Pertanika J. Sci. & Technol. 32 (6): 2903 - 2929 (2024)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

# Secure Data Aggregation and Transmission System for Wireless Body Area Networks Using Twofish Symmetric Key Generation

**Insozhan Nagasundharamoorthi[1]*, Prabhu Venkatesan[2] and Parthasarathy Velusamy[3]**

[1]*Department of Computer Science & Engineering, VelTech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Tamil Nadu 600062, India*

[2]*Department of Electronics and Communication Engineering, VelTech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Tamil Nadu 600062, India*

[3]*Department of Computer Science Engineering, Karpagam Academy of Higher Education (Deemed to be University), Tamil Nadu 641021, India*

## ABSTRACT

Nowadays, Wireless Body Area Networks (WBANs) are mostly used in the healthcare industry. They represent a portable, inexpensive network that exhibition adaptability. The data developed using WBAN devices is vulnerable to transmission-related internal and external attacks; nevertheless, this vulnerability arises due to resource restrictions; by employing data aggregation technologies to conduct statistical analyses of medical data while protecting patient privacy, medical professionals can enhance the precision of diagnoses and assist medical insurance firms in selecting optimal plans for their clients. Maintaining the confidentiality and integrity of sensitive health information becomes more stimulating at the stages of aggregation and transmission due to security issues. This study proposes a novel method, Twofish Symmetric Key Generation (TFSKG), combined into a Secure Data Aggregation (SDA) and transmission system intended for WBANs. The Twofish technique is animatedly employed to make the secure symmetric keys chosen for its robust encryption capabilities. These keys are used to encrypt and decrypt aggregated health data through transmission. The proposed TFSKG-SDA method implements effective algorithms for aggregating data to safeguard end-to-end privacy and preserve data accuracy while reducing bandwidth consumption. Thus, for improved performance, an innovative genetic algorithm for data security is presented in this study. This paper introduces TFSKG-SDA, a system that, by employing rigorous simulation testing, enhances security protocols, resistance against recognized threats, and data transmission

ARTICLE INFO

*Article history:*
Received: 07 February 2024
Accepted: 01 August 2024
Published: 25 October 2024

DOI: https://doi.org/10.47836/pjst.32.6.25

*E-mail addresses*:
insozhann@gmail.com (Insozhan Nagasundharamoorthi)
prabhu.cvj@gmail.com (Prabhu Venkatesan)
sarathy.vp@gmail.com (Parthasarathy Velusamy)
* Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

efficacy in the context of resource-constrained WBANs. We assess the encryption strength, computational cost, and communication efficiency of the TFSKG- SDA method to prove its significance to real-world healthcare applications.

*Keywords:* Data privacy, medical data, secure data aggregation, transmission system, Twofish symmetric key generation, wireless body area network

## INTRODUCTION

The development of technology for wireless communication in recent years has transported unique ways that incorporate wireless networking and modern healthcare monitoring (Salem et al., 2020). Significant progress in healthcare has been made possible due to these growths. WBANs are advanced for personalized treatment, real-time monitoring of health, and analysis. The transmission system is vital to WBAN, as it simplifies the dependable and efficient transfer of physical data within the human body. Wireless Body Area Networks (WBAN) make it easy for small, energy-efficient sensor nodes to communicate with one another and the rest of the human body with the help of transmission technology. This dangerous network of sensor nodes is essential for the quick and correct delivery of health-related data to researchers, doctors, and patients. Repeated assembly of important health comprehensions like temperature, heart rate, and other physical parameters facilitates the unrestricted exchange of serious information. Because of these aspects' substantial impact on data transmission latency, energy consumption, and reliability, researchers in this area have focused on transmission system design and efficiency.

Van Dam presented the WBAN conception in 2001 as a result of progress in low-energy devices and the Internet of Things (IoT) (https://www.geeksforgeeks.org/wireless-body-area-network/). Biosensor nodes devoted to the human body should be used in the WBAN network to enhance patient care and overall life excellence. Combining biosensor–implanted nodes may offer physical data, including blood pressure, blood glucose, ECG and EEG parameters. With technical development, the WBAN has become a vital implement for slightly monitoring patients' health. The IoT simplifies the sample collection, storage, processing, and transmission of essential health data in hospital IT systems (Tseng et al., 2019). Medical devices using wireless networks can track vital signs, such as respiration rate (RR) (Santos et al., 2020), pulse, heart rate (HR), temperature (T), blood pressure (BP) (Wang et al., 2019), electrocardiogram (ECG) (Abualsaud et al., 2018), electroencephalogram (EEG) (Hu et al., 2016), electromyogram (EMG) (He et al., 2017) an anonymous authentication for WBAN (Subramani et al., 2023) fog-based data aggregation Scheme for WBANs (Liu et al., 2021) and other health-related variables. These devices depend on healthcare cost management, public health, and hospital congestion expectations.

Physical indicator data transmitted overhead from wearables or biosensors is more probable to be overhead, interrupted, or altered during transmission because the data is

transmitted across open channels prior to data aggregation. Additionally, manipulated health-related data may cause clinicians to make incorrect conclusions. Worse, it could result in medical mishaps that deteriorate a patient's condition. If health insurance companies colluded to increase premiums, the patient would suffer. A person looking for coverage may allow many insurance providers to review their medical information to obtain the best possible health insurance rate. For this reason, the patient may want access to the sensitive data gathered by medical sensors to be restricted to authorized individuals and anonymous to one another. As a result, preserving patient privacy when aggregating medical data while achieving anonymity across multiple approved recipients is crucial and challenging.

The issues of fine-grained access, multiple recipient anonymity, and data privacy aggregation can currently be solved using a variety of cryptographic algorithms. However, these solutions only address a fraction of these issues and do not solve all three simultaneously. Two viable options to address the three security concerns in WBAN mentioned above are attribute-based encryption (Hu et al., 2016) and broadcast encryption. However, these techniques typically involve lengthy ciphertexts, private keys, public parameters, and some laborious processes. IoT body sensors and other low-energy wearable devices are not suited for many attribute-based encryption methods and broadcast encryption techniques now in use. On the other hand, more problems with efficiency or data security occur when these methods are coupled with data aggregation. For example, complex computations can lead to communication latency problems and recipient information may be exposed due to attributes in attribute-based encryption systems, among other issues.

The proposed TFSKG-SDA system is important as it provides a robust encryption framework that protects the security and integrity of patient information while preventing illegal access and modification. Utilizing Twofish, a well-known cryptographic technique known for its strength and dependability, the system generates a secure communication channel across wireless body area networks, promoting confidence and compliance with severe privacy rules. In addition, the system's improved data aggregation approaches progress network performance, permitting more accurate and timely medical data processing. Lastly, this new explanation not only progresses the security of wireless healthcare systems but also assists in better patient care outcomes by allowing the safe and fast transmission of essential medical information.

The primary contribution to this study is:

- To develop a novel method to overcome these difficulties by developing the combination of Twofish Symmetric Key Generation (TFSKG) into a Secure Data Aggregation (SDA) and transmission system established for WBANs
- Secure symmetric keys can be generated by dynamically employing the Twofish algorithm, renowned for its robust encryption capabilities. These keys are crucial

for transferring aggregated health data securely because they provide encryption and decryption.

- The proposed system uses outstanding data aggregation algorithms to reduce bandwidth usage without sacrificing data accuracy. Through rigorous simulations and performance evaluations, TFSKG-SDA improves security measures, resilience against common attacks, and data transmission efficiency in the resource-constrained setting of WBANs
- Assessing the TFSKG-SDA system's encryption strength, computational overhead, and communication efficiency proves its applicability to practical healthcare applications.

## LITERATURE SURVEY

Zhong et al. (2022) conducted extensive and in-depth research on the demands and challenges of WBANs. They focused on WBAN standards and issues after first carefully examining WBAN applications. An original aspect of the article was its investigation of WBAN data transfer standards and technology. A brief discussion of the significance, features, and mitigation of energy usage in the WBAN was provided. The article is overly cursory, and the mention of security and privacy issues is one of its shortcomings. By implementing artificial intelligence algorithms and protocols that progress the speed and lower the energy consumption of the WBAN, this study seeks to address this gap. It also categorizes dissimilar types of attacks and highlights common security problems in WBANs.

Dynamic capability testing in numerous WBAN scenarios was given by Thippun et al. (2023). The use of IEEE 802.15.4 low-power sensor nodes in establishing a WBAN allowed this to be achieved. The experimental results show that the packet delivery ratio (PDR), which measures the reliability of WBAN connections, is affected by several significant elements. The findings demonstrate that the diverse environment testbed can impact network performance for WBAN data transmission. The study recommends that to achieve a Packet Delivery Ratio (PDR) of more than 90% and excellent network reliability in all test situations, a packet interval length longer than 15 ms is essential.

Azees et al. (2021). While protecting patients' and physicians' privacy, the recommended anonymous authentication technique aids in confirming the credibility of both parties. Although cryptographic encryption systems like AES and DES guarantee privacy, the challenges related to key sharing and key size significantly hinder the achievement of suitable security levels. Therefore, associated with other existing encryption algorithms, this study's efficient affine cipher-based encryption method needs a reduced key size and proposes a high level of privacy. To ensure its suggestions provide more protection, the security analysis of the recommended work shows how strong its security is against a variation of harmful security risks. For WBAN with limited resources, Subramani et al.

(2022) provide a computationally efficient privacy-preserving anonymous authentication technique. It also protects sensor physical security and biological information (BI) confidentiality and provides WBAN users conditional privacy.

With the energy constraints of tiny wireless sensors in mind, Wang et al. (2020) generated a physiological data transmission system that is dependable and efficient. They consider a particular WBAN scenario aimed at building an adaptive power control system and allotting time slots to improve total energy efficiency for performing health monitoring duties. They used a Markov decision process (MDP) to express the maximizing problem with latency and the energy budget restrictions of the sensors. According to the random oracle model, Kumar (2020) established the security of the anonymous authentication technique for wireless body area networks. Here, we cryptanalyze this system and develop an attack model that illustrates a key replacement assault that preserves client anonymity by having the adversary substitute a user's public key with a predetermined value. As a result, this method is unreliable and insufficient for creating a safe wireless band network.

Kaleem and Devarajan (2023) proposed WBAN utilizing data transmission techniques based on prediction. This method uses anticipated rather than actual sensor values while maintaining the same level of data quality. The quantity of data transferred between the base station and sensor nodes is being minimized. It is still very difficult to accurately forecast results within a given error margin. Most of the time, the base station will adjust the transmission settings using a prediction model, lowering the quantity of data provided to the sink. Despite having a lower computing cost and a faster recall path, this model performs better than its predecessors.

Mehmood et al. (2020) suggested a communication method based on trust to guarantee the dependability and confidentiality of WBAN. A cooperative communication approach guarantees dependability and a cryptography method protects privacy. For IoT devices, Mathews and Jose (2024) proposed a number of lightweight cryptographic (LWC) protocols and offered a thoughtful investigation into present ubiquitous ciphers. Also, the paper evaluates the security of numerous newly proposed hybrid homomorphic LWC and lightweight (LW) block ciphers.

In this work, Khan et al. (2022) proposed an actual and safe architecture for ABEs by outsourcing compound encryption and decryption tasks. We present a workable substitute for expensive pairing procedures using elliptic curve scalar point multiplication as the core technology for Attribute-Based Encryption (ABE). It also supports the verifiability of outsourced medical data and attribute/user revocation. The recommended technique using the selective-set security model is considered secure under the elliptic curve decisional Diffie-Hellman (ECDDH) assumption u. Moreover, this method is appropriate and effective for access control in eHealth smart societies. This efficiency is proven by performance calculations and top scores obtained using the fuzzy logic-based EDAS (Evaluation based on Distance from Average Solution) approach.

The Mobile Agent-Based Data Aggregation (DA) method for WBANs was established by Mehmood et al. (2022) and is a dependable energy conservation technique. Cluster heads are appointed when the network has been separated into groups according to the approach. The base station then sends a mobile agent to collect data from these cluster heads. If problems compromise network performance with the present route, the scheme swiftly progresses to a backup approach.

Two software agents are introduced in a fog node by Mohapatra et al. (2022): the Software agent for Blockchain Formation and Monitoring (SAB), which implements a blockchain security framework, and the Software agent for Network Formation and Monitoring (SAN), which oversees and manages the Internet of Things device network. They use group key sharing with three different AES versions (128, 192, and 256) to enable encrypted communication within blockchain blocks. An approved IoT device uses a proof of work (PoW) based on AES 128 for block addition. Additionally, the blockchain uses SHA 256 for hashing. The experiment considers three systems, System 1, System 2, and System 3, with varying design parameter choices.

Shyja et al. (2023) discussed a link quality and energy effectual optimal clustering-multipath (LEOC-MP) system's primary goals are to ensure node-to-node link quality, extend network life, and compute high-performing cluster heads to ensure reliable multipath data transfer. This project was completed in three stages. First, an effective simplified clustering method for data collection from body sensors is obtainable based on an enhanced pelican optimization (ICO) algorithm. Numerous design restrictions are applied to node rank computation, energy efficiency, network quality, path loss, distance, and delay.

Kumar and Chand (2020) suggested creating a cutting-edge, publicly verifiable, secure, and effective cloud-based IoMT smart healthcare system. The system innovation secures data transfer via an escrow-free identity-based aggregate signcryption (EF-IDASC) approach, which is also suggested in this paper. The proposed EF-IDASC approach aggregates and encrypts medical data gathered from multiple implanted sensors on the patient's body. The data is then sent via a smartphone to a medical cloud server. Kumar and Chand (2021) created the identity-based anonymous authentication and key agreement (IBAAKA) protocol for cloud-assisted WBANs to ensure user anonymity and enable mutual authentication. Based on the widely accepted computational Diffie-Hellman assumption and the random oracle model, our security analysis shows that this IBAAKA approach is provably secure and satisfies the relevant security requirements.

Anh et al. (2023) developed multiple-input multiple-output (MIMO) systems based on a cell-free architecture incorporating multiple access points (APs) supporting numerous sensors simultaneously. They suggest a novel system model in which sensors are dispersed throughout the body and communicate directly with APs, as opposed to via a coordinator. The transmission power control method for uplink data development takes into account

minimizing interference generated by several sensors transmitting signals simultaneously to improve the system's spectrum efficiency.

### Limitations of the Existing System

- The available bandwidth for communication in WBANs is frequently constrained, resulting in data transmission rate constraints. Transferring enormous amounts of data, such as high-resolution medical images or continuous streaming of high-frequency physiological signals, can be a considerable difficulty.
- The human body is a complex medium that can induce signal attenuation and interference. Tissues, organs, and bodily fluids can degrade signals and shorten the effective communication range. Furthermore, interference from nearby electronic devices and rival wireless networks might lower connection dependability.
- WBAN devices frequently operate on batteries, so energy consumption is an important consideration. The energy required for wireless data transmission is substantial, and finding the sweet spot between efficient energy use and dependable connection is no easy feat.
- Because the human body is always changing, so can the placement and movement of any devices implanted or connected to it. Due to its dynamic nature, assembly quality could fluctuate, leading to communication interruptions or decreased reliability, particularly in active or mobile environments.

## MATERIALS AND METHODS

The proposed system model uses the combination of TFSKG-SDA and WBAN transmission. Twofish algorithm dynamically generated secure symmetric keys, well-known for its strong encryption capabilities. These keys ensure end-to-end confidentiality by encrypting and decrypting aggregated health data while it is transmitted. By using effective data aggregation techniques, the proposed method reduces bandwidth consumption without sacrificing data accuracy u. Simulations and performance testing have displayed that our TFSKG-SDA solution improves data transmission efficiency, security, and resilience against common attacks in resource-constrained WBANs. There are practical healthcare uses for the TFSKG-SDA system, as displayed by an inspection of its computational overhead, communication efficiency, and encryption strength.

The proposed TFSKG-SDA system provides a robust encryption way to preserve the security and integrity of sensitive information, which is mainly important in healthcare applications. By employing Twofish, known for its powerful cryptographic properties, the explanation reduces the risks connected with data breaches. It progresses the efficiency of data aggregation processes, optimizing network speed while adhering to high-security values. The security and dependability of communication channels for transmitting medical

data are enhanced by this new method, suggestively improving the safety of wireless body area networks.

## System Model

Our proposed TFSKG-SDA model uses four main dissimilar entities: trusted authority (TA), wearable devices, multiple data users (the receivers), and cloud server (CS). Figure 1 displays the proposed diagram.

(i) Trusted Authority:

Its responsibilities include launching the system overall, supplying data users with necessary authentication and organizational services, and offering wearables equipped with Internet of Things sensors.

(ii) Cloud Server:

Our system's cloud server collects and stores data with ample storage capacity and robust processing power.

(iii) Wearable devices:

Wearable devices collect data in real-time by observing vital signs like heart rate and blood pressure using a network of Internet of Things (IoT) sensors. Doctors can then utilize the encrypted data for future diagnostic purposes by sending it to a server over the Internet.

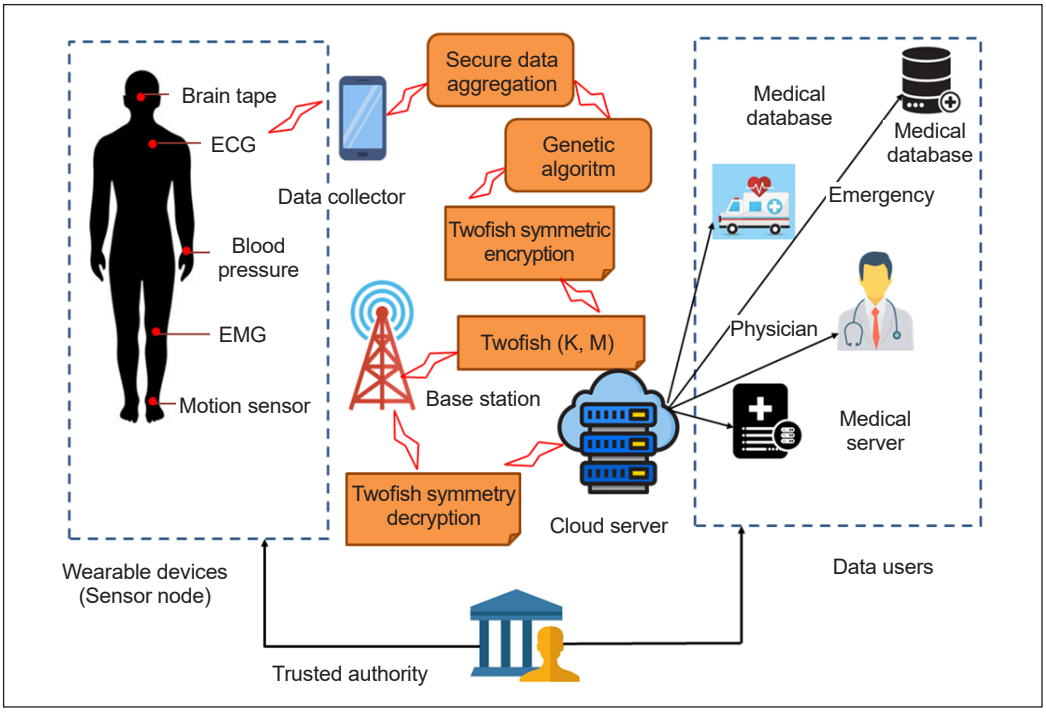


*Figure 1.* The proposed technique of TFSKG-SDA

(iv) Multiple Data Users:

They function as data recipients. Data users, such as doctors and medical facilities, receive the encrypted version of the patient's aggregated data from the cloud server for a specific duration. Subsequently, with the decryption key still in their possession, they retrieve the plaintext of this aggregated data.

### *System Configuration*

A TA sets up the system's public parameters at this stage.

$pk \leftarrow Setup(1^k)$: The public key $pk = (po, PO, GP)$ for the entire system is retrieved by the trustworthy authority executing the Setup procedure by entering k, where $GP =< PO >$ is an additive cyclic group of prime order $po$ produced by a generator $PO$. The element $H_0$ was randomly selected for group G. Furthermore, it selects a cryptographic hash function $H_1 : \{0,1\}^* \rightarrow Z_{po}$. In addition, it selects two random values $u_1, u_2 \in Z_{po}$ to compute $GP_1 = u_1 PO \ and \ GP_2 = u_2 H_0$. Table 1 shows notations and descriptions of the proposed method.

Table 1
*Describes the main notations in the proposed method*

| Notations | Description |
|---|---|
| $M_e$ | Message |
| $C_t$ | The current time of sent message |
| $Sig(BS_n)$ | Signature of Base station |
| $h$ | Hash function |
| $k_{id}$ | Sensor node's identity |
| $PU_K$ | Public key |
| $C_{kid}$ | A certificate was issued to identify the sensor node |
| $c_e$ | Certificate expiration time |

### Twofish Symmetric Key Generation

The National Institute of Standards and Technology's AES design standards follow the Twofish symmetric block cipher, which utilizes a single key and a predefined block configuration to process 128-bit input messages. There are three different key length options: 128 bits, 192 bits, or 256 bits. Because of its flexible form and sturdy keys, it stands out. It is fast on both hardware and software, efficient, and performs well across a range of systems. And lastly, it works well for stream ciphering (Zhang & Dong, 2022; Rane, 2016). The 16-iteration Feistel network is the basis of Twofish's main functionality. Before starting the input whitening procedure, Twofish divides the 128-bit plaintext into four 32-bit block words called W0, W1, W2, and W3. Subsequently, XOR combines each word with four additional 32-bit words (K0, K1, K2, and K3). The outputs of the whitening procedure are given into the modules and F function (Apoorva, 2013). The Fixed Maximum Distance Separable (MDS) matrix and the Twofish directive function F conform to the same mathematical code. Each of the four S-boxes in this function has an 8-bit input, an 8-bit output, and five operational components. It also involves four dependent keys. 232

is added modularly to a simple 32-bit mixing process known as the pseudo-Hadamard transform. Twofish does further output whitening after 16 cycles.

As displayed in Figure 2, the XOR operation is replaced with a new operation in every cycle of the Twofish algorithm. This innovative approach involves the utilization of multi-state tables and dynamic block sizes, characterized by their intricate design and rapid retrieval speeds, leading to enhanced computational efficiency. The fundamental elements constituting the foundation of the

Twofish algorithm includes:

**i. Feistel:** The fundamental approach, initially introduced by Horst in the DES algorithm, can be employed to transform any function F into a permutation within a block cipher. This process involves generating two blocks from the input block, followed by the repeated execution of identical procedures.

**ii. Confusion and Diffusion:**

In 1949, Shannon introduced encryption methods that incorporate both confusion and diffusion. Confusion is introduced through the replacement approach, intensifying the complexity of the relationship between the ciphertext and the key to enhance the challenge of deciphering the plaintext. Also, diffusion employs the permutation approach (Geetha et al., 2022; Kareem et al., 2020) to elevate the statistical intricacy between the plaintext and ciphertext.

---

Algorithm 1

*pseudocode for the Twofish algorithm*

Pseudo code for Twofish algorithm:

1 Initialize:

Set the encryption algorithm=“two fish”

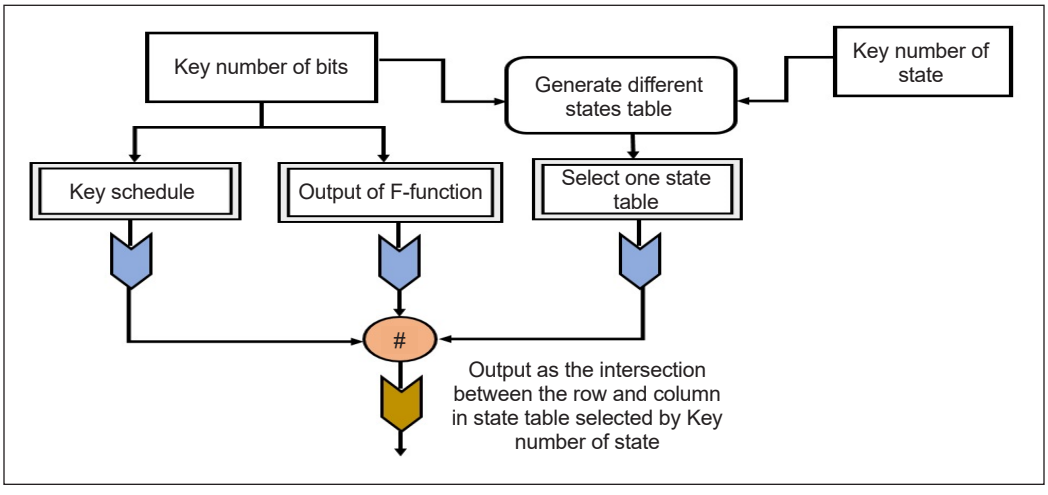


*Figure 2.* Workflow of the Twofish algorithm

```
        crypt.put _Crypt Algorithm (“two fish”);
        crypt.put_CipherMode (“ebc”);
         // Electronic code block (EBC)
2       The length of the key can be 128,192,256.
        Crypt.put _KeyLength (256);
3       Crypt.put_Padding scheme (0);
4       Crypt.put_Encoding Mode (“hex”);
5      String Hex =“000102030405060708090A0B0C0D0E0F”
       Crypt.Set EncodedIV (Hex,”hex”);
6      String keyHex=000102030405060708090A0B0C0D0E0F1011112131415161
           71819A1B1C1D1E1F
  Crypt.SetEncodedKey (keyHex,”hex”);
7           Encrypt a string….
       The input string is 44 ANSI characteristics (i.e.44 bytes),so
       the output should be 48 bytes (a multiple of 16)
       System.out.println (encStr);
8      Finally, decrypt:
       String decStr =crypt.decryptStringENC (encStr);
       System.out.println (decStr);
```

**iii. Substitution Boxes (S-Box) and MDS Matrices:** Driven by a table and with adjustable input and output sizes, the S-box functions as a non-linear replacement. An algorithm or a random technique can be used to generate it. Twofish uses two predetermined 8-by-8-bit permutations, including the necessary components, to generate four different S-boxes. A composite vector of 32 bits is formed through a linear mapping of two fields, ‘a’ and ‘b,’ with components expressed as (a + b). This method is utilized to ascertain the MDS code for a specified field. The MDS matrix, a 4×4 transformation matrix, provides diffusion. Multiplication of four-byte vectors in the GF (28) matrix is achieved by the irreducible polynomial $x^4 + x^6 + x^5 + x^3 + 1$.

**iv. Pseudo-Hadamard Transforms (PHT):** The PHT encourages dispersion due to its inherent mixing capability. To illustrate, let us consider two inputs, denoted as ‘a’ and ‘b.’ The following is a description of the 32-bit PHT:

**v. Whitening:** It is crucial to employ XOR operations on plaintext and key components before and after the initial round to enhance the key’s defense against potential attacks.

### *Functions Used in Twofish*

***1. Function F.*** Function F is an important component that modifies the 128-bit plaintext post-whitening in the Twofish Feistel network. It is a significant and interdependent role.

Three important parameters—round number (r), determining subkey selection, and two words (P0, P1)—are requisite for properly executing this function. Before entering the g function, R1 undergoes an 8-bit left rotation, yielding T1, while R0 is directly fed into the g function to generate T0. Combining two words from the expanded key forms a Piling-up Hash Table (PHT) using the resulting outputs T0 and T1. Synopsis of the F function Equations 1 to 4 are as follows.

$$T_0 = g(R_0) \quad [1]$$

$$T_1 = g(ROL(R_1, 8)) \quad [2]$$

$$F_0 = (T_0 + T_1 + K_{2r+8}) \bmod 2^{32} \quad [3]$$

$$F_1 = (T_0 + 2T_1 + K_{2r+9}) \bmod 2^{32} \quad [4]$$

***2. Function g.*** The fundamental component of the Twofish algorithm is its core function, 'g,' which is essential to organizing inputs into four bytes per word, each consisting of 32 bits. Subsequently, the S-box is employed to process each byte, and the MDS matrix combines the four S-box outputs, resulting in a 32-bit output. A brief explanation of the g function Equations 5 to 8 as follows.

$$x_i = \left\lfloor X / 2^{8i} \right\rfloor \bmod 2^8 \qquad i = 0,..3 \quad [5]$$

$$y_i = s_i[x_i] \qquad I = 0,...3 \quad [6]$$

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} \square & \square & \square & \square \\ MDS & & & \\ \square & \square & \square & \square \end{pmatrix} \cdot \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} \quad [7]$$

$$Z = \sum_{i=0}^{3} z_i . 2^{8i} \quad [8]$$

Z represents the outcome of the function g, and $s_i$ denotes the S-boxes influenced by the key. Performing addition in GF ($2^8$) is equivalent to the exclusive OR (XOR) operation on the bytes. Thus, this can be considered the "inherent" mapping. Algorithm 1 shows the pseudocode for the Twofish algorithm.

## Secure Data Aggregation

In this step, we will describe the operation of the suggested data aggregation system. A wearable implant gathers physiological data from the user and employs the

AHEncrypt method to generate a verified homomorphic ciphertext based on this data. $CT(M',T) \leftarrow AHEncrypt(pk, sk_w, M', T, PCL)$: Using the public parameters $pk$, the private key $sk_w$ of the wearable device, the sensed data $M'$ and time t, and the public key list PCL of the doctor users serving as receivers as inputs, the algorithm runs as follows:

1) It selects $k_T \in Z_p$ at random and computes $B_i = k_t.H_0 + sk_w.p_i$ for $p_i \in PCL$;

2) $p_i \in PCL$ creates a polynomial with a degree $|PCL| = -1$, specifically, Equation 9 relates to polynomial interpolation.

$$f_i(y) = \prod_{j=1, j\neq i}^{|PKL|} \frac{y - y_j}{y_i - y_j} = \sum_{j=0}^{|PKL|-1} b_{i,j} y_j \bmod p \quad [9]$$

Where the number of doctor users' public keys in the PCL- is indicated by $y_i = H_1(sk_w, p_i)$ and |PCL|.

3) $f_i(y)$ are computed, after all. Once the necessary corrections are identified, these polynomial coefficients are employed in the computation process. Given Equation 10, this could be related to ciphertexts in cryptographic contexts.

$$CT_i = \sum_{j=1}^{|PCL|} b_{j,i} B_j \quad (i = 0, ....., |PCL| - 1) \quad [10]$$

4) After that, it computes. $U_1$ and $U_2$ are the results of Equations 11 and 12, potentially representing an output value related to a cryptographic operation, computation, or message encoding.

$$U_1 = M'PO + k_T H_0 \quad [11]$$

$$U_2 = sk_w.M'.G_1 + H_0 + k_t + GP_2 \quad [12]$$

5) The ultimate homomorphic ciphertext generated by Equation 13.

$$CT(M,T) = (CT_0, ..., CT_{|PCL|-1}, U_1, U_2) \quad [13]$$

In addition, Equation 14 shows for each $CT_i$.

$$\begin{aligned} CT_i &= \sum_{j=1}^{|PCL|} b_{j,i} B_j = \sum_{j=1}^{|PCL|} b_{j,i} (k_t H_0 + sk_w.p_i) \\ &= k_T . \boxed{\sum_{j=1}^{|PCL|} b_{j,i}, H_0} + \boxed{sk_w . \sum_{j=1}^{|PCL|} b_{j,i}, p_i} \end{aligned} \quad [14]$$

With a constant PCL receiver set, computing $CT_i$ simply requires one addition and multiplication operation, as known from the $CT_i$ computation method.

A wearable device requires real-time data observation and uploading to a cloud server. As such, ciphertexts $CT(M_j, j)$ will be sent to the cloud server when $j \in TimeIndex$ needs them. Afterward, the wearable device's data is kept on the cloud server as a Time Series Data Table.

Obtaining a patient's pathology data from time $T_1$ to time $T_n$ is as simple as sending a request to a cloud server. In the given time range ($T_1$ to $T_n$), the cloud server must gather the sensed data from the wearable device using the approved aggregation technique.

Equations 15 to 18 show that it decodes the ciphertexts of the detected data $CT(M_1, T_1), ...., CT(M_n, T_n)$ as $(CT_{i,0,....,} CT_{i|PCL|,} V_{i,1}, V_{i,2})$ for $i \in [1, n]$ after receiving them. The aggregate is then computed.

$$\overline{CT}_0 = \sum_{j=1}^{n} CT_{j,0} = a_{0,0} \sum_{j=1}^{n} B_{j,0} + .... + a_{|PCL|,0} \sum_{j=1}^{n} B_{j|PCL|} \quad [15]$$

$$\overline{CT}_i = \sum_{j=1}^{n} CT_{j,i}, \quad i =, ..., |PCL| - 1 \quad [16]$$

$$\overline{U}_1 = \sum_{j=1}^{n} U_{j,1} = \sum_{j=1}^{n} M_j P + \sum_{j=1}^{n} k_j H_0 \quad [17]$$

$$\overline{U}_2 = \sum_{j=1}^{n} U_{j,2} = s. \sum_{j=1}^{n} M_i . G_1 + nH_0 + \sum_{j=1}^{n} k_j G_2 \quad [18]$$

The j-th ciphertext, $B_i$ matches the $B_i$. Let us assume $M = \sum_{j=1}^{n} M_i$ and $K = \sum_{j=1}^{n} k_j$. The combined result then has the structure shown in Equation 19.

$$CT_{M,t[1,n]} = (\overline{CT}_0, ..., \overline{CT}_{|PCL|-1,} \overline{U}_1, \overline{U}_2) \quad [19]$$

**Data Protection Using Genetic Algorithm (GA)**

The genetic algorithm (GA) is a well-known and widely used optimization method that draws inspiration from natural selection. By modeling the search for solution space after an environmental process, the GA takes into account the Darwinian theory of species evolution. Each member of a GA population—a chromosome—stands for a possible answer to the problem. The objective function serves to define the problem that is being solved. The value that symbolizes the quality of an individual is assigned to them based on how well they fit the objective function. One important metric is this number, which is called the individual's fitness. Highly esteemed people are more likely to be chosen for the next generation. The three operators in GAs are selection, crossover, and mutation. In selection, individuals are chosen based on their fitness values from the previous generation. In crossover, two individuals are chosen to exchange parts of themselves. Mutation involves randomly changing the values

of specific genes. In this paper, we study approaches to strengthen the data protection mechanisms of WBANs by including Genetic Algorithms (GAs) in its transmission system. Genetic algorithms have successfully optimized complicated problems by drawing on genetics and natural selection concepts. Data transmission efficiency and security in WBANs are the focus of this research, which aims to use their adaptive and evolutionary characteristics.

***Mathematical Modelling of Genetic Algorithm***

Equation 20 shows that W denotes the provisional data, updated in accordance with operational procedures, and x is the plaintext subjected to an XOR operation with k, which is the produced key's value.

$$W = x \oplus k \quad [20]$$

Equation 21 performed mutation values assigned to the indexes of the data array.

$$W_1 = M.T \quad [21]$$

$W^{c1}{}_1$ *and* $W^{c2}$ signifying four bits each form the entire 8 bits of data, equivalent to $W_2$ shown in Equation 22.

$$W_2 = W_1 C_1 \rightarrow W_1 \bar{C}_1 \quad [22]$$

The following step in Equation 23 shows that a crossover operation is carried out following the division of the data into two halves. When the values on the right and left sides are switched, $W_3$ results.

$$W_3 = W_1 \bar{C}_2 \rightarrow W_1 \bar{C}_1 \quad [23]$$

The $W_3$ short-term produced cipher is replaced with S-box values and assigned to $W_4$ shown in Equation 24.

$$W_4 = W_3 \rightarrow S_{box} \quad [24]$$

Now,

$$W_5 = W_4 \rightarrow A \min o_{Acid} \quad [25]$$

Additional amino acid coding values over the $W_4$ created data will equal to $W_5$ shown in Equation 25.

Using Equation 26, which recognizes "0" as "A" and "1" as "B," the resulting strings of A's and B's equal Z6, the ciphertext.

$$W_6 = W_5 \rightarrow String_{Mapping} \quad [26]$$

**Transmission Security**

Using the $HDec(pk, p_w, sk_w, CT_{M,T[1,n]})$ algorithm, the doctor user decrypts the aggregated findings $CT_{M,T[1,n]}$ that he receives from the cloud server.

$M \leftarrow AHDec(pk, p_w, sk_w, CT_{M,T[1,n]})$. The public parameters $P_k$ wearable device, public key, $p_w$ doctor user private key, $sk_w$ and aggregated output $CT_{M,T[1,n]}$ are the inputs.

1) To compute $y_i = H(sk_i, p_w)$, it utilizes its private key ski.

2) After that, Equation 27 calculates *W.*

$$W = \overline{C}T_0 + \sum_{j=1}^{|PCL|} y_i^j \overline{C}T_j \quad [27]$$

3) The aggregated plaintext is then producing Equation 28.

$$M = \log_{PO}(\overline{U}_1 - W + n.sk_i.p_w) \quad [28]$$

4) Finally, Equation 29 can be used to verify the retrieved plaintext's correctness.

$$\overline{U}_2 = M.u_1 p_w + n.H_0 + u_2\left(\sum_{j=1}^{n} k_j H_0\right) \quad [29]$$

Where $(\sum_{j=1}^{n} k_j H_0) = W - n.sk_i.p_w$.

**Advantages of the Proposed Method**

- Twofish is a symmetric key block cypher recognized for its strong security. It proposes strong encryption. Because of its high level of encryption, data transmitted over a wireless body area network is protected from tampering and unauthorized access.
- TFSKG progresses key generation efficiency, which is important for secure communication in wireless band networks. By ensuring cryptographic keys are created swiftly and securely, efficient key generation lowers the possibility of key compromise and improves system security as a whole.
- Twofish has been considered to withstand a range of cryptographic attacks, such as linear and dissimilarity cryptanalysis. Because of this resistance, the security system is more resilient and complete, and it is more problematic for attackers to take advantage of encryption algorithm flaws.
- Within the WBAN, SDA lets efficient data aggregation. SDA lets information be analyzed and transmitted rapidly while preserving security and privacy by safeguarding that collective data is private and immutable

The choice of the TFSKG method for obtaining WBAN data is sufficient because of its many features. To initiate, Twofish is well-known for its strong security features, which

provide extreme encryption strength and resilience to different cryptographic attacks. Its symmetric key creation development authorizes data to only be decrypted by authorized parties with the exact key, increasing the secrecy and integrity of data transmission inside WBAN. Furthermore, Twofish is impeccable for WBANs due to its capability to handle short data packets regularly encountered in healthcare monitoring performances. Its nearer encryption and decryption methods reduce computing costs, declaring that real-time data transfer performance and latency are not negatively impacted, which is well-known in healthcare circumstances. Also, the evolutionary algorithm simplifies key management and distribution by regularly generating and growing cryptographic keys based on predefined parameters such as randomness and entropy. It lowers the overhead of manual key management, confirming smooth operation and scalability in large-scale WBAN allocations.

## RESULTS

With a 2.4 GHz ISM band operation, 2 MHz bandwidth, and 0 dBm of transmission power, our wireless signal can be detected using IEEE 802.15.4 values. This setup was implemented so that our entire university could contribute to the RSSI dataset. Each of the four MICAz Mote modules has a 2.4 GHz ZigBee transceiver and an ATmega128L low-power MCU, and the housing can hold two AA 1.5-volt batteries. The individual has ten chip antennas placed thoughtfully on their left arm, right arm, chest, left finger, right front pocket, left front pocket, right hip pocket, and left hip pocket. Several simulation configurations are listed in Table 2 and were taken into consideration for the research.

A packet was sent from each antenna at intervals of 0.1 seconds during 150 seconds in each experimental session to measure the Received Signal Strength Indicators (RSSIs) at the remaining nine antennas. We used a combination of indoor and outdoor settings to experiment. The participant performed a variety of poses and movements, including sitting for 20 seconds, standing up for 20 seconds, standing motionless for 20 seconds, turning about for 20 seconds in a room, walking for 30 seconds in a hallway and 40 seconds outside, sitting down, and sitting motionless for 20 seconds outside. Genetic algorithm with Markov decision process (GA-MDP) (Roy et al., 2021), Multiple-input multiple-output (MIMO) (Anh et al., 2023), hospital-centered wireless body area network (HCWBAN) (Dangi et al., 2020), compensation adaptive sampling algorithm and resuscitation adaptive sampling algorithm (RASA -CASA) (Lee & Lee, 2017), convolutional neural network, and long-short-term memory network (CNN-LSTM) (Paulraj & Baburaj, 2023) are using the existing systems used in research.

Table 2
*Analysed simulation parameters*

| Simulation metric | Values |
|---|---|
| Simulator | MATLAB R2020b |
| Type of channel | Wireless |
| Number of nodes | 300 |
| Simulation time | 150 s |
| Energy | 10 Joule |
| MAC type | 802.5.4 |

## Performance Metrics

The classifier's performance is assessed statistically utilizing the subsequent performance evaluation metrics:

### *Efficiency Rate Analysis*

The efficiency rate measures how efficiently and optimally data are transmitted within the network. It assesses the system's ability to transmit information with minimal energy consumption, low latency, and high throughput, ensuring reliable communication between wearable devices within the body area network.

The efficiency rate analysis of the TFSKG-SDA Method is displayed in Figure 3 and Table 3, among other existing models. The graph shows how the efficiency rate was maintained while efficiency was increased using the WBAN approach. The efficiency rate for 50 nodes of the TFSKG-SDA model is 91.213%, while the efficiency rates for the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models are 79.920%,

Table 3
*Efficiency rate analysis for TFSKG-SDA method*

| Number of nodes | MIMO | HCWBAN | GA-MDP | RASA-CASA | CNN-LSTM | TFSKG-SDA |
|---|---|---|---|---|---|---|
| 50 | 79.920 | 87.627 | 85.324 | 82.636 | 90.524 | 91.213 |
| 100 | 78.563 | 86.536 | 84.213 | 81.425 | 89.526 | 91.062 |
| 150 | 78.924 | 86.927 | 84.738 | 81.927 | 89.725 | 91.727 |
| 200 | 79.314 | 87.324 | 85.029 | 82.415 | 90.324 | 92.526 |
| 250 | 78.314 | 86.314 | 83.827 | 80.029 | 89.042 | 92.827 |
| 300 | 79.625 | 88.526 | 85.121 | 83.627 | 90.121 | 92.313 |

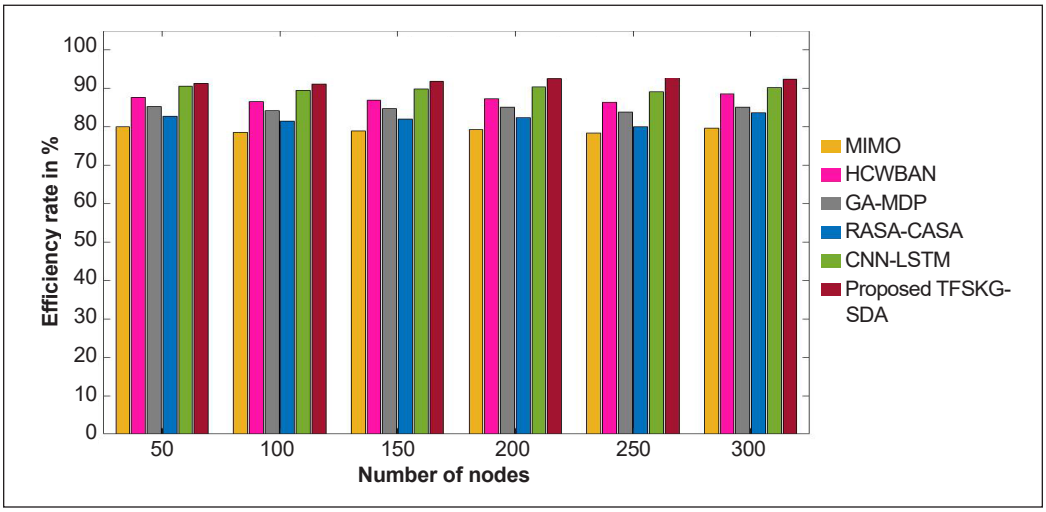


*Figure 3.* Efficiency rate analysis for TFSKG-SDA method

87.627%, 85.324%, 82.636%, and 90.524%, respectively. With different data quantities, however, the TFSKG-SDA model fared better. In comparison, the efficiency rates of the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models are 79.625%, 88.526%, 85.121%, 83.627%, and 90.121%, respectively while the TFSKG-SDA model has a 92.313% efficiency rate under 300 nodes.

### *Encryption Time Analysis*

The quantity of time needed to secure and encrypt data before it is transferred wirelessly over the network is referred to as the encryption time. This process involves applying cryptographic algorithms to transform the information into a coded format, ensuring privacy and security during communication between devices within the body area network. Encryption time is essential in maintaining the confidentiality of sensitive health-related data transmitted over the wireless network.

Figure 4 and Table 4 illustrate an encryption time comparison of the TFSKG-SDA Technique with other known models. According to the data, the TFSKG-SDA strategy

Table 4
*Encryption time analysis for TFSKG-SDA method*

| Number of nodes | MIMO | HCWBAN | GA-MDP | RASA-CASA | CNN-LSTM | TFSKG-SDA |
|---|---|---|---|---|---|---|
| 50 | 78.425 | 74.625 | 69.425 | 61.728 | 55.324 | 51.029 |
| 100 | 77.314 | 72.425 | 66.928 | 60.415 | 53.425 | 51.314 |
| 150 | 78.672 | 75.432 | 70.627 | 62.983 | 56.827 | 51.816 |
| 200 | 77.927 | 73.029 | 67.972 | 61.324 | 54.029 | 52.314 |
| 250 | 78.425 | 75.213 | 71.234 | 63.272 | 57.324 | 52.716 |
| 300 | 76.827 | 73.526 | 65.324 | 59.324 | 53.726 | 52.526 |

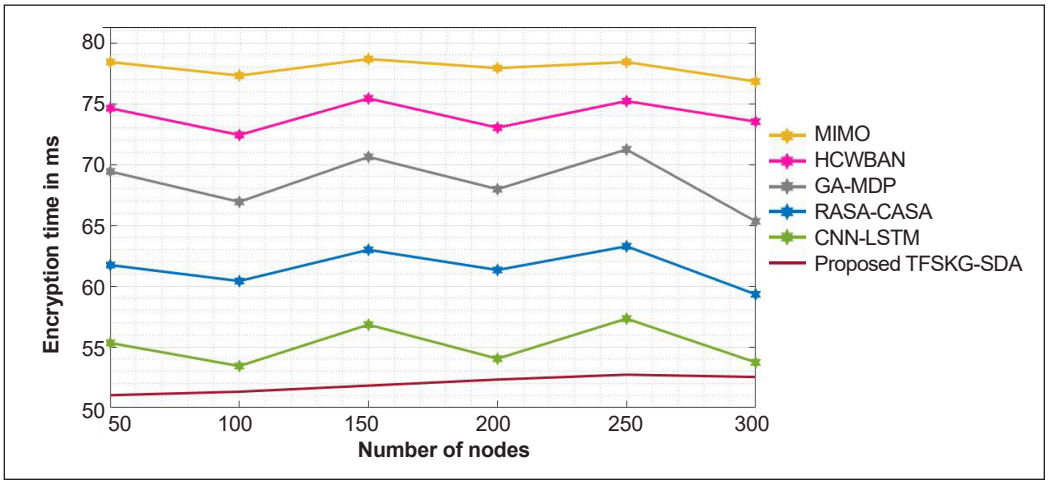


*Figure 4*. Encryption time analysis for TFSKG-SDA method

outperformed all other tactics. For example, the proposed TFSKG-SDA strategy took just 51.029 ms to encrypt 50 nodes, whereas other current approaches such as MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM took 78.425 ms, 74.625 ms, 69.425 ms, 61.728 ms, and 55.324 ms, respectively. Similarly, the proposed TFSKG-SDA strategy takes 52.526ms to encrypt 300 nodes, whereas existing techniques such as MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM take 76.827 ms, 73.526 ms, 65.324 ms, 59.324 ms, and 53.726 ms, respectively for encryption.

### *Decryption Time Analysis*

"Decryption time" is the duration necessary for the recipient of a transmission to decipher encrypted material. Efficient decryption plays a critical role in the timely and secure transmission of sensitive health information in the context of wearable and implanted medical devices, or WBANs. The decryption time influences the overall communication latency and is critical in ensuring these networks' real-time monitoring and management of health-related data.

Table 5
*Decryption time analysis for the TFSKG-SDA method*

| Number of nodes | MIMO | HCWBAN | GA-MDP | RASA-CASA | CNN-LSTM | TFSKG-SDA |
|---|---|---|---|---|---|---|
| 50 | 321.72 | 171.02 | 272.72 | 211.82 | 142.72 | 112.62 |
| 100 | 332.92 | 179.52 | 279.52 | 218.82 | 148.76 | 123.82 |
| 150 | 361.02 | 195.61 | 292.52 | 242.72 | 164.92 | 119.72 |
| 200 | 358.62 | 186.42 | 286.72 | 239.71 | 157.52 | 126.52 |
| 250 | 342.72 | 181.52 | 281.76 | 231.82 | 151.02 | 139.62 |
| 300 | 372.82 | 199.81 | 296.42 | 263.82 | 165.72 | 131.62 |

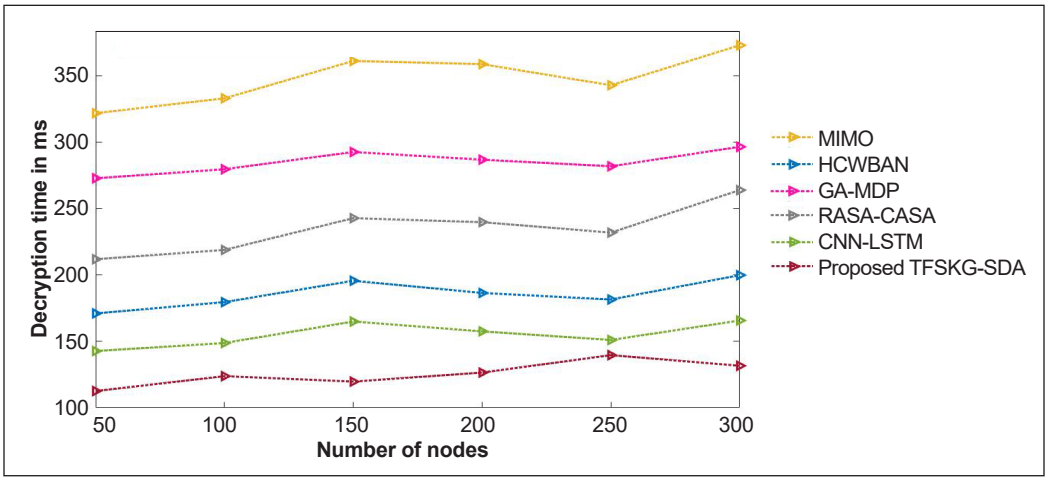


*Figure 5* Decryption time analysis for TFSKG-SDA method

The results of the decryption time analysis, comparing the TFSKG-SDA Method to several established models, are displayed in Figure 5 and Table 5. Based on the statistics, the TFSKG-SDA strategy outperformed all other tactics. The suggested TFSKG-SDA strategy, for example, required just 112.62 ms to decrypt 50 nodes, whereas MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM have taken 321.72 ms, 171.025 ms, 272.72 ms, 211.82 ms, and 142.72 ms, respectively. Similarly, the proposed TFSKG-SDA method decrypts 300 nodes in 131.62 ms, while existing approaches such as MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM require 372.82 ms, 199.816 ms, 296.42 ms, 263.82 ms, and 165.72 ms, respectively for decryption.

***Packet Delivery Ratio (PDR) Analysis***

PDR is defined as Equation 30.

$$Packet\ Delivery\ \ Ratio = \frac{data_{DS}(Total\ \ packets\ \ received\ \ by\ \sin k)}{data_{SL}(Total\ \ packets\ \ sent\ \ by\ \ LMUs)} \quad [30]$$

Without present strategies, the Local Monitoring Units (LMUs) would determine packet transmission using a routing protocol on their own. Classically, this protocol needs numerous control signals from the network to determine the best course of action for each state.

The PDR analysis of the TFSKG-SDA Method with other existing models is shown in Figure 6 and Table 6. The graph shows how the WBAN strategy improves efficiency while maintaining PDR. In comparison to the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models, which have PDR of 82.728%, 62.029%, 69.516%, 77.435%, and 66.019%, respectively, the TFSKG-SDA model has a PDR of 89.026% for 50 nodes. The TFSKG-SDA model, on the other hand, fared better with different data sizes. Under 300 nodes, the TFSKG-SDA model has a PDR of 94.726%, whereas the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models have a PDR of 88.829%, 65.324%, 75.726%, 81.028%, and 67.324%, respectively.

Table 6
*Packet delivery ratio analysis for the TFSKG-SDA method*

| Number of nodes | MIMO | HCWBAN | GA-MDP | RASA-CASA | CNN-LSTM | TFSKG-SDA |
|---|---|---|---|---|---|---|
| 50 | 82.728 | 62.029 | 69.516 | 77.435 | 66.019 | 89.026 |
| 100 | 86.826 | 65.873 | 72.928 | 79.435 | 67.728 | 90.627 |
| 150 | 84.536 | 64.782 | 71.425 | 78.536 | 66.415 | 91.425 |
| 200 | 83.928 | 63.526 | 70.616 | 77.825 | 66.314 | 92.725 |
| 250 | 87.452 | 64.324 | 73.724 | 80.627 | 68.524 | 93.672 |
| 300 | 88.829 | 65.324 | 75.726 | 81.028 | 67.324 | 94.726 |

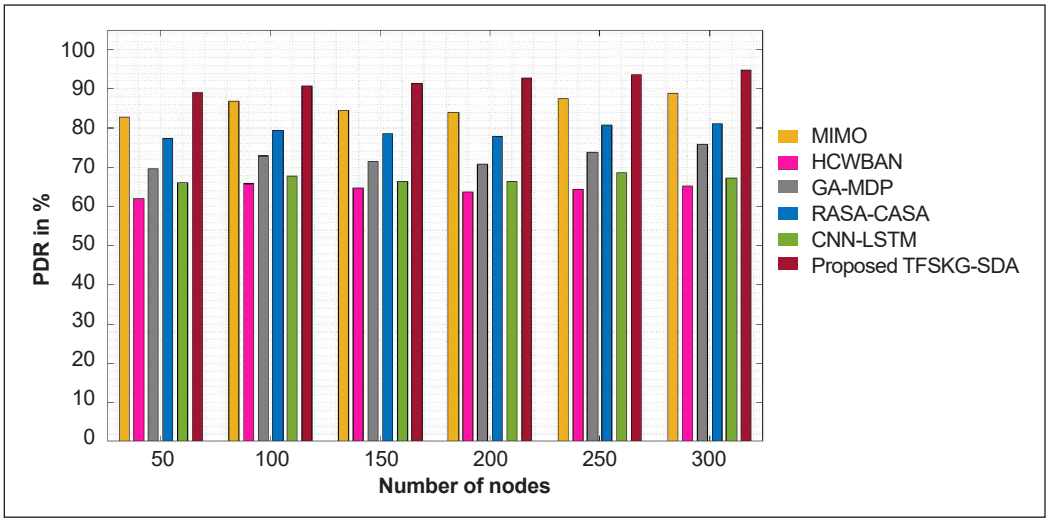


*Figure 6.* Packet delivery ratio analysis for the TFSKG-SDA method

### *Accuracy Analysis*

Accuracy (ACC): The precision was designed by dividing the total number of examples by the sum of the true positives (TP) and true negatives (TN) (Equation 31).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad [31]$$

TP denotes successfully predicted data labels corresponding to the actual data. FP, on the other hand, refers to incorrectly expected negative data labels assigned to the incorrect category of image labels. TN is an abbreviation for expected negative sample data sets. FN signifies positive data labels that were mistakenly predicted.

Figure 7 and Table 7 depict the accuracy of the study of the TFSKG-SDA Method in comparison with other existing models. The graph illustrates how the WBAN method increased efficacy without sacrificing accuracy. The TFSKG-SDA model exhibits a PDR of 92.424% for 50 nodes, surpassing the accuracy values of 75.052%, 82.728%, 89.314%,

Table 7
*Accuracy analysis for TFSKG-SDA method*

| Number of nodes | MIMO | HCWBAN | GA-MDP | RASA-CASA | CNN-LSTM | TFSKG-SDA |
|---|---|---|---|---|---|---|
| 50 | 75.052 | 82.728 | 89.314 | 87.029 | 79.324 | 92.424 |
| 100 | 77.025 | 84.324 | 90.827 | 87.526 | 81.526 | 92.827 |
| 150 | 76.324 | 83.926 | 90.423 | 88.524 | 80.728 | 93.627 |
| 200 | 78.425 | 86.625 | 90.072 | 88.927 | 82.526 | 94.536 |
| 250 | 77.526 | 85.728 | 91.252 | 87.062 | 81.829 | 94.972 |
| 300 | 76.762 | 83.526 | 89.738 | 87.425 | 79.627 | 95.536 |

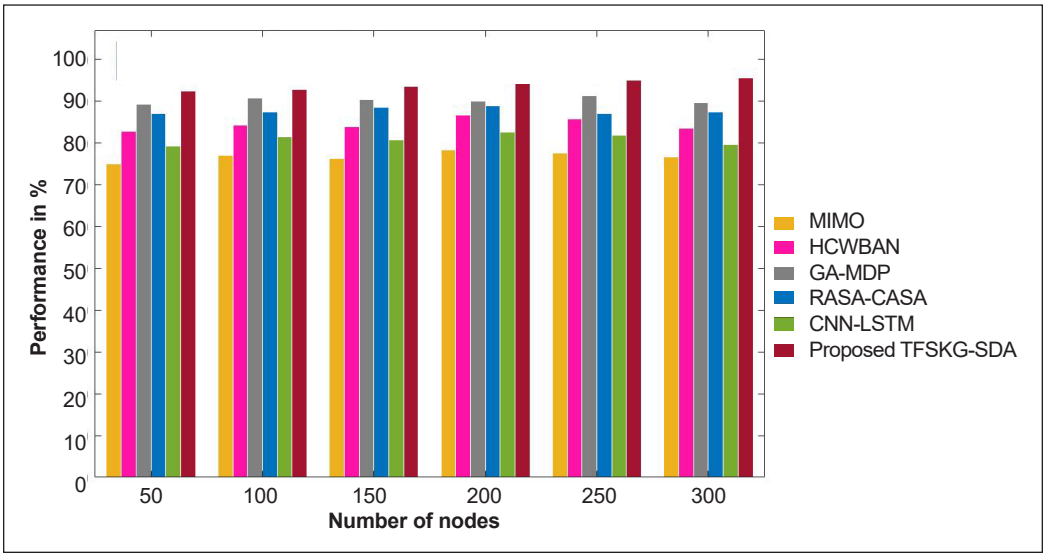


*Figure 7.* Accuracy analysis for TFSKG-SDA method

87.029%, and 79.324% for the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models. Notably, with varying data sizes, the TFSKG-SDA model outperformed its counterparts in contrast to the MIMO, HCWBAN, GA-MDP, RASA-CASA, and CNN-LSTM models, which demonstrated accuracy values of 76.762%, 83.526%, 89.738%, 87.425%, and 79.627%, respectively, the TFSKG-SDA model achieved an accuracy of 95.536% under 300 nodes.

## DISCUSSION

In WBANs, the suggested Secure Data Aggregation and Transmission System with TSFKG showed strong performance in guaranteeing data integrity and secrecy. Employment can obtain a reliable technique for aggregating private health data by efficiently decreasing possible security risks throughout the aggregation procedure. The encryption method was accomplished estimably in terms of encryption time and competence rate. The encryption algorithm professionally protected the secrecy of the cooperative data, preventing illegal access during communication. The security mechanisms are vital in preserving the integrity and privacy of sensitive medical data shared via WBANs, addressing significant apprehensions in healthcare data management and communication.

## CONCLUSION

In conclusion, TFSKG-SDA and transmission have expressive WBAN data privacy and security. The Twofish algorithm, known for its robust encryption method, assists in protecting sensitive data being moved through networks by providing an extra layer of

security against probable threats and illegal access. When considering WBANs, these improvements are even more important, as the transmission of medical data must be secure and uninterrupted for healthcare treatments to be both rapid and operative. The primary limitation is the probable computational overhead associated with the Twofish encryption procedure, which could influence real-time data transmission frequently in resource-constrained circumstances. Also, managing symmetric keys for encryption labels is problematic for key distribution and security management, mainly in large-scale network installations. Despite these limitations, the system significantly develops healthcare data security by preservative privacy and integrity, resulting in better patient care results in WBAN. As the use of WBANs becomes progressively common in healthcare and other industries, the necessity of strong security measures cannot be stressed. By providing a dependable and effective method of preserving sensitive data throughout its lifecycle, the Twofish method in research proposed an accurate explanation for the problems faced by security threats in WBANs. As a result, an innovative genetic algorithm for data security is proposed for increased performance in this work. Our proposed framework, the TFSKG-SDA method, performs an outstanding accuracy of 95.536%. Future WBAN communication dependability assessments should be made using extra performance metrics. Implementation will also be recommended to prioritize network performance and energy efficiency. Finally, radio propagation models with computed path loss coefficients in wireless band situations will be discussed.

## ACKNOWLEDGEMENTS

The authors thank VelTech Multi Tech Dr. Rangarajan Dr. Sakunthalal Engineering College, Tamil Nadu, India, for providing facilities and testing for this research. The authors would also like thank all the reviewers for their helpful comments and suggestions during the research's execution. The authors greatly appreciate their generosity with their time.

## REFERENCES

Abualsaud, K., Mohamed, A., Khattab, T., Yaacoub, E., Hasna, M., & Guizani, M. (2018). Classification for imperfect EEG epileptic seizure in IoT applications: A comparative study. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 364-369). IEEE Publishing. https://doi.org/10.1109/IWCMC.2018.8450279

Anh, B. T., Quoc, D. D., & Hiep, P. T. (2023). Optimizing transmission power for uplink data in cell-free wireless body area networks. In *2023 IEEE Statistical Signal Processing Workshop (SSP)* (pp. 275-279). IEEE Publishing. https://doi.org/10.1109/SSP53291.2023.10208084

Apoorva, Y. K. (2013). Comparative study of different symmetric key cryptography algorithms. *International Journal of Application or Innovation in Engineering & Management*, *2*(7), 10-15. https://doi.org/10.4236/jis.2020.113009

Azees, M., Vijayakumar, P., Karuppiah, M., & Nayyar, A. (2021). An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. *Wireless Network, 27*(3), 2119–2130. https://doi.org/10.1007/s11276-021- 02560-y

Dangi, K. G., Bhagat, A., & Panda, S. P. (2020). Emergency vital data packet transmission in hospital centered wireless body area network. *Procedia Computer Science*, *171*, 2563-2571. https://doi.org/10.1016/j.procs.2020.04.278

Geetha, B. T., Mohan, P., Mayuri, A. V. R., Jackulin, T., Aldo Stalin, J. L., & Anitha, V. (2022). Pigeon inspired optimization with encryption based secure medical image management system. *Computational Intelligence and Neuroscience, 2022*(1), Article 2243827. https://doi.org/10.1155/2022/2243827

He, D., Zeadally, S., Kumar, M., & Lee, J. H. (2017). Anonymous authentication for wireless body area networks with provable security, *IEEE Systems Journal, 11*(4), 2590-2601. https://doi.org/10.1109/JSYST.2016.2544805

Hu, C., Li, H., Huo, Y., Xiang, T., & Liao, X. (2016). Secure and efficient data communication protocol for wireless body area networks. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(2), 94-107. https://doi.org/10.1109/TMSCS.2016.2525997

Kaleem, M., & Devarajan, G. G. (2023). Wireless body area networks utilizing data transmission techniques based on prediction. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1586-1591). IEEE Publishing.

Kareem, S. M., & Rahma, A. M. S. (2020). A novel approach for the development of the Twofish algorithm based on multi-level key space. *Journal of Information Security and Applications*, *50*, Article 102410. https://doi.org/10.1016/j.jisa.2019.102410

Khan, S., Iqbal, W., Waheed, A., Mehmood, G., Khan, S., Zareei, M., & Biswal, R. R. (2022). An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society. *Sensors, 22*(1), Article 336. https://doi.org/10.3390/s22010336

Kumar, M., & Chand, S. (2020). A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. *IEEE Internet of Things Journal, 7*(10), 10650-10659. https://doi.org/10.1109/JIOT.2020.3006523

Kumar, M., & Chand, S. (2021). A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. *In IEEE Systems Journal, 15*(2), 2779-2786. https://doi.org/10.1109/JSYST.2020.2990749

Kumar, M., (2020). Cryptanalysis and improvement of anonymous authentication for wireless body area networks with provable security. *Cryptology ePrint Archive*. https://eprint.iacr.org/2020/936

Lee, C., & Lee, J. (2017). Harvesting and energy aware adaptive sampling algorithm for guaranteeing self-sustainability in wireless sensor networks. In *2017 International Conference on Information Networking (ICOIN)* (pp. 57-62). IEEE Publishing. https://doi.org/10.1109/ICOIN.2017.7899475

Liu, Q., Mkongwa, K. G., & Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. *SN Applied Sciences, 3*(2), Article 155. https://doi.org/10.1007/s42452-020-04058-2

Mathews, R., & Jose, D. V. (2024). Hybrid homomorphic-asymmetric lightweight cryptosystem for securing smart devices: A review. *Transactions on Emerging Telecommunications Technologies, 35*(1), Article e4866. https://doi.org/10.1002/ett.4866.

Mehmood, G., Khan, M. Z., Fayaz, M., Faisal, M., Rahman, H. U., & Gwak, J. (2022). An energy-efficient mobile agent-based data aggregation scheme for wireless body area networks. *Computers, Materials & Continua, 70*(3), 5929-5948. https://doi.org/10.32604/cmc.2022.020546

Mehmood, G., Khan, M. Z., Waheed, A., Zareei, M., & Mohamed, E. M. (2020). A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. *IEEE Access, 8*, 131397-131413. https://doi.org/10.1109/ACCESS.2020.3007405

Mohapatra, D., Kumar, S., Bhoi., Jena, K. K., Nayak, S. N., Singh, A., (2022). A blockchain security scheme to support fog-based internet of things. *Microprocessors and Microsystems, 89*, Article 104455. https://doi.org/10.1016/j.micpro.2022.104455

Paulraj, D., & Baburaj, E. (2023). Admission control policy and key agreement based on anonymous identity in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 12*(1), 1-18. https://doi.org/10.1186/s13677-023-00446-2

Rane, D. D. (2016). Superiority of twofish over blowfish. *International Journal of scientific research and management*, *4*(11), 4744-4746. https://doi.org/10.18535/ijsrm/v4i11.01

Roy, M., Chowdhury, C., & Aslam, N. (2021). Designing GA based effective transmission strategies for intra-wban communication. *Biomedical Signal Processing and Control, 70*, Article 102944. https://doi.org/10.1016/j.bspc.2021.102944

Salem, O., Alsubhi, K., Mehaoua, A., & Boutaba, R. (2020). Markov models for anomaly detection in wireless body area networks for secure health monitoring. *IEEE Journal on Selected Areas in Communications*, *39*(2), 526-540. https://doi.org/10.1109/JSAC.2020.3020602.

Santos, M. A., Munoz, R., Olivares, R., Rebouças Filho, P. P., Del Ser, J., & de Albuquerque, V. H. C. (2020). Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook. *Information Fusion*, *53*, 222-239. https://doi.org/10.1016/j.inffus.2019.06.004

Shyja, V., Irine., Ranganathan, G., & Bindhu., V. (2023). Link quality and energy efficient optimal simplified cluster-based routing scheme to enhance lifetime for wireless body area networks. *Nano Communication Networks, 37*, Article 100465. https://doi.org/10.1016/j.nancom.2023.100465.

Subramani, J., Azees, M., Rajasekaran, A. S., & Al-Turjman, F. (2023). EPF-FDA: Efficient pairing free and confidentiality preserving fog-based data aggregation scheme for WBANs. *IEEE Instrumentation & Measurement Magazine, 26*(8), 10-16. https://doi.org/10.1109/MIM.2023.10292620

Subramani, J., Maria, A., Rajasekaran, A.S., and Al-Turjman. F. (2022). Lightweight privacy and confidentiality preserving anonymous authentication scheme for WBANs. *IEEE Transactions on Industrial Informatics, 18*(5), 484-3491. https://doi.org/10.1109/TII.2021.3097759

Thippun, P., Sasiwat, Y., Buranapanichkit, D., Booranawong, A., Jindapetch, N., & Saito, H. (2023). Implementation and experimental evaluation of dynamic capabilities in wireless body area networks: Different setting parameters and environments. *Journal of Engineering and Applied Science*, *70*(1), Article 1. https://doi.org/10.1186/s44147-022-00171-8

Tseng, T. W., Wu, C. T., & Lai, F. (2019). Threat analysis for wearable health devices and environment monitoring internet of things integration system. *IEEE Access*, *7*, 144983-144994. https://doi.org/10.1109/ACCESS.2019.2946081

Wang, C., Qin, Y., Jin, H., Kim, I., Vergara, J. D. G., Dong, C., Jiang, Y., Zhou, Q., Li, J., He, Z., Zou, Z., Zheng, L. R., Wu, X., & Wang, Y. (2019). A low power cardiovascular healthcare system with cross-layer optimization from sensing patch to cloud platform. *IEEE Transactions on Biomedical Circuits and Systems*, *13*(2), 314-329. https://doi.org/10.1109/TBCAS.2019.2892334

Wang, L., Zhang, G., Li, J., & Lin, G. (2020). Joint optimization of power control and time slot allocation for wireless body area networks via deep reinforcement learning. *Wireless Networks*, *26*, 4507-4516. https://doi.org/10.1007/s11276-020-02353-9

Zhang, J., & Dong, C. (2022). Secure and lightweight data aggregation scheme for anonymous multi-receivers in WBAN. *IEEE Transactions on Network Science and Engineering*, *10*(1), 81-91. https://doi.org/10.1109/TNSE.2022.3205044

Zhong, L., He, S., Lin, J., Wu, J., Li, X., Pang, Y., & Li, Z. (2022). Technological requirements and challenges in wireless body area networks for health monitoring: A comprehensive survey. *Sensors*, *22*(9), Article 3539. https://doi.org/10.3390/s22093539