Efficient Cryptographic Technique for Data Protection of Wireless Body Area Network

Saddiqa Javaid , Humaira Ashraf * , NZ Jhanjhi *

Posted Date: 21 December 2023

doi: 10.20944/preprints202312.1609.v1

Keywords: wireless body area networks; data security; internet; man-in-the-middle attack; efficient cryptographic technique; cryptography; DNA; ECC

Article

Efficient Cryptographic Technique for Data Protection of Wireless Body Area Network

Saddiqa Javaid , Humaira Ashraf * , NZ Jhanjhi *

Posted Date: 21 December 2023

doi: 10.20944/preprints202312.1609.v1

Keywords: wireless body area networks; data security; internet; man-in-the-middle attack; efficient cryptographic technique; cryptography; DNA; ECC

 doi:10.20944/preprints202312.1609.v1

Article

Efficient Cryptographic Technique for Data Protection of Wireless Body Area Network

Saddiqa Javaid [1], Humaira Ashraf [1,*] and NZ Jhanjhi [2]

[1] Department of Computer Science & Software Engineering Faculty of Basic and Applied Sciences, International Islamic University Islamabad, Pakistan; saddiqa.mscs1107@iiu.edu.pk; humaira.ashraf@iiu.edu.pk
[2] School of Computer Science (SCS), Taylor's University, Subang Jaya 47500, Malaysia; noorzaman.jhanjhi@taylors.edu.my
* Correspondence: Author: Dr. Humaira Ashraf; humaira.ashraf@iiu.edu.pk

Abstract: WBAN is a blessing to mankind because it can monitor people's health and activities regardless of place or time. It brings feasibility in patients' treatment. The main problems with WBAN, however, are related to the security and privacy of health data. To prevent data misuse, health information should be safeguarded. On the other hand, the medical professional needs to receive the patient's health information promptly. As security of health data impact human life greatly so secure an efficient method is required. Efficient cryptographic technique for data protection of wireless body area network is proposed. This research aims to provide data protection in WBAN to increase data security and efficient transmission. The suggested approach offers effective security with quick key generation, quick encryption, and secure data transmission across the network. The proposed methodology is considered to be secure and will consume less time. The proposed method further uses a less complex encryption algorithm. The less complex the approach is the higher performance it will provide in wireless network. The proposed methodology will prevent many attacks, which makes the proposed approach highly suitable for wireless body area network's security.

Keywords: Wireless body area networks; data security; internet; man-in-the-middle attack; efficient cryptographic technique; cryptography; DNA; ECC

1. INTRODUCTION

Nowadays, wireless communication is critical for sharing information anywhere and at any time. The convenience of people's lives is increasing as the Internet of Things matures." Healthcare is becoming part of information technology". The Internet of Things is exemplified by smart homes, intelligent grids, automated transportation, and smart medical systems. It's worth emphasizing that, as an emerging network, Wireless Body Area Network (WBAN) can enable remote monitoring, telemedicine, and wearable, implanted emergency medical aid. Basically, the term "Wireless Body Area Network" was coined by Van Dam in 2001 and is a network of sensors that are connected to the human organs and used to measure biological signals (frequency, heart rate, blood pressure, brain signals, etc.) of humans [1].

Numerous sensors that may communicate wirelessly and are located on or below the surface of the body are connected by a wireless body area network. These sensors have the capacity to openly share data electronically and interact with one another. The WBANs are divided into two categories: intra WBANs and beyond WBANs. In contrast to beyond WBAN, which refers to a network where the gateway provides the connection link to the medical server, intra WBAN incorporates wearable nanosensors that are employed by the human body. [2] A wireless sensor network makes it possible to access the stored data and provides the ability to transmit data wirelessly through the network. The wireless body Area Network (WBAN), which offers continuous long-term monitoring on or within the human body and updates of medical records over the Internet, transmits real-time data, which can be voice and video or in other forms, to monitor the state of vital organ functions. By continuously monitoring health data and sending it to medical professionals, it aids in the early detection of illness. As in the era of covid 19 [3] it is unfeasible to visit medical centers and get treated. Technology of WBAN in such situation provide huge facility for the treatment of patient suffering from various diseases. [4,5]

 doi:10.20944/preprints202312.1609.v1

In 2021 there are lot of healthcare data breaches, in US every 7 seconds 10 individuals are affected by healthcare data breaches. Total 42.5 million individuals are affected and its cost 9.2 million dollars. Still in 2022 there are 337 data breaches and are increasing day by day. These data breaches are caused by IT incidents and un authorized access and data loss, these statistics is true picture that there is still need of security in healthcare. [6]

Data security is critical when sharing information via a public network, as outsiders may misuse or change the information or attacker might access the data and attack. Because nodes are typically situated in hostile environments with insecure transmission medium, it is a difficult task in remote health monitoring systems. A hostile attack, such as data manipulation or data falsification, is a possibility in this scenario. [7]. It is crucial to protect patient health information at both edge nodes and the communication channel. [8] To safeguard patient data from outsiders and ensure patient's data confidentiality and safety , specific security protocols should be followed. For the patient's treatment to proceed as intended, secure and valid data communication is required. [9] Valid and fast data improves the treatment of present and future patients with the same disease or issue. For all states, including data collection, transport, processing, and storage in a remote environment, essential security aspects should be enabled.

In literature multiple approaches were exists for enhancing the security of wireless body area network. Multiple limitations are extracted from existing literature. Some are using more complex algorithms with high computational cost and computational time to provide security. Some are also vulnerable to attacks when using the single key and other conditions. So efficient, secure and low computational cost and time mechanism are still required, which provide efficient security within minimum time. Mostly block ciphers are used for providing security no doubt they are efficient and effective but they provide security in various rounds and become computationally expensive. [10–12] This study aims to provide security to patient data with low computational time, encryption time, decryption time, response time and transmission delay and high through by using simple phases and steps. It not only computationally efficient but also fastly encrypt data and transmit over the network in this way patient's data can be secure and timely reach the destination.

This document is divided into the following sections: Section 2 provides a brief overview of the various researches for wireless body area network security suggested in the publications; Section 3 presents the methodology; Section 4 demonstrates the simulation model; Section 5 shows the outcomes; Section 6 provides a security analysis; and Section 7 provides conclusions.

2. LITERATURE REVIEW.

This section goes into great depth on the research of the papers that were chosen. The primary objective of their research is to provide security.

- *Block Ciphers:*

The majority of literary publications employ block ciphers, an encoding system that conceals data in blocks and generates ciphertext using a secret key and secure procedure. For data security and effective performance, the block ciphers RSA, AES, RC7, PRESENT, and ECC are employed in the literature. In Kalaivani et al., the secure format of ECG data is compressed and transmitted between individuals through wireless communications using Enhanced and Modified RSA and Run length Encoding. Run Length Encoding is used to compress the data before it is encrypted with the Enhanced and Modified RSA technique. The receiver receives the protected health data through the Internet. Run Length encoding is basically lossless compression technique which represents the long length of a sequence by shorter sequence and store run of data as a single value and RSA is asymmetric algorithm and block cipher, it is modified using prime numbers instead of two number for encryption. [13,14]

Another author use AES block cipher used in phase of encryption, AES consists of multiple rounds and each round have steps like sub-byte, shifting, mix columns add round key while in other phase Genetic Algorithm(GA) which is evolutionary algorithm and focus on optimization is used for task scheduling. Additionally, GA includes a number of stages and fitness function values that allow for efficient task flow scheduling and the transmission of confidential data into the cloud. [15].

Sivasangari et al. suggested a lightweight safety mechanism that uses a logistic chaotic scheme with three phases. Communication among the sensor node and cluster head (SH) occurs during the first phase. Both provide the logistic chaotic RC7 algorithm's seed value, which generates the key

 doi:10.20944/preprints202312.1609.v1

sequence. Coordination between the cluster head and base station develops during the second phase. The final stage involves sending the medical server, using the present algorithm, with medical data that has been secured. [16]

For safe transmission of patient's sensitive information, the authors of Chandrasekaran et al integrate Ciphertext-Policy Attribute-Based Encryption (CPABE) and Constant Size Ciphertext (CPABE-CSC) using the Blowfish method. Whenever the session key is valid, the transmitted data undergoes encryption and decryption using the Blowfish technique and CPABE-CSC. The findings show that the suggested architecture lowers both computing and storage expenditures [17].

AES and ECC (Elliptic Curve Cryptography) are cryptographic mechanisms of security. RSA and ECC both provide public key cryptography but this literature study replaces RSA with ECC to provide efficient security to keys of AES while AES is used for securing data across the network. Nodes are separated into energy-rich and energy-saving modes based on the basis of energy. Energy-saving modes use the AES algorithm to move further data on the route and energy-rich modes use both AES and ECC for proper utilization of energy. [18]

The author of this paper provides a study for the efficient protection of patient's health information. Data encryption is accomplished using a hybrid encryption algorithm. The suggested methodology consists of 5 stages. Registration, Authentication, ECDH key exchange, Encryption phase and Decryption phase. In registration phase registration numbers are assign to patients and node ids are assigned to sensors. Base station and sink nodes employ the registration number (RN), node id (NID), and the time stamp (TM) for authorization during the authentication phase. following that, the sink node and base station interchange keys as part of the key exchange phase. Next input is taken and divides it into equal blocks then these blocks are divided into two parts. First part is encrypted using Elliptic curve cryptography and second part is encrypted used AES algorithm then hash of first part is calculated after this hash of second part is calculated and in last both are ciphers are combined to form cipher and similarly decryption is its reverse. [19]

- *Evolutionary Algorithm.*

An evolutionary algorithm (EA) is a type of algorithm that solves problems by using mechanisms inspired by nature and processes that mimic the behaviors of live creatures. An evolutionary algorithm (Genetic algorithms) can create high-quality solutions for a variety of problems, a genetic algorithm is also used for the security of data and higher performance, in this study data is converted into binary and is XORing with a key. Key is generated by choosing integer and converting it into binary and taking 1'complement of it after it shits 2 bits right This involves multiple genetic steps for encryption of data like mutation, substitution box, crossover, string mapping of amino acids etc. After xor with key mutation is performed. In the crossover phases of algorithm positions are interchanged, Now the resultant data will proceed to the next step of S-box. The amino acid table will provide the corresponding substitution data for the resultant alphabet entries from the substitution-box, and the generated code will run the next stage of string mapping to produce the encrypted text or cipher. Inverse process of encryption will results decryption. [20]

- *Block Chain.*

A blockchain network secures data using cryptographic techniques at two layers. One is key encryption, while the other is hashing. Using IOMT, the author of this paper presents a safe and energy-efficient approach. Clustering is employed in this research for selecting the sink nodes. The cypher blockchain method is used for both encryption and decryption, while Kruskal's algorithm is implemented to obtain subgraphs, assess the least cost value, and improve the route choice from sensors to healthcare centers. Data is divided into data blocks and encrypted. The shared key of a node is used for authorization, and the secret key of a node is used to digitally sign the ciphertext. The data block of a node is xor with the cipher block of the previous node. And decrypted inversely [21,22]

- *Policy Homomorphism Encryption.*

The technique of converting data into ciphertext that can be studied and used, Complicated mathematical calculations on encrypted data can be carried out using homomorphic encryption without compromising the encryption [23]. Liu et al suggested to use privacy homomorphic technology to encrypt data before it is aggregated by a cloud service, guaranteeing data security and preventing data decryption. Accumulate user data labels for batch verification to secure the

 doi:10.20944/preprints202312.1609.v1

information's integrity while cutting down on user data authentication's administrative burden. Finally, a greedy forwarding model is employed to forward user data to increase the effectiveness of data transmission. For encryption seed mask is calculated and encrypts data via hash and divides a message into parts and cipher. This cipher is aggregated by the cloud and sent to health professionals where the data is decrypted by calculating hash and seed mask etc. [24]

- *Hash Algorithm.*

A hash algorithm is an operation that produces a fixed-length numerical string result from a data string. The output string is typically significantly shorter than the original data. In Al Hasib et al Digital signatures and SHA-1 are employed to offer security. The suggested solution makes use of shared secret keys between the BNC and all of the network's sensor nodes. With the BNC, each sensor node registers. The BNC digitally authenticates and verifies the freshness of each data packet by adding an SK and broadcasting the PK to all sensor nodes. When a data is verified as valid, BNC uses a digital signature to certify it and forwards it to the medical server for processing. Data encryption using the proposed D-Sign approach utilized the SHA-1 hash function. The resultant hash value is then encrypted using senders PK. A digital signature is created using the hash value and the sender's SK and is then attached to the data packet. The sender's PK, which is already included in the digital signature, is used by BNC to decrypt the hash value when it receives the packet. The results reveal that the suggested method is more effective at protecting data and making the best use of network resources. [25–27]

3. Proposed Efficient Cryptographic Technique for Data Security of Wireless Body Area Network

This section describes proposed methodology of data security is applied on. The sensor node (could be user) sends data to the sink node/gateway and finally it is sent to BS from where it can route to other directions. Multiple techniques of Data security of WBAN are discussed in the literature but these also have some limitations and issues, that's why there is a need for efficient techniques for the security of WBAN's data. This study or research method presents technique for the security purposes.

➢ *Proposed Framework:*

In this section of research study overview of the proposed methodology is presented. The suggested framework's architecture consist of some sensors that are embed on human body, a sink node and a server. These sensors sense patient data, secure it, calculate hash and transmit to sink, At sink hashes of data are matched and further transmits the encrypted data to the medical server's associated with internet cloud. From this medical server health professionals access medical data. Health-critical data must be stored on a medical server that is completely secured. In Figure 1 architecture of proposed scheme is shown and an efficient cryptographic technique has been used for the security of WBAN as shown in Figure 2. This technique encrypt data safely and fastly for efficient transmission across the network [31–42]. In the pursuit of enhancing data protection within Wireless Body Area Networks (WBANs), our research draws upon the foundational principles elucidated in [43–55].

➢ *Data Encryption and Decryption method:*

An efficient cryptographic technique for wireless body area network's data protection (ECTWBAN) is used for safety of patient data. An encryption method is used to protect against threats and data compromises and to encrypt patient health data. ECTWAN is combination of multiple phases i.e., Transformation, Logical operation, S-box, DNA cryptography, mRNA, Authentication and Public key cryptography. In the transmission stage plain text is taken firstly as simple text and then conversions are applied on it. First it is converted into asci characters then this asci is converted to its corresponding binary. After this, next phase of Logical operation in this phase logical XOR operation is performed between generated binary and Key. Key is totally random and is equal to generated binary in transmission stage, key is generated randomly by random key generator. In next step there is generation of S box (substitution box). S Box is substitution box from which different values are substitute, its purpose is to obscure key and cipher. In our scheme the S-box is generated from which values are substituted. S-box is generated by the using mathematical operations, Boolean operations and complement operation on the input of rows and column. The input for the S-box is taken in alteration sequence, first of all text or binary to be substituted are divided into pairs then first bit is read from row and next bit two bits are from the column and fourth

 doi:10.20944/preprints202312.1609.v1

bit is also read from row. And corresponding value obtained from row and column pass through some mathematical calculations and binary operations which results in unique value, this value is not again repeated in the whole S-Box and able to reverse in the process of decryption. S-Box is shown in Table 1 and the mathematical equation of this is shown below.

$$S(r,c) = r(i) \veebar c(j).(r(i))'. \qquad \text{eq (a)}$$

In equation a, r and c represent rows and columns respectively whereas i and j are the number of rows and number of columns respectively.

Table 1. WBAN Substitution Box of Proposed Technique.

	00	01	10	11
00	0011	0111	1011	1111
01	0110	0010	1110	1010
10	1001	1101	0001	0101
11	1100	1000	0100	0000

The generation of DNA-encoded data from S-Box comes next. Different values are encoded according to DNA patterns as shown in Table 2. DNA encoding is not conventional In DNA encryption 4! Pairs Adenine couples with Thymine and Cytosine pairs with Guanine. [28], however I try to combine the two as indicated in Table 3 by pairing Adenine with Cytosine and Guanine with Thymine. It guarantees data secrecy and data security. In DNA cryptography, nitrogenous bases are given values according to eight criteria, and during the DNA encoding phase, we encode the values using the nitrogenous bases of DNA as shown in Table 3, which are A=00, C=01, G=10, and T=11. In this phase, we substitute the value from S-Box and whole 8-bit values are converted to DNA bases in this way we encode binary values to DNA encodes as indicated in Table 3.

Table 2. DNA-encoded S-box.

	00	01	10	11
00	AT	CT	GT	TT
01	CG	AG	TG	GG
10	GC	TC	AC	CC
11	TA	GA	CA	AA

Table 3. DNA encoding table.

DNA Bases	Binary Value
Adenine (A),	00
Cytosine (C)	01
Guanine (G)	10
Thymine (T)	11

After it, RNA encode phase is next phase to be executed and, in this phase, DNA encode is replaced with RNA encode. There are three types of RNA: tRNA, rRNA, and mRNA. mRNA has four nucleotides, whereas other RNAs have three. mRNA stands for messenger RNA. We encode the values received from DNA encodes to mRNA encodes again during the mRNA encoding phase. To convert into mRNA, we take the complement of DNA bases, and their complement results in or produces RNA bases, where the complement of DNA bases are U, G, C, and A.

$$A \rightarrow U, C \rightarrow G, G \rightarrow C, T \rightarrow A.$$

DNA adenine (A) base complement is uracil (U), which is an RNA base, DNA cytosine (C) base complement is guanine (G), which is an mRNA base, DNA guanine (G) base complement is cytosine (C), which is an RNA base, and DNA thymine (T) base complement is adenine (A), which is an mRNA base. Table 4 indicates the values of various mRNA bases.

 doi:10.20944/preprints202312.1609.v1

Table 4. mRNA encoding table.

mRNA Base	Binary Values
Uracil (U)	00
Guanine (G)	01
Cytosine (C)	10
Adenine (A),	11

After the encoding phases of both DNA and mRNA. There is phase of authentication to be performed. In phase of the technique is Public Key Cryptography, and in it (Elliptic Curve Cryptography) ECC is used, ECC is public key cryptographic technique that uses two keys instead of one that are public and private, the encrypted text is further re-encrypted by the receiver 's public key and is decrypted by receiver's private key [29]. In last for Authentication of ECTWBAN technique, (Hashed Message Authentication Code) HMAC is used. At sink node this hash is calculated and matched but data remain encrypted and packet is transmitted forward towards base as shown in Figure 3. After encryption hash is applied on encrypted data and that data moves towards the sink node. At sink data is not decrypted only hash of encrypted data is matched and authenticated that whether encrypted data is valid and data integrity factor is maintained or not. If data is valid and successful authentication data is moved to other middle node or to the server if data is invalid. Sink node discard the packet and request the valid data again. Similarly hashed is also matched on other nodes and server too.

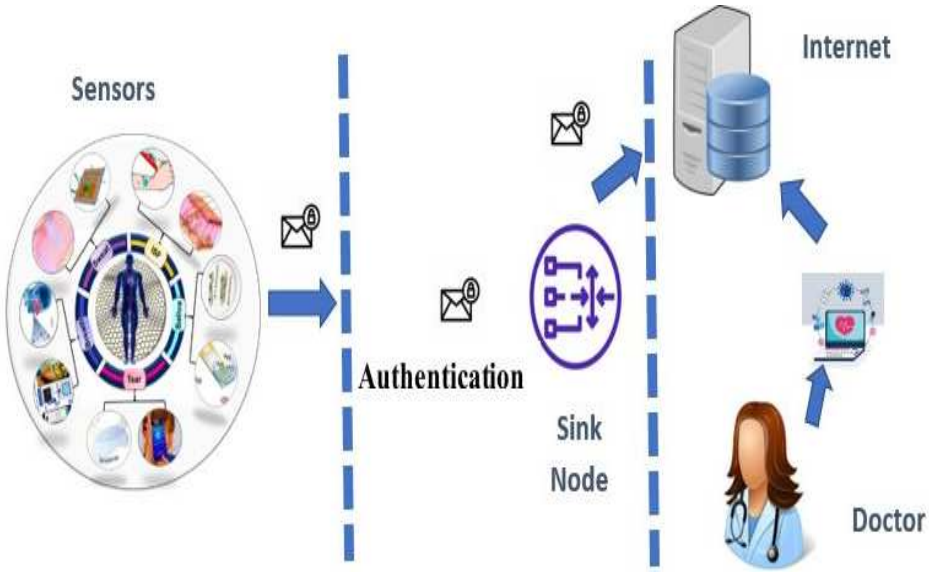

Figure 1. Overview of Proposed Work.

Algorithm

Begin

Input: Plaintext P

Output: Ciphertext C

Creates a DNA encoding table that is used to encode plain text into a DNA sequence.

Converted P into ASCII numbers.

Transform generated ASCI into binary representation(B).

Input K

 doi:10.20944/preprints202312.1609.v1

B ⊕ K

IF (B is received) **THEN**

Apply S-Box on B and DNA sequence is created.

if (data bits are not even)

add zero padding

ELSE

continue sequencing

Transform into mRNA code then it is converted into C (Cipher text).

ELSE IF (not received) then

Go to step 6

ELSE IF (successfully created C) then

Apply ECC

C and k are sent to the Receiver side.

Apply HMAC

END IF

END

4. Mathematical Model of ECTWBAN:

Table 5. Notation Table.

Z	Data which updates
P	Plaintext
K	Key
Bi	Binary
S-b	S-Box

The information that needs to be converted is demonstrated as €. Each encryption or decryption operation updates the temporary data-saving variable temp.

$$€ = P \tag{1}$$

$$Z = P \rightarrow Z`_{(ASCI)} \tag{2}$$

The P variable is used to represent plaintext, while Z is the provisional-based data that is modified in accordance with how operations are carried out. As operations are carried out, this variable is changed to Z1, Z2,... Here $Z`_{(ASCI)}$ represent the asci values. In equation 1 plain text is converted to asci values and result is stored in Z.

$$Z1 = Z\_{Bi} \tag{3}$$

 doi:10.20944/preprints202312.1609.v1

Here in Equation 3, transformations are performed. Z1 represents data that is updated in this step. In this equation conversion of binary of resultant data formed which is obtained from the previous equation 2,

$$Z2 = Z1 \oplus K \tag{4}$$

Z1 denotes data obtained from the previous equation, now key K generated by the random generation technique is XORed with Z1, xor encryption maintains data confidentiality and makes encryption stronger and result of both are stored in Z2. Here size of key is equal to the text so that it can make attacker difficult to extract key and unable to perform attacks or computations.

$$Z3 = Z2+X_{(S\text{-}b)} \tag{5}$$

The next step of equation 5 presents that DNA S-Box is applied to Z2 data that is generated from the step and is d updated based on the technique. As it is mentioned before that S boxes are of two types user can select it on base of size of the input, if input is small user can use mini S-Box and in case of large input Extended S box can be used.

$$Z4 = Z3.\ Y_{(DNA\ seq)} \tag{6}$$

In equation 6 there is Z3 which is taken from equation 4 and then on this Z3 value DNA sequence encoding is applied and transform it to securable form**.**

$$Z5 = Z4.\ \check{Z}_{(mRNA)} \tag{7}$$

In equation 7 variable Z4 pass through phase of mRNA encoding and data is stored in Z5 in mRNA sequences. RNA sequences are created using nitrogenous bases of RNA.

$$Z6= Z5_{(ECC)} \tag{8}$$

The next step after the formation of Z5 is the re-encryption of data by using Public key cryptography. ECC algorithm is applied on data generated from equation 8.

$$Z7=Z6_{(HMAC)} \tag{9}$$

The cipher generated from equation 8 further pass through phase of HMAC for authentication and for maintaining integrity of data. Additionally, it makes the scheme secure against additional attacks and defends it from Man in the Middle attacks.

5. SIMULATION MODEL:

The proposed approach is implemented through simulations. The simulation setup consists of Python simulation software, an Intel Core i3 processor running the Windows operating system 64-bit, and Four gigabytes of RAM.

6. RESULTS:

In order to evaluate the efficiency of a cryptographic technique, it is applied to the WBAN sensor environment. Experimental findings are given with regard to the encryption and decryption times required by the algorithm.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1609.v1

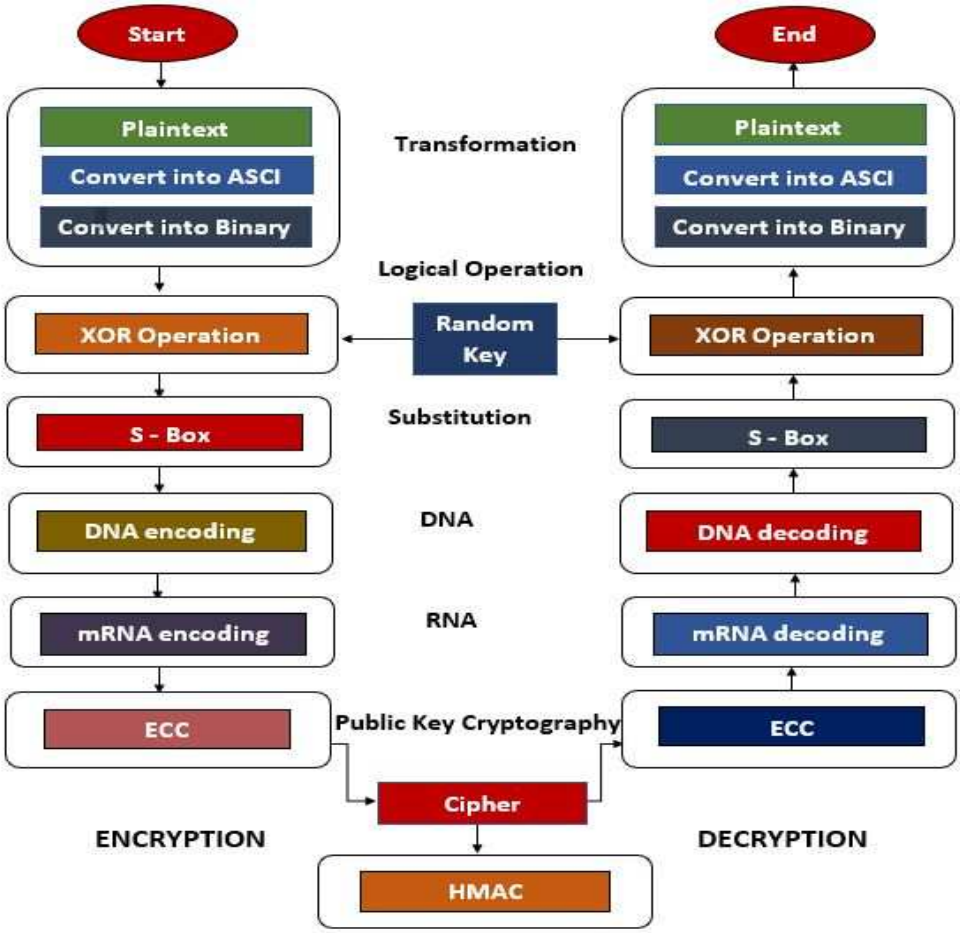

Figure 2. Proposed Technique Flowchart.

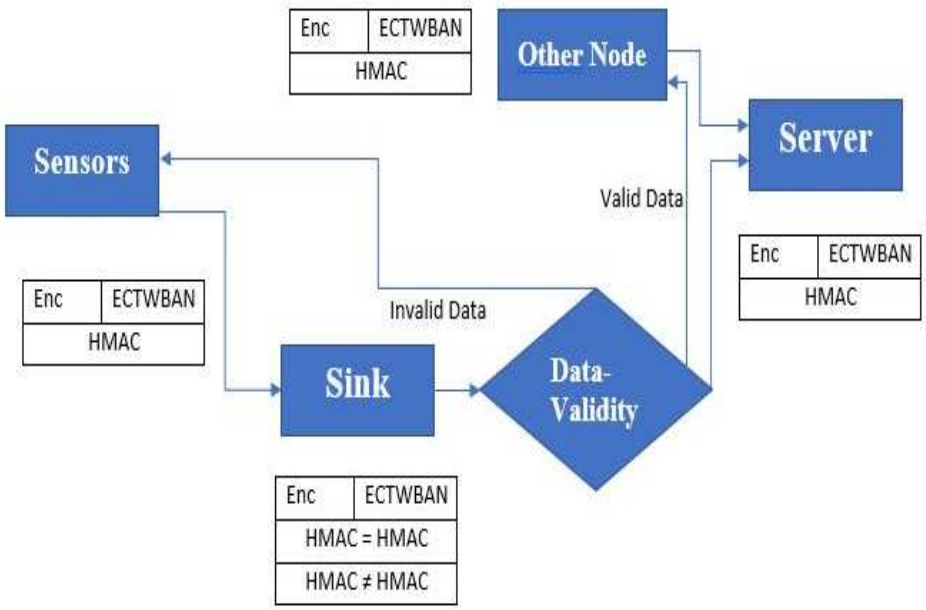

Figure 3. Data Routing.

- *Algorithmic time*

 doi:10.20944/preprints202312.1609.v1

The Algorithmic time is the total span of time needed by an algorithm to execute a calculation. Since it shows how many times an operation must be performed during a protocol interaction, time spent on computation is an essential performance indicator for an encryption strategy. Because the key creation process is straightforward, the suggested algorithm's computational time complexity for key generation is lower than that of literature techniques.

Figure 4 demonstrated that even though the number of data bytes increased the number of milliseconds needed for key generation, the overall degree of time complexity remained fairly low.

Figure 6 analyses the input information given to the encryption technique with the time complexity, and it shows that the recommended research steps are simple and effective, so the time needed by the algorithm to transform plaintext into ciphertext is as minimal as conceivable.

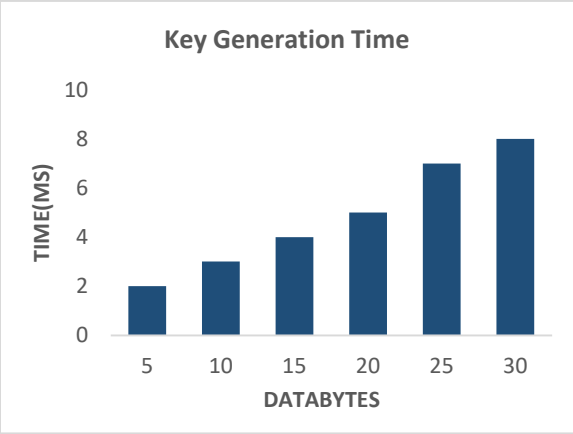

Figure 4. Key Generation Time of Proposed Technique.

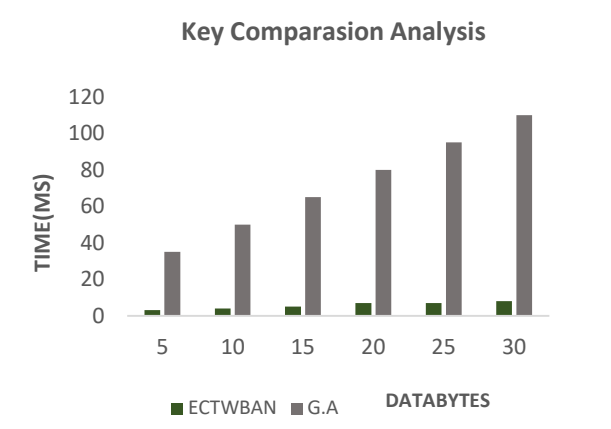

Figure 5. Key Comparison Analysis of Proposed Technique.

- *Time of computation for Encryption*

The algorithmic time of encryption is the time taken by various steps to convert the plaintext to cipher or encode text. Time taken by ECTWBAN is less as compared to literature schemes.

- *Time of computation for Decryption*

Algorithmic time for various operations to transmit the encoded text to plaintext or to convert the ciphertext to decoded or plaintext as shown in Figure 7 and comparative analysis is shown in Figure 9 that shows that the time taken by ECTWBAN is much less as compared to various literature researches.

➢ *Comparison Analysis of Key Generation*

Time needed to generate key for proposed study is far less as compared to literature study [20] comparison analysis of this study with literature scheme is shown in Figure 5.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 December 2023 doi:10.20944/preprints202312.1609.v1

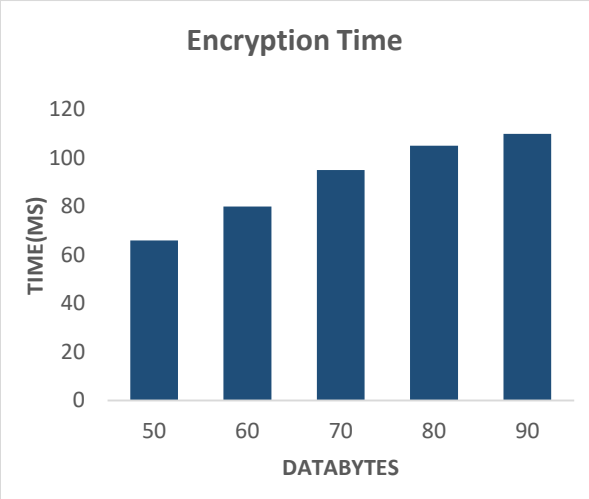

Figure 6. Encryption Time of Proposed Technique.

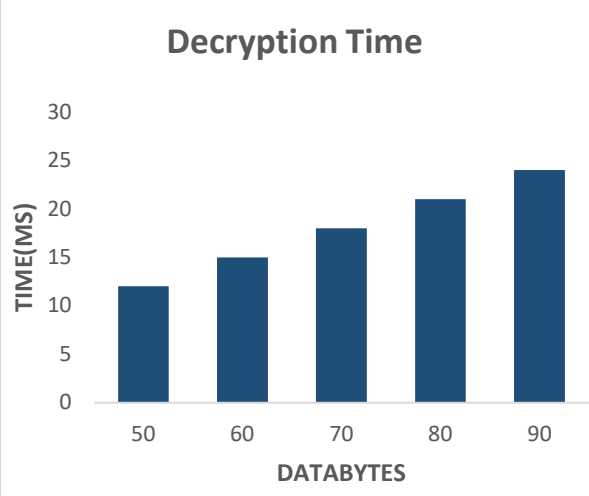

Figure 7. Decryption Time of Proposed Technique.

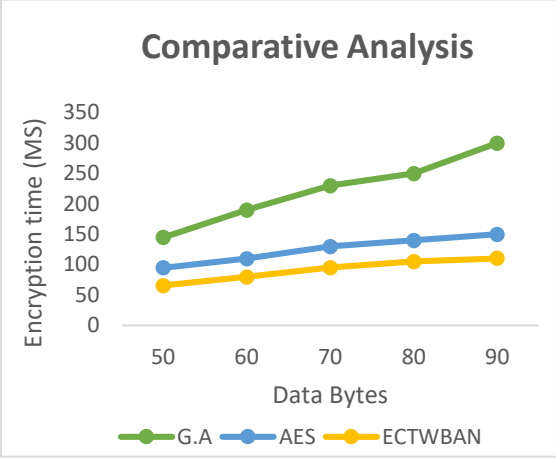

Figure 8. Comparison of Encryption Time of various schemes.

 doi:10.20944/preprints202312.1609.v1

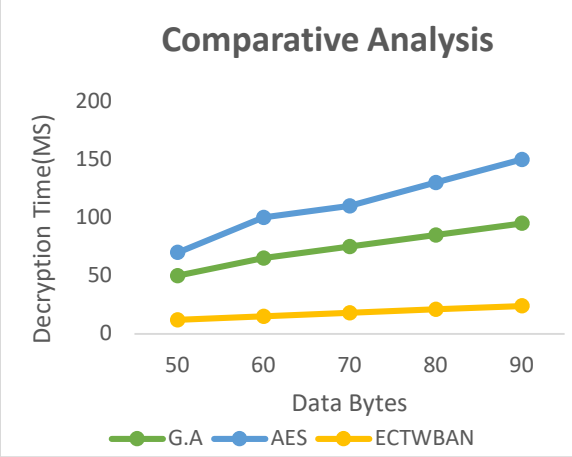

Figure 9. Comparison of Decryption Time of various schemes.

➢ *COMPARISON SCRUTINY OF ENCRYPTION AND DECRYPTION ALGORITHM*

The proposed efficient cryptographic algorithm is compared to the various techniques' encryption and decryption times. The recommended technique encodes and decodes data much faster than the alternatives, as seen in Figures 6 and 7. According to testing on the decryption timings of the different systems, the suggested approach for decrypting data has a lower temporal complexity than existing techniques. Performance of AES [15] and G.A [20] with presented algorithm is studied, and it is concluded that literature schemes are consuming more time and having more calculations while proposed approach has less computations.

7. SECURITY ANALYSIS

To secure the data from different threats, some measures are being implemented. As a result, it is crucial to treat data transmission security seriously since cyberattacks could have an impact on how network traffic is routed.

- *MEET IN THE MIDDLE ATTACK*

A Meet-in-the-Middle (MITM) attack is a cryptanalysis method that includes splitting the assault into two sections and looking for a collision between two cryptographic processes. For a subset of the potential inputs, the attacker runs one phase and records the intermediate outcomes. The attacker then executes the second phase on a different subset of all feasible inputs and compares the final findings to the interim results. The attacker has discovered a collision and can retrieve the key when they find a match. [30].

Consider a scenario where a plaintext message P is converted into a ciphertext message C using a 64-bit key encryption technique. The definition of the encryption algorithm is:

$$\text{Where } K,\ C = E(K,P) = K1 \text{ xor } (P \times K2)\ (K1,K2) \tag{10}$$

If xor is the bitwise exclusive OR operator and x stands for multiplication, K1 and K2 are two 32-bit keys. Consider a scenario where an attacker has access to a pair of plaintexts and ciphertext (P, C) and wishes to retrieve the key

$$K = (K1, K2).\ ) \tag{11}$$

The meet-in-the-middle attack can be used by the attacker as follows:
Create all 232 potential K1 values and use each one to encrypt the plaintext message P. The intermediate results should be kept in a Table T1.
Decrypt the ciphertext message C using each of the 232 potential values for K2, and then store the intermediate results in a Table T2. Look for a corresponding intermediate outcome in T1 and T2. If a match is discovered, the attacker has obtained key K. For a given pair of K1 and P, the attacker can compute the intermediate result as follows:

$$M1 = K1 \times P) \tag{12}$$

 doi:10.20944/preprints202312.1609.v1

And the intermediate outcome for a particular K2 and C combination is:

$$M2 = K2 \text{ xor } (C \times P)) \quad (13)$$

The attacker then looks for two numbers (K1, K2) that meet the following criteria:

$$M1 = M2) \quad (14)$$

The key K may be retrieved as follows after the attacker has discovered such a pair:

$$K = (K1, K2)) \quad (15)$$

The Meet-in-the-middle attack reduces the key space from 2^64 to 2^32 + 2^32 = 2^33, making the attack feasible with moderate computational resources.

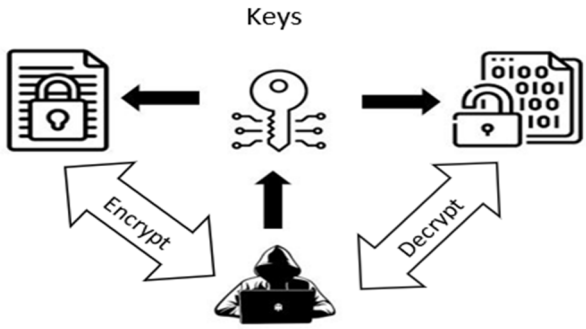

Figure 10. Meet in the middle attack scenario.

- *PLAINTEXT ATTACK*

When an attacker has some plaintext and ciphertext, they attempt to determine how they relate to one another. This cryptographic attack is fairly straightforward. This known piece of information is used by the attacker to identify the encryption procedure, which is also used for decryption.

$$P(C(S,R) = Z(P,C)). \quad (16)$$

Sender S must have the original text P, to deliver to recipient R. Z is a hacker who obtains original and encrypted data in order to access all content, and C is the ciphertext produced by the encryption technique.

The suggested method will prevent this attack since the user won't communicate basic plaintext across the network. Plaintext always utilized a key produced by the proposed method which was totally random every time, then carried out the steps. As a result, the data may not be decryptable by the attacker.

$$Z(C) = P(E(C(S, R) + R(E)) \quad (17)$$

P is the original data that was not transmitted via the communication networks. The original information is initially encrypted with the encryption method E before being converted into ciphertext P. From sender S to receiver R, encrypted data is transmitted. As a result, attacker Z cannot decipher text Y's original information, which is only available to receiver R.

- *MAN IN THE MIDDLE ATTACK*

The sender, the recipient, and the Man in the Middle (the attacker) are the main rivals in the system. As seen in fig. 11, Man-in-the-Middle disrupts a smooth communication channel and surreptitiously overhears what the sender and receiver are saying to one another.

$$Z(E(X,Y) + Z(Ei+1), (D)) = P(X,Y) \quad) \quad (18)$$

The letter P stands for the plaintext, which transmitter X must communicate to receiver Y. In the receiver's direction false data packets is Injected, the man-in-the-middle Z gains access to encrypted data E. This situation is likewise not possible because the suggested approach includes an integrated authentication process and data encryption. It prevents outside spying as the authentication process,

 doi:10.20944/preprints202312.1609.v1

only allows authorized individuals to interact. The usage of secret keys and effective algorithms in encryption secure the data from attacker

$$P(X,Y) \text{ equals } Z(E(X,Y), \text{ plus } R(E(X,Y)) \quad) \tag{19}$$

A must communicate with B using plaintext P.

Due to the HMAC protocol's built-in authentication mechanism, an invader in the middle cannot stop the transfer of encrypted data E. Hence, original material is likewise protected from the attacker after being changed from plaintext to ciphertext.

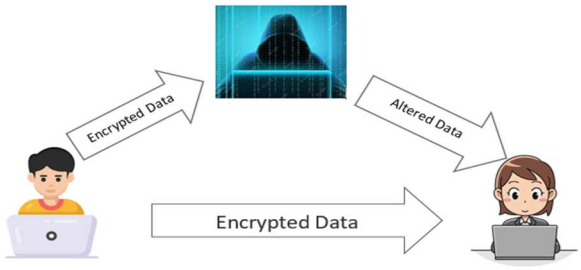

Figure 11. Man in the middle attack.

- *CHOSEN CIPHERTEXT ATTACK*

In a chosen-ciphertext attack, the attacker has access to a piece of the encrypted communication. By decrypting this portion of the ciphertext, the attacker may reconstruct the plain text. With the selected cipher-text, the attacker can additionally attempt to discover the secret key. Data cannot be recovered from the selected ciphertext in the ECTWBAN. Because the text value has changed. The value of C is not always transformed into G, as seen in Table (2). Their worth changes depending on the text piece. Thus, it is difficult to decipher the chosen ciphertext's plain text.

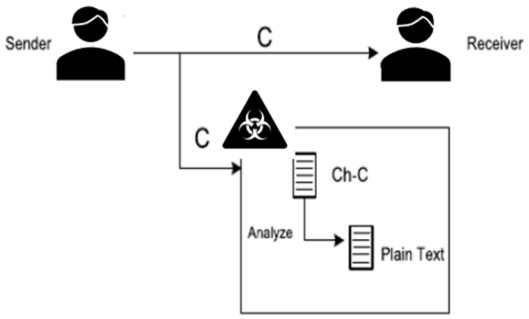

Figure 12. Chosen Cipher text attack scenario.

- *RELATED KEY ATTACK*

A related key attack is one in which the attacker, even without knowledge of the starting values, is able to observe encryption using a variety of keys and comprehends some mathematical relationships relating to the key. For instance, the attacker is aware that the last bits are constant but is unaware of the initial bits. Figure 13 depicts a related-key assault scenario. With ECTWBAN, a new encryption key is produced each time. Even if the attacker discovers the key, he will only be able to decode one encrypted file, not all of them

 doi:10.20944/preprints202312.1609.v1

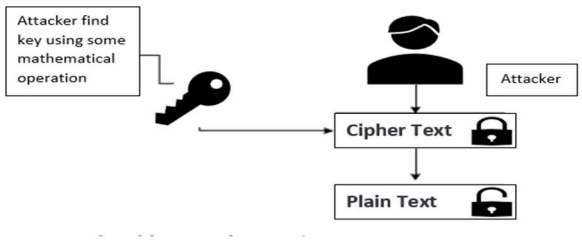

Figure 13. Related key attack scenario.

8. CONCLUSION

The wireless body area network (WBAN) is a new technology in the medical profession that improves quality of life for people, Patients are monitored and treated from miles away by support of wireless body area network of nano sensors. It fascinates whole world, along with-it security and privacy of data is also critical as it is transmitted over the network. Therefore, in this study efficient cryptographic algorithm is proposed for the security of medical data of WBAN, it encrypts the data and make it protected and transmits it confidentially and securely over network

References

1. Dharshini, S., & Subashini, M. M. (2017). An overview on wireless body area networks. 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 1-10.
2. Jabeen, T., Ashraf, H. & Ullah, A. A survey on healthcare data security in wireless body area networks. J Ambient Intell Human Comput 12, 9841–9854 (2021). https://doi.org/10.1007/s12652-020-02728-y
3. Jabeen, T., Jabeen, I., Ashraf, H., Jhanjhi, N., Humayun, M., Masud, M., & Aljahdali, S. (2022). A Monte Carlo based COVID-19 detection framework for smart healthcare. Computers, Materials, & Continua, 70(2), 2365-2380.
4. "Wireless Body Area Network: An overview and various applications." [Online]. Available: https://www.scirp.org/pdf/JCC_2017051714502747.pdf. [Accessed: 24-Oct2022].
5. "CyberGlossary guide and definitions," Fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary. [Accessed: 24-Oct-2022].
6. Chris Brook on Monday August 22, "How much does a data breach cost in 2021?," Digital Guardian. [Online]. Available: https://digitalguardian.com/blog/how-muchdoes-data-breach-cost-2021. [Accessed: 24-Oct-2022].
7. A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," in IEEE Access, vol. 9, pp. 16849-16865, 2021, doi: 10.1109/ACCESS.2021.3052850.
8. M. Azeem et al., "FoG-Oriented Secure and Lightweight Data Aggregation in IoMT," in IEEE Access, vol. 9, pp. 111072-111082, 2021, doi: 10.1109/ACCESS.2021.3101668.
9. 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.
10. Al Hasib, A., & Haque, A. A. M. M. (2008, November). A comparative study of the performance and security issues of AES and RSA cryptography. In 2008 third international conference on convergence and hybrid information technology (Vol. 2, pp. 505-510). IEEE.
11. D'souza, F. J., & Panchal, D. (2017, May). Advanced encryption standard (AES) security enhancement using hybrid approach. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 647-652). IEEE.
12. Rajasekaran, A. S., & Azees, M. (2022). An Anonymous Blockchain-Based Authentication Scheme for Secure Healthcare Applications. Security and Communication Networks, 2022.
13. Haghighi, K. G., Mirnia, M., & Navin, A. H. (2016). Optimizing run-length algorithm using octonary repetition tree. arXiv preprint arXiv:1611.09664
14. Kalaivani, V. (2022). Secure Transmission of Patient Physiological Data in Wireless Body Area Networks Based on Enhanced and Modified RSA Cryptosystem and Run Length Encoding.
15. Shanmugavadivel, G., B. Gomathy, and S. M. Ramesh. (2021) "An Enhanced Data Security and Task Flow Scheduling in Cloud-enabled Wireless Body Area Network." Wireless Personal Communications 120.1: 849-867.
16. Sivasangari, A., Ajitha, P., & Gomathi, R. M. (2020). Light weight security scheme in wireless body area sensor network using logistic chaotic scheme. International Journal of Networking and Virtual Organisations, 22(4), 433-444.

17. [CPABE] Chandrasekaran, B., Balakrishnan, R., & Nogami, Y. (2020). Secure information transmission framework in wireless body area networks. Journal of Applied Security Research, 15(2), 279-287.
18. Basnet, A., Alsadoon, A., Prasad, P. W. C., Alsadoon, O. H., Pham, L., & Elchouemi, A. (2019). A novel secure patient data transmission through wireless body area network:
19. Farooq, S., Prashar, D., & Jyoti, K. (2018). Hybrid encryption algorithm in wireless body area networks (WBAN). In Intelligent communication, control and devices (pp. 401410). Springer, Singapore
20. Jabeen, T., Ashraf, H., Khatoon, A., Band, S. S., & Mosavi, A. (2020). A lightweight genetic based algorithm for data security in wireless body area networks. IEEE Access, 8, 183460-183469.
21. Health tele-monitoring. International Journal of Communication Networks and Information Security, 11(1), 93-104.
22. Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. Journal of Infection and Public Health, 13(10), 1567-1575.
23. L. Morris, "[PDF] analysis of partially and fully homomorphic encryption: Semantic scholar," undefined, Jan-1970. [Online]. Available: https://www.semanticscholar.org/paper/Analysis-of-Partially-and-Fully-HomomorphicMorris/03036b989a3f838a9e130563357492fcc4d76402. [Accessed: 24-Oct-2022].
24. Liu, H., Chen, Y., Tian, H., & Wang, T. (2019). A Secure and Efficient Data Aggregation Scheme for Cloud-Assisted Wireless Body Area Network. J. International Journal of Network Security, 21(2), 243-249.
25. M. Wiener. Cryptanalysis of short rsa secret exponents. IEEE Transactions on Information Theory, 160:553-558, March 1990.
26. Anwar, M., Abdullah, A. H., Butt, R. A., Ashraf, M. W., Qureshi, K. N., & Ullah, F. (2018). Securing data communication in wireless body area networks using digital signatures. Technical Journal, 23(02), 50-55.
27. Monga, C., Raju, K. S., Arunkumar, P. M., Bist, A. S., Sharma, G. K., Alsaab, H. O., & Malakhil, B. (2022). Secure techniques for channel encryption in wireless body area network without the Certificate. Wireless Communications and Mobile Computing, 2022.
28. Kaur, H., Jameel, R., Alam, M. A., Alankar, B., & Chang, V. (2023). Securing and managing healthcare data generated by intelligent blockchain systems on cloud networks through DNA cryptography. Journal of Enterprise Information Management.
29. Hema, T., Raj, K. M., & Rabara, S. A. An Analytic Method of Elliptic Curve Cryptography Security.
30. Li, R., & Jin, C. (2016). Meet-in-the-middle attacks on 10-round AES-256. Designs, Codes and cryptography, 80(3), 459
31. Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.
32. Wassan, S., Chen, X., Shen, T., Waqar, M., & Jhanjhi, N. Z. (2021). Amazon product sentiment analysis using machine learning techniques. Revista Argentina de Clínica Psicológica, 30(1), 695.
33. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In 2018 4th International conference on computer and information sciences (ICCOINS) (pp. 1-5). IEEE.
34. Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.
35. Humayun, M., Alsaqer, M. S., & Jhanjhi, N. (2022). Energy optimization for smart cities using iot. Applied Artificial Intelligence, 36(1), 2037255.
36. Hussain, S. J., Ahmed, U., Liaquat, H., Mir, S., Jhanjhi, N. Z., & Humayun, M. (2019, April). IMIAD: intelligent malware identification for android platform. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
37. Diwaker, C., Tomar, P., Solanki, A., Nayyar, A., Jhanjhi, N. Z., Abdullah, A., & Supramaniam, M. (2019). A new model for predicting component-based software reliability using soft computing. IEEE Access, 7, 147191-147203.
38. Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. Computers and Electrical Engineering, 95, 107374.
39. Nanglia, S., Ahmad, M., Khan, F. A., & Jhanjhi, N. Z. (2022). An enhanced Predictive heterogeneous ensemble model for breast cancer prediction. Biomedical Signal Processing and Control, 72, 103279.
40. Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. Wireless Personal Communications, 85, 671-696.
41. Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. Human-Centric Computing and Information Sciences, 11, NA.

 doi:10.20944/preprints202312.1609.v1

42. Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2021). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. Journal of King Saud University-Computer and Information Sciences, 33(10), 1202-1210.
43. E. Ndashimye, N. I. Sarkar, and S. K. Ray, "A Multi-criteria based handover algorithm for vehicle-to-infrastructure communications," Computer Networks, vol. 185, no. 202152, Article ID 107652, 2020
44. Ray, S. K., Pawlikowski, K., & Sirisena, H. (2009). A fast MAC-layer handover for an IEEE 802.16 e-based WMAN. In AccessNets: Third International Conference on Access Networks, AccessNets 2008, Las Vegas, NV, USA, October 15-17, 2008. Revised Papers 3 (pp. 102-117). Springer Berlin Heidelberg.
45. Srivastava, R. K., Ray, S., Sanyal, S., & Sengupta, P. (2011). Mineralogical control on rheological inversion of a suite of deformed mafic dykes from parts of the Chottanagpur Granite Gneiss Complex of eastern India. Dyke Swarms: Keys for Geodynamic Interpretation: Keys for Geodynamic Interpretation, 263-276.
46. Ray, S. K., Sinha, R., & Ray, S. K. (2015, June). A smartphone-based post-disaster management mechanism using WiFi tethering. In 2015 IEEE 10th conference on industrial electronics and applications (ICIEA) (pp. 966-971). IEEE.
47. Chaudhuri A, Ray S (2015) Antiproliferative activity of phytochemicals present in aerial parts aqueous extract of Ampelocissus latifolia (Roxb.) planch. on apical meristem cells. Int J Pharm Bio Sci 6(2):99–108
48. Hossain, A., Ray, S. K., & Sinha, R. (2016, December). A smartphone-assisted post-disaster victim localization method. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1173-1179). IEEE.
49. Airehrour, D., Gutierrez, J., & Ray, S. K. (2018). A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol. Journal of Telecommunications and the Digital Economy, 6(1), 41-49.
50. Ray, S. K., Ray, S. K., Pawlikowski, K., McInnes, A., & Sirisena, H. (2010, April). Self-tracking mobile station controls its fast handover in mobile WiMAX. In 2010 IEEE Wireless Communication and Networking Conference (pp. 1-6). IEEE.
51. Dey, K., Ray, S., Bhattacharyya, P. K., Gangopadhyay, A., Bhasin, K. K., & Verma, R. D. (1985). Salicyladehyde 4-methoxybenzoylhydrazone and diacetylbis (4-methoxybenzoylhydrazone) as ligands for tin, lead and zirconium. J. Indian Chem. Soc.;(India), 62(11).
52. Airehrour, D., Gutierrez, J., & Ray, S. K. (2017, November). A testbed implementation of a trust-aware RPL routing protocol. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.
53. Ndashimye, E., Sarkar, N. I., & Ray, S. K. (2016, August). A novel network selection mechanism for vehicle-to-infrastructure communication. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 483-488). IEEE.
54. Ndashimye, E., Sarkar, N. I., & Ray, S. K. (2020). A network selection method for handover in vehicle-to-infrastructure communications in multi-tier networks. Wireless Networks, 26, 387-401.
55. Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, "Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study" International Journal of Advanced Computer Science and Applications(IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969