANs based on logistic mapping is proposed. Meanwhile, Power Spectral Entropy (PSD)and Peak to Average Power Ratio (PAPR) analysis of quantized chaotic sequences were performed to determine the chaotic characteristic between different quantization precision to overcome the ineffectiveness of the Lyapunov factor in quantized systems [15]. Therefore, a security framework is required to protect the overall IoT system against unauthorized entities [16]. Efficient and simple key generation algorithms support the encryption scheme so, using the physiological signal, Aneesh M. Koya *et al.* proposed a hybrid anonymous authentication and key agreement scheme [17]. The fully homomorphic encryption algorithm to incorporate safe channel communication between the data sink and third-party access and methods for enhancing the monitoring of healthcare in the telecommunications system using implantable tools that do not impact patient mobility [8].

Lightweight Encryption Algorithm (LEA) is the most appropriate for WBAN settings were the devices used (sensors and mobile devices) have limited memory space and low processing power is very low compared to traditional algorithms for encryption [19]. The scheme adopts the concept of hybrid encryption to reduce data encryption's computational overhead, that is, to use the symmetric key to encrypt data to ensure performance, and to use the CP-ABE method to encrypt the symmetric key for protection. [20].

This contribution is about proposing a new modulation technique to ensure safe communication in a completely wireless environment. At the physical layer, the information is applied by the thermal noise produced in connection between two terminals. A loop scheme is designed to

recover the shared knowledge especially. The probability of error/detection for the lawful users and the third undesirable listener (passive or active attacker) is analytically determined [21]. Author Simone Soderi *et al.* suggests a watermark-based, blind physical layer protection using a jamming receiver in combination with the watermarking technique of the spread spectrum. The likelihood of loss of the secrecy power is determined analytically, regardless of the location of the eavesdropper. The theoretical analysis lets us draw a safe zone around the valid receiver. Results indicate how the protection of the watermark based blind physical layer aims to be a valuable technique for the implementation of physical layer health [22]. The rapid change in technology results in WBAN into a smart healthcare system and the confidentiality of the encrypted data remain challenging over a wireless network. Multiple techniques of data transmission are presented to secure the data. The author used a software-defined networking layout and authentication protocol known as Kerberos protocol [23].

Another technique is used to secure physical layer data transmission by using a multi-hop topology formation game algorithm without any key requirement [24]. To encrypt or decrypt the patient's data the PRESENT based cipher implementation focused on the block ciphers that use 64 block text and 128 bits key [25]. WBAN requires lightweight and effective data transmission services over the network [26]. Many techniques are proposed for security, a group-based collaboration on the development of symmetric key through the collection of data from the physical or link-layer obtained signal strength indicator (RSSI) is also focused. HEA is used for encryption and decryption to secure the data over the WBAN environment along with the authentication process and the Diffie-Hellman algorithm is used for the key exchange phase [27].

The scheme is based on the Jules and Sudan (JS) algorithm. According to JS algorithms two communicating parties must lock in polynomial value [28].

The homomorphic encryption method is used to secure the sensitive data of the patients in 18 bytes text blocks. This encryption method performs specific computations on the plaintext and the ciphertext is generated [29].

III. PROPOSED METHODOLOGY

In this section, the system architecture of WBAN with MQTT protocol is presented. Nano sensors are involved in the body area networks that generate patient data and transfer it towards MQTT broker while MQTT is the publish-subscribe messaging protocol. MQTT broker forwards the encrypted data towards the internet cloud which is connected to the medical server. The medical server used to store and retained as health critical data must be secured unconditionally.

A. DATA ENCRYPTION AND DECRYPTION PROCESS

A lightweight genetic-based encryption algorithm is presented to secure the patient's data over WBAN. After sensing the patient's health data, the proposed encryption algorithm is implemented to convert the data into ciphertext over sensor devices. Encrypted data transmits towards the collector through Bluetooth, and the collector will further transfer it over the network towards the medical server. This encryption scheme uses fewer steps which makes the algorithm simple and efficient. The key generation algorithm is also using very simple mathematical operations that generate 8 bits of a key which later used in the genetic encryption algorithm. Then encrypted data is transferred in the direction of the cloud server through a message queuing telemetry transfer protocol. The genetic-based algorithm takes 8 bits of plaintext as patients' data is in the form of decimal numbers and then convert this text into binary numbers. After the conversion of binary performs exclusive or (XOR) with the key generated by a simple step. Key generation is performed by taking a random integer and convert that integer into the binary. Then perform 1's complement over the generated binary bits. After this step do circular two shifts right and now the generated binaries will act as a key in the genetic algorithm

TABLE 1. Mutation t exchange values in array index.

Mutation T							
0	1	2	3	4	5	6	7
5	7	1	4	6	0	3	2

This key performs XOR with the 8-bit binaries of the patient's data, then mutation T replacement is carried out on index values of an array to make data in an incomprehensible form from table 1. Now, 8 bits of data are divided into four bits each for crossover operation. In crossover exchange of right side of four bits into the left side and left side of four bits into the right side is positioned. The generated data will perform the next step of S-box values that took the first two bits of the left side as rows and first two bits of the right side as columns respectively from table 2. Then the generated alphabets values from the s-box will obtain their substitution code from amino acid table 3 and the produced code performs string mapping like '0' mapped with 'A' and '1' mapped with 'B'. The obtained combination of 'As' and 'String is calculated ciphertext from a genetic algorithm.

Table 1 shows the mutation T values that are used in the genetic-based encryption algorithm for swapping binaries of temporarily generated ciphertext. These values used an array index of '0' to '7' for 8-bits of values to swap according to the assigned values on that index. All the 8-bits binaries are shuffled with their corresponding index values. E.g. binary value at index 1 will shuffle the binary value of index 7 while decrypting the binary data at index 7 will replace with the binary of index 1 value.

Table 2 presents substitution values for resultant binary generated data after performing crossover which gives two subsets (4-bits each) of 8-bits data used s-box. The values of

TABLE 2. S-box values for replacing data.

S-box	00	10	11	01
00	T	E	Y	A
10	N	U	H	C
11	I	S	R	B
01	G	K	F	M

TABLE 3. Amino acid code values for substitution.

Amino Acid	Code
T	0000
E	0001
Y	0010
A	0011
N	0100
U	0101
H	0110
I	0111
S	1000
R	1001
C	1010
B	1011
G	1100
K	1101
F	1110
M	1111

the s-box are substituted by the following pair of first 2-bits as rows and second 2-bits as columns of the first subset. The same process is for the second subset of data. S-box contains rows and columns of binary pairs and the value that are being substituted from the table are in alphabetic form to make temporary cipher. S-box generating 1 resultant alphabets against one subset of 4-bits. Likewise, 1 alphabet resultant of second 4-bits. Therefore, the s-box provides a temporary cipher of two alphabets.

Table 3 contains amino acid codes for the S-box generated alphabets. Amino acid table assigned some specific codes of binaries to the specific alphabets which are near to cipher-text. Every alphabet assigned 4-bits of binaries, so the s-box resultant two alphabets replaced with the Amino acid 4-bits binary to make 8-bits data again.

Table 4 demonstrated the step by step procedure of genetic-based encryption algorithm writeup. Firstly, the algorithm will calculate the key by performing key generation steps. Secondly, apply genetic-based encryption algorithm layers from step 1 to step 10 to produce ciphertext.

TABLE 4. Genetic based encryption and decryption algorithm write-up with key generation steps.

Key Generation:

Setup of nodes, base station
Select any integer value.
Convert into binary
Perform 1's complement
Circular 2 shifts right which is key value

Encryption:

Step 1: Plaintext of 8-bit size

Step 2: Convert ϵ into binary values

Step 3: $temp_{\epsilon'} = \overline{Key \oplus \epsilon}$ (take XOR with key generated above with plaintext)

Step 4: $temp2_{\epsilon'}$ = Mutation T

Step 5: $temp3_{\epsilon'} = \frac{temp2_{\epsilon'}(Lenght)}{2}$ (two subsets)

Step 6: $temp3\epsilon'$ = Crossover (L-R & R-L)

Step 7: $temp4\epsilon' = Sbox$

Step 8: $temp5\epsilon' = Amino\ Acid$

Step 9: $temp6\epsilon' = String\ Mapping$

Step 10: $temp6\epsilon'$ = Ciphertext

Decryption:

Conversion of ciphertext into plaintext:

Step 1: ϵ' in Characters

Step 2: Convert ϵ' into binary values (A as '0' and B as '1')

Step 3: $temp\epsilon' = Amino\ Acid$

Step 4: $temp1\epsilon' = Sbox$

Step 5: $temp2\epsilon' = Crossover$[Set1 = 1 to $\frac{n}{2}$ and Set2 = $\frac{n}{2}$ - n, where n is data(length)] (R-L & L-R)

Step 6: $temp3_{\epsilon} = Mutation\ T$

Step 7: $temp4_{\epsilon'} = \overline{Key \oplus \epsilon}$

Step 8: $temp4_{\epsilon'} = Plaintext$

Symbol ϵ presentsZ the data which is being converted into binary values. Temp is a temporary data saving variable that is updated by performing each step of encryption or decryption. Step 3 of encryption algorithm will perform XOR operation between plaintext binary and the generated key binary. Step 4 performs mutation T from table 1 and step 5 divides the 8-bits data into two subsets containing 4-bits each. Crossover is being performed at step 6 and s-box values are substituted at the next phase 7. Resultant data from step 7 is then replaced with the amino acid coding binaries from table 3 at step 8. Then the string mapping was performed by the substitution of A's and B's with 0's and 1's respectively. Step 9 generated data is the ciphertext at step 10. Thirdly, the generated ciphertext has converted into the plaintext by performing decryption steps. All the encryption steps are performed backward to decrypt or recover the plaintext.

B. MATHMETICAL MODELLING OF GENETIC ALGORITHM

$$Z = y \oplus k \tag{1}$$

Z is the provisional based data that is updated according to the working of operations and y is the plaintext which is calculating XOR operation with the k value of a generated key.

$$Z_1 = M.T \tag{2}$$

Equation 2 performed mutation values assigned to the indexes of the data array accordingly from the table.

$$Z_2 = Z_1\dot{C}1 \rightarrow Z_1\dot{C}2 \tag{3}$$

Z_1^{c1} and Z_1^{c2} denoting four bits each form the total 8-bits of data which is equal to Z_2.

$$Z_3 = Z_1\dot{C}2 \rightarrow Z_1\dot{C}1 \tag{4}$$

The next step of equation 4 present that after dividing two halves of the data, crossover operation is performed. The right-side half values are swapped with left side which is equal to Z_3.

$$Z_4 = Z_3 \rightarrow S_{box} \tag{5}$$

S-box values are substituted over the Z_3 which is short term generated cipher and assigned to Z_4. Now,

$$Z_5 = Z_4 \rightarrow Amino_{Acid} \tag{6}$$

substitute amino acid coding values over the Z_4 generated data which will equal to Z_5.

$$Z_6 = Z_5 \rightarrow String_{Mapping} \tag{7}$$

At last, is done with the rule of '0' as 'A' and '1' as 'B' and the generated strings of A's and B's is ciphertext which is equals to Z_6.

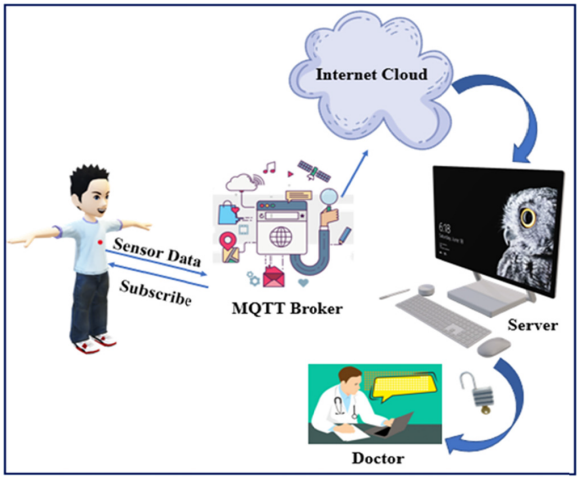

FIGURE 2. shows the architecture of WBAN with MQTT Protocol.

C. WBAN DATA ROUTING WITH MQTT PROTOCOL

Patients data generated from sensors are transmitted towards MQTT broker to request for the publishing of data over the network. Then MQTT broker responds with a subscribe message to the sensor. After subscription of data topic, encrypted data is transferred towards internet clouds on the networks. Now internet cloud will transfer encrypted data to the biomedical server which is accessible to the doctor for the required actions. Figure 2 demonstrated the routing scenario of genetic-based encrypted data from a patient sensor to the medical server and doctor.

Figure 4 shows the actual working of the routing protocol with WBAN's sensor data. Sensors are wearable devices that are placed in the human body which monitors patients' real time health status and the recorded data is further encrypted with the genetic-based encryption algorithm. All the procedure step by step procedure of genetic-based algorithm is described in table 4. Then the encrypted data is sent for publish to the MQTT broker and the broker responds with a subscription of generated data. Then encrypted data is subscribed with the topic of the transmitted data over the network and the decryption process of the received data are being done which is finally received to the biomedical server for further processing from the doctor.

IV. RESULTS AND ANALYSIS

The proposed methodology is tested over the MATLAB environment. A genetic-based encryption algorithm is implemented on WBAN's sensor environment to check the efficiency of the proposed encryption scheme. Experimental results are computed with respect to encryption and decryption time taken by the algorithm.

A. COMPUTATIONAL TIME

Computational time is the cumulative amount of time an algorithm takes to complete an amount of computation. The computational time is a vital performance parameter for an encryption approach that shows how many times is taken by a specific operation to perform during one protocol transaction.

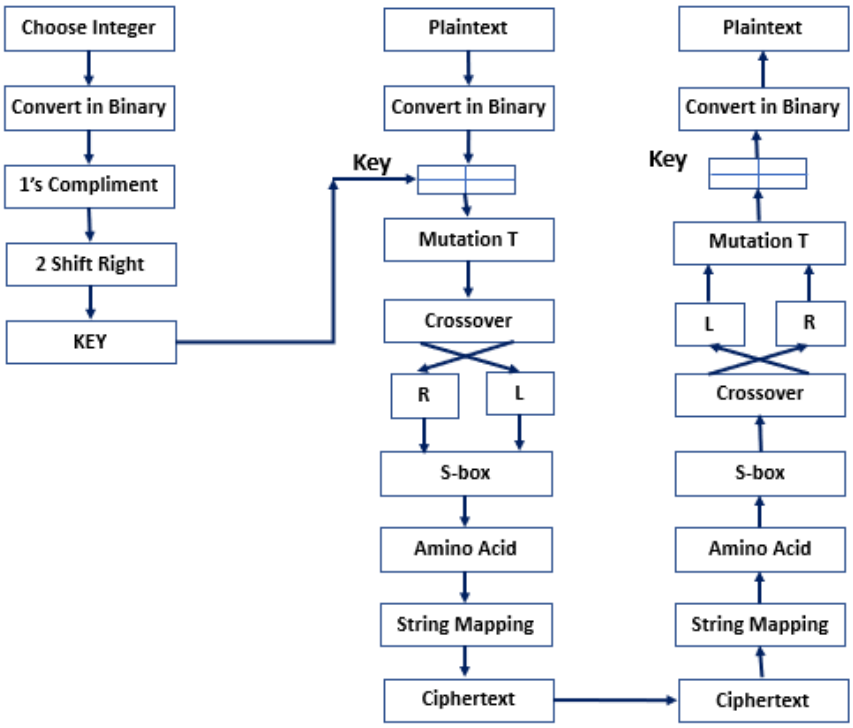

FIGURE 3. Encryption and Decryption phases along with key generation procedure.

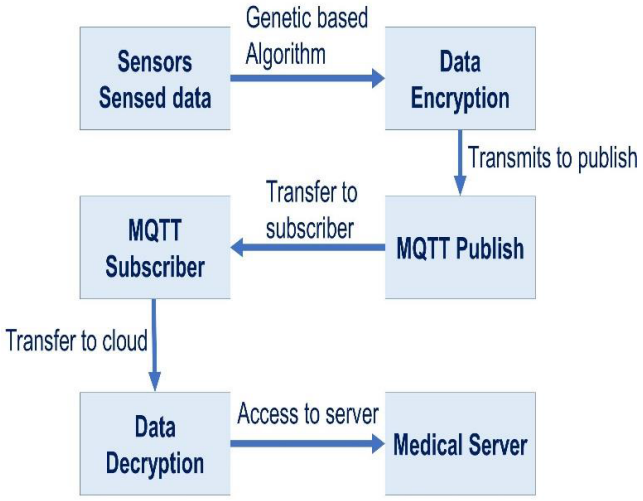

FIGURE 4. MQTT routing protocol strategy with WBAN's encrypted data transmission.

The time complexity of the key generation algorithm is analyzed by implementing the algorithm and it is notified that the time complexity of the proposed algorithm is as low as the procedure of key generation is simple.

Figure 5 demonstrated that as the data bytes increased the time in millisecond for key generation is also increased but the overall time complexity is very low.

B. COMPUTATIONAL TIME OF ENCRYPTION ALGORITHM

The time complexity of genetic-based encryption algorithm is shown in figure 6 which is elaborating the data bytes and encryption time accordingly.

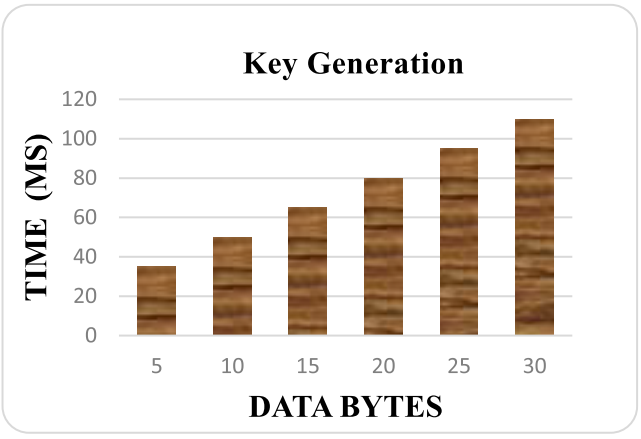

FIGURE 5. The time complexity of the key generation algorithm.

Figure 6 shows the time complexity with the comparison of input data given to the genetic-based encryption algorithm and it is notified that the algorithm taking time for conversion of plaintext into ciphertext is as low as the algorithm steps are simple and effective.

C. COMPUTATIONAL TIME OF DECRYPTION ALGORITHM

Time taken in conversion of a genetic based algorithm's ciphertext into back in its plaintext position is also analyzed. Figure 7 described the input data values and the time is taken values which are as less the time at the level of encryption.

D. COMPARISON ANALYSIS OF KEY GENERATION ALGORITHM

A key generation algorithm based on the simple steps is proposed in this study which has less computational time

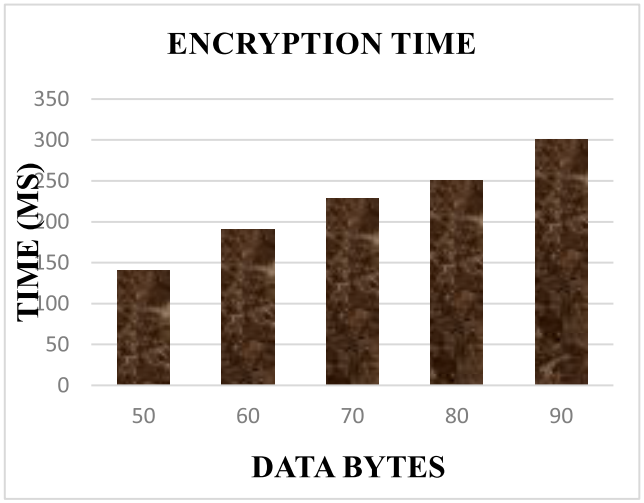

FIGURE 6. The time complexity of the encryption algorithm.

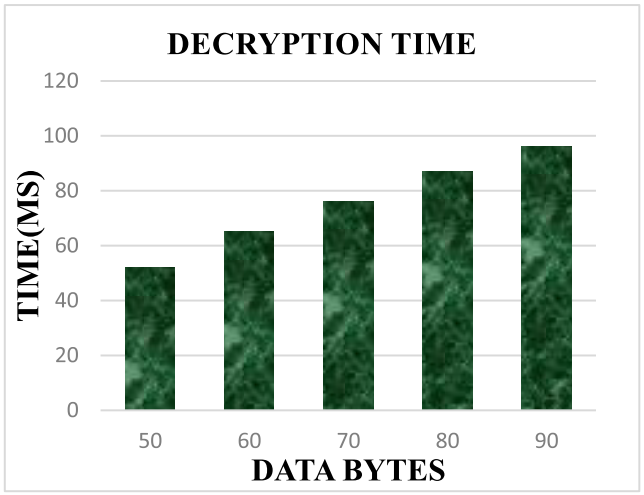

FIGURE 7. Time complexity of decryption algorithm.

as compared to the literary techniques. Shahwar *et al.* used a modified version of the Diffie-Hellman algorithm [1], by comparing with the proposed scheme the results are in figure 8.

E. COMPARISON ANALYSIS OF ENCRYPTION AND DECRYPTION ALGORITHM

Encryption and decryption time of the various techniques are compared with the proposed genetic-based algorithm. Figure 10 illustrates that the proposed algorithm takes less time to encrypt and decrypt data as compared to the other techniques. Decryption time of the multiple schemes is tested where the proposed genetic-based algorithm has less time complexity as compared to other schemes for decryption of data. Time of AES [2] and ECC [30] with proposed genetic based algorithm is observed, and it is noted that AES is taking more time and have high computations and genetic based algorithm have less computations.

F. COMPARISON ANALYSIS OF MQTT PROTOCOL

MQTT is a very efficient and lightweight protocol for routing sensors data which ensures the confidentiality and availability

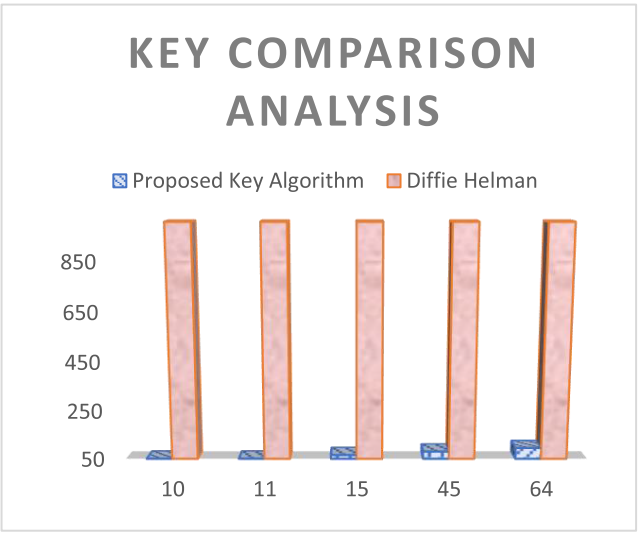

FIGURE 8. Time complexity comparison analysis of the key generation algorithm.

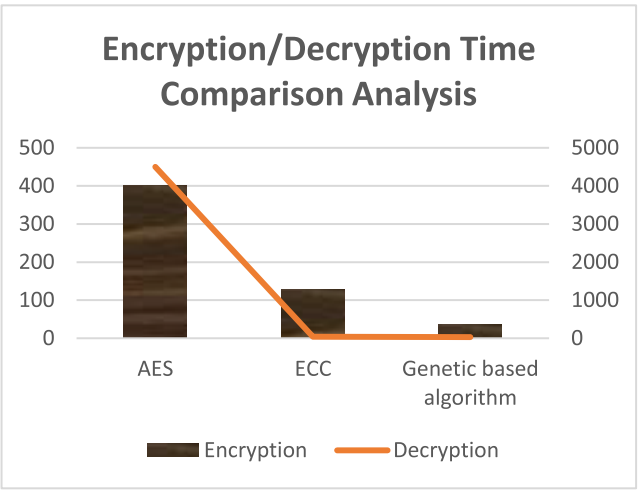

FIGURE 9. Time complexity comparison analysis of encryption and decryption algorithm.

of data. MQTT protocol strictly avoids the man-in-middle attack, collision attack, and flows the encrypted data towards the server. The author Shahwar *et al.* used Low energy adapted cluster-based protocol (LEACH) in the proposed study [3]. LEACH is lightweight and works with the cluster heads' sensors node. In comparison with LEACH protocol, the proposed MQTT protocol is very secure and lightweight because of its built-in feature of authenticity [2].

V. SECURITY ANALYSIS

Some steps are being taken to protect the data from various attacks. It is therefore very important to take security of data transmission because of attacks the routing data on the network may be affected.

A. MAN-IN-MIDDLE ATTACK

In the whole system, the sender, the receiver and the Man-in - Middle (the attacker) are mainly involved. Figure 10 states that Man-in-Middle interrupts the smooth transmission

FIGURE 10. A man-in-middle attack disturbs the smooth transmission of data and secretly get the original data.

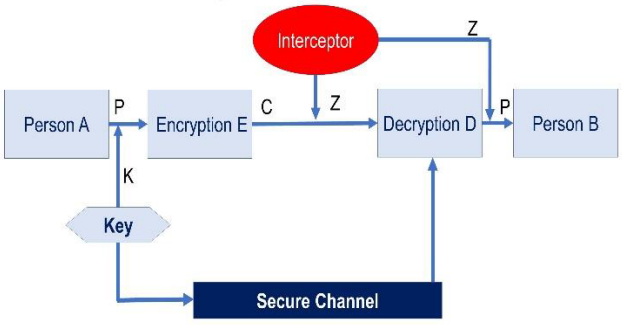

FIGURE 11. Man-in-middle attack avoidance scenario.

channel and listens to the conversation between the sender and receiver in secret.

$$P(A, B) = Z(E(A, B) + Z((E_i+1), (D)) \quad (8)$$

P is the plaintext that transmitter A must transfer towards receiver B. Z is the man-in-middle that access encrypted data E and inject fake data packets towards receiver.

This scenario is not possible due to the data encryption algorithm and the built-in authentication process in the suggested system of MQTT protocol, either. The authentication process will help to prevent third parties from listening to the conversation, as this process only allows legitimate users to communicate. Encryption algorithms also help to avoid this attack because of using secret keys and efficient algorithms as shown in figure 11.

$$P(A, B) = Z(E(A, B) + R(E(A, B)) \quad (9)$$

Plaintext P is must be sent from person A to Person B. Attacker in middle does not interrupt the transmission of encrypted data E because of built-in authentication or registration process R in MQTT protocol. Plaintext converted into the ciphertext C therefore, original data is also saved from the attacker.

B. KNOWN PLAINTEXT ATTACK

The attacker tries to analyze a relationship between plaintext and ciphertext when the attacker gets a piece of plaintext and ciphertext. This is a very simple cryptographic attack. Figure 11 illustrates the attack scenario when the user sends the data to encapsulate the piece of plaintext for encryption. Through this known chunk of data, the attacker attempts to recover the algorithm used for the encryption process which

FIGURE 12. Plaintext Attack, on which the attacker tries to recover original data from chunk of known data.

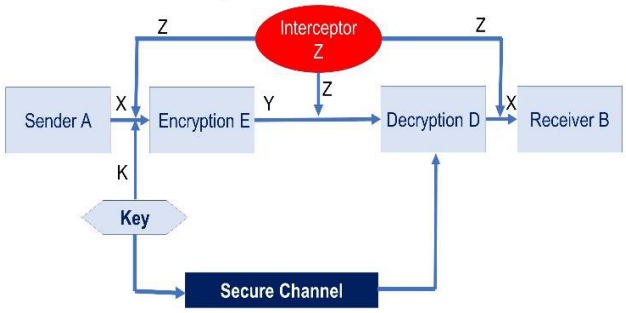

FIGURE 13. Plaintext Attack Avoidance Scenario.

is then also used for decryption.

$$X(Y(S, R) = Z(X, Y) \quad (10)$$

X is the original text that sender S must have to send towards receiver R. Y is the ciphertext generated from the encryption algorithm additionally, Z is an attacker who gets original and encrypted data to access complete information.

The proposed approach will avoid this plaintext attack because simple plaintext is not sending over the network by the user. Plaintext always used key generated by the simple proposed algorithm and then follow the procedure. Therefore, the attacker may not be able to decrypt the data.

$$X(E(Y(S, R) = Z(Y) + R(E) \quad (11)$$

X is the plaintext that is not sent over the wireless channel originally. The original data is encrypted from the encryption algorithm E and converted into ciphertext Y. Sender S transmits encrypted data towards receiver R. Therefore, attacker Z do not get original information from ciphertext Y and only accessible to receiver R.

VI. CONCLUSION

WBAN is all over a fascinating field in healthcare, contains nano sensors for the monitoring of patient's data. Security and privacy of the critical data of sensors user is very essential because it is transmitted over the public network. Therefore, a novel genetic-based encryption algorithm is proposed to secure the data in an uncomprehensive form. Besides, the transmission of encrypted data over the network also remains confidential and protected by using a lightweight telemetry transport protocol.

REFERENCES

[1] M. Anwar, A. H. Abdullah, R. A. Butt, M. W. Ashraf, k. N. Qureshi, and F. Ullah, "Securing data communication in wireless body area networks using digital signatures," *Tech. J.*, vol. 23, no. 2, pp. 50–55, 2018.

[2] F. S. Chowdhury, A. Istiaque, A. Mahmud, and M. Miskat, "An implementation of a lightweight end-to-end secured communication system for patient monitoring system," in *Proc. Emerg. Trends Electron. Devices Comput. Techn. (EDCT)*. Kolkata, India: At Guru Nanak Institute Technology, Mar. 2018, pp. 1–5.

[3] S. Ali, H. Ashraf, and M. S. Ramazan, "An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 6, p. 24, 2020.

[4] F. Wu, T. Wu, and M. R. Yuce, "An Internet-of-Things (IoT) network system for connected safety and health monitoring applications," *MDPI Sensors*, vol. 19, no. 1, pp. 1–21, Dec. 2018.

[5] A. Bashir and A. H. Mir, "Securing communication in MQTT enabled Internet of Things with lightweight security protocol," *EAI Endorsed Trans. Internet Things*, vol. 3, no. 12, pp. 1–6, Apr. 2018.

[6] M. Boumaiz, M. El Ghazi, A. Bouayad, M. Fattah, M. El Bekkali, and S. Mazer, "The impact of transmission power on the performance of a WBAN prone to mutual interference," in *Proc. Int. Conf. Syst. Collaboration Big Data, Internet Things Secur. (SysCoBIoTS)*, Casablanca, Morocco, Dec. 2019, pp. 1–4.

[7] S. F. Raza, C. Naveen, V. R. Satpute, and A. G. Keskar, "A proficient chaos based security algorithm for emergency response in WBAN system," in *Proc. IEEE Students' Technol. Symp. (TechSym)*, Nagpur, India, Sep. 2016, pp. 18–23.

[8] I. A. Sawaneh, I. Sankoh, and D. K. Koroma, "A survey on security issues and wearable sensors in wireless body area network for healthcare system," in *Proc. 14th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Dec. 2017, pp. 1–5.

[9] D. S. Agha, F. H. Khan, and R. Shams, "A secure crypto base authentication and communication suite in wireless body area network (WBAN) for IoT applications," *Wireless Pers. Commun.*, vol. 103, pp. 2877–2890, Sep. 2018.

[10] S. Sindhu, S. Vashisth, and S. K. Chakarvarti, "A review on wireless body area network (WBAN) for health monitoring system: Implantation protocol," *Commun. Appl. Electron.*, vol. 4, no. 7, pp. 1–5, 2016.

[11] A. Sammoud, M. A. Chalouf, O. Hamdi, A. Bouallegue, and N. Montavont, "A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101838.

[12] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Comput. Netw.*, vol. 148, pp. 196–213, Jan. 2019.

[13] P. Dodangeh and A. H. Jahangir, "A biometric security scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 41, pp. 62–74, Aug. 2018.

[14] P. K. D. Pramanik, A. Nayyar, and G. Pareek, "WBAN: Driving e-healthcare beyond telemedicine to remote health monitoring: Architecture and protocols," in *Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare*. Amsterdam, The Netherlands: Elsevier, 2019, pp. 89–119.

[15] J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, and J. Lin, "A logistic mapping-based encryption scheme for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 110, pp. 57–67, Sep. 2020.

[16] M. Gowtham and S. S. Ahila, "Privacy enhanced data communication protocol for wireless body area network," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Coimbatore, India, Jan. 2017, pp. 6–7.

[17] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018.

[18] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[19] A. Z. Alshamsi and E. S. Barka, "Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks," in *Proc. Int. Conf. Informat., Health Technol. (ICIHT)*, Riyadh, Saudi Arabia, Feb. 2017, pp. 21–23.

[20] M. Xiao and X. Hu, "Multi-authority attribute-based encryption access control scheme in wireless body area network," in *Proc. 3rd Int. Conf. Inf. Syst. Eng. (ICISE)*, Shanghai, China, May 2018, pp. 4–6.

[21] S. Soderi, L. Mucchi, M. Hamalainen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 7, pp. 1–13, Jul. 2017.

[22] L. Mucchi, L. S. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Wireless Pers. Commun.*, vol. 51, no. 1, pp. 67–80, Oct. 2009.

[23] M. A. Shayokh, A. Abeshu, G. B. Satrya, and M. A. Nugroho, "Efficient and secure data delivery in software defined WBAN for virtual hospital," in *Proc. Int. Conf. Control, Electron., Renew. Energy Commun. (ICCEREC)*, Bandung, Indonesia, Sep. 2016, pp. 12–16.

[24] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 9–13.

[25] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Tiruchirappalli, India, Dec. 2019, pp. 13–14.

[26] M. S. A. Malik, M. Ahmed, T. Abdullah, N. Kousar, M. Nigar, and M. Awais, "Wireless body area network security and privacy issue in E-healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, p. 7, 2018.

[27] S. Farooq, D. Prashar, and K. Jyoti, "Hybrid encryption algorithm in wireless body area networks (WBAN)," in *Intelligent Communication, Control and Devices*, R. Singh, S. Choudhury, and A. Gehlot, Eds. Singapore: Springer Nature, 2018, p. 10.

[28] S. Zou, Y. Xu, H. Wang, Z. Li, S. Chen, and B. Hu, "A survey on secure wireless body area networks," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, May 2017.

[29] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[30] V. Kumar, R. Kumar, M. A. Barbhuiya, and M. Saikia, "Multiple encryption using ECC and its time complexity analysis," *Int. J. Comput. Eng. Res. Trends*, vol. 3, no. 11, p. 568, Nov. 2016.