An Energy Efficiency Based Secure Data Transmission in WBSN Using Novel Id-Based Group Signature Model and SECC Technique

C. Ramesh Kumar[1], T. Ganesh Kumar[1], A. Hemlathadhevi[2], D. R. Thirupurasundari[3]*

[1] School of Computing science and Engineering, Galgotias University, India
[2] Department of Computer Science & Engineering, Panimalar Engineering College, India
[3] Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, India
c.ramesh@galgotiasuniversity.edu.in, t.ganesh@galgotiasuniversity.edu.in, hemlathadhevi@gmail.com, tpsdrlagok@gmail.com

Abstract

A wireless network composed of wearable sensing along with computing systems connected via a wireless communication channel is termed Wireless Body Sensor Network (WBSN). It enables continuous monitoring through sensors for medical and nonmedical applications. WBSN faces several security problems such as loss of information, access control, and authentication. As WBSN collects vital information and operates in an unfriendly environment, severe security mechanisms are needed in order to prevent the network from anonymous interactions. The different security threats are evaluated with the support of the data transmitted via the sensor networks amongst smart wearable devices. The whole network lifetime together with the Data Transmission (DT) quality is mitigated whilst performing DT utilizing sensor networks, which consume more energy. Hence, in this paper, an energy-efficient secure data transmission mechanism is proposed in WBSN using a novel authentication id-based group signature model and SECC technique. At first, the Group Manager (GM) is selected from the sensors in the remote body sensor system using Normalized Opposition Based Learning BAT Optimization Algorithm (NOBL-BOA). Afterward, clustering with Information Entropy induced K-Means Algorithm (IEKMA) takes place to improve energy efficiency. Next, to provide security to the WBSN, message authentication is carried out based on novel authentication ID-based group signature protocol. Finally, Secret key induced Elliptic Curve Cryptography (SECC) is used to encrypt the message for secure transmission. The simulation results reveal that in comparison with existing works, the proposed work achieves improved security and energy efficiency.

Keywords: Wireless Body Sensor Network (WBSN), Authentication, BAT Optimization Algorithm (BOA), ID-based group signature model

1 Introduction

In Health-Care Monitoring (HCM) applications, the Wireless Sensor Network (WSN) gives an important benefit for the subsequent evaluation [1]. The development of a specialized biological network named Body Sensor Networks (BSNs) or Body Area Networks (BANs) are been provoked by the major advancements in WSN algorithms along with applications [2]. WSBN is a kind of WSN, which is particularly associated with healthcare applications [3]. In HCM, for checking the useful parameters exactly, the Sensor Nodes (SN) are located above the human bodies' surface or implanted into the human body tissues [4]. Sensing a patient's significant signs, processing, along with communicating data are the three important tasks presented by the sensors in WBANs [5]. The human body's essential physiological parameters like blood pressure, ECG, and pulse are gathered by SN [6]. Through Body Sensor Units (BSUs), these biosensors collect physical data and for further assessment, the biosensor transmits the physical data to its final destination (personal display assistant, gateway, Base Station (BS)) [7]. Since the WBAN collects the profits of continuous progress, it can save human lives by employing it not just in medicine but also in military applications and sports activities [8-9]. Security together with privacy in WBANs based HCM services has constantly been a critical problem, even though WBANs enhance the value of health care services [10].

As a consequence of the sensitivity of data, trusted information has huge significance for healthcare providers in Remote Patient Monitoring (RPM) [11] as shown in the Figure 1. The output attained by WBANs should be accurate, reliable, trustworthy, and authenticated as it deals with various critical health-related parameters which may impact a patient's health and life [12-13]. Any kind of data leakage or alteration may put the patient's life in danger because those sensitive patient data are the base of clinical diagnosis [14]. Currently, WBANs are not just utilized in HM; it is also utilized in military activities, sports training, entertainment, etc. [15].

The data integrity, freshness, and secrecy can be simply affected by security problems including outsider attacks like eavesdropping, malicious attack, and insider attacks by compromising SN [16]. The primary concern for the acceptance of health systems in conjunction with their implementation is security along with the privacy of transferring medical data from WBAN to the gateway or

*Corresponding Author: C. Ramesh Kumar; E-mail: c.ramesh@galgotiasuniversity.edu.in
DOI: 10.53106/160792642023052403014

towards a remote server [17]. As there are still security concerns about the WBANs, the WBANs technology will not be espoused [18].

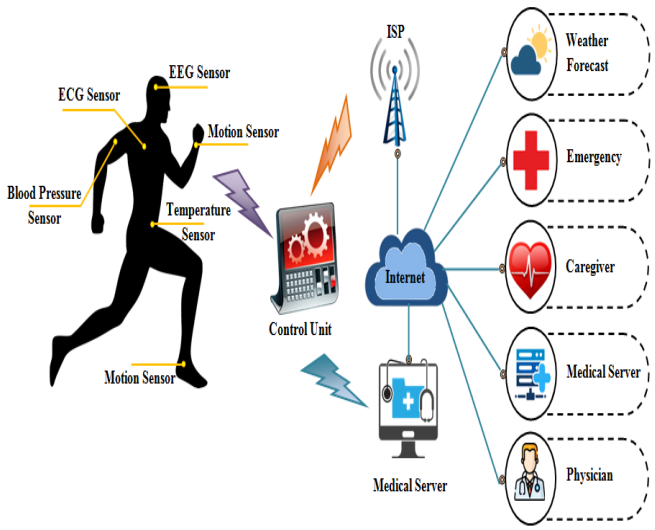

Figure 1. General architecture of WBSN

Hence, it is essential to create a stronger outcome with the given resource constraints and for the challenges of security along with privacy in WBAN. Here, by utilizing a new authentication IDGS model and SECC technique, an energy-efficient secure DT approach is proposed in WBSN.

The balance section is arranged as follows; the related works are surveyed in section 2; the details along with basic concepts of the proposed methodology is explicated in section 3; the competence of the proposed work analogized to a few of the conventional methods are determined in section 4; the conclusion is provided in section 5.

2 Literature Survey

Kakali Chatterjee [19] introduced a strong mutual authentication protocol centered on public-key cryptography for fulfilling every security needs. To the gateway node, every data gathered by every SN were dispatched. Via the network coordinator that was known as User Device, the data was mailed to the local processing center (Base Station (BS)) by the gateway node. In the health cloud, every captured data was collected via that device. Pallier cryptosystem was employed by the scheme mainly for safeguarding the sensor data's privacy. The experimental outcomes revealed that with low computational load together with communicational load, the scheme opposed the major vulnerable attacks in wireless BSNs. The major disadvantage of this methodology was the Pallier cryptosystem utilized large keys to obtain security, and it was extremely slow.

Subramani Jegadeesan et al. [20] introduced an Efficient Privacy-Preserving Anonymous Mutual Authentication method for Wireless BANs (EPAW). System initialization, registration, and EPAW anonymous mutual authentication were the three phases of this approach. The works were dissimilar in two phases. Primarily the users were authenticated anonymously; also, conserved the real identities of the user from other users. Secondarily, by disclosing the real identities of misbehaving doctors, conditional privacy was given by the tracking device. The experimental simulation outcomes ensured that regarding data security along with privacy, the prevailing systems were outperformed by the anonymous authentication technique with lesser computational overhead. Anyhow, it has a disadvantage that for a few type of attacks like reverse configuration attacks, it may be vulnerable.

Tallat Jabeen et al. [21] introduced a data protection generic-based encryption approach for advanced performance. While MQTT was a public-subscribe messaging protocol, in BANs nano-sensors were involved that produced patient data along with transmitted it towards Message Queuing Telemetry Transfer (MQTT) broker. Internet cloud was linked to the medical server; the encrypted data as of the MQTT broker was forwarded towards it. The medical server, which was utilized to store along with retain health critical data, should be safeguarded completely. Owing to the built-in feature of authenticity, the MQTT protocol was extremely secure along with lightweight than the LEACH protocol. Conversely, 8 bits of plain text were taken as input by the genetic algorithm; it was then, converted into a binary number. Hence, the loss of important data might happen if large bits of plain text were there.

Hyunho Ryu and Hyunsung Kim [22] executed a privacy-preserving authentication protocol in healthcare services for WBANs. A one-way function and an exclusive or-operation, which was lightweight, are the factors on which the protocol relied. There were four phases for the protocol; firstly, for all the networks, the initialization phase placed up a security building. The targets for the registration phase were the patients who possessed SN along with access points. The basic security service to verify whether the entity was legal or not, in addition, to set a session key for further secure communications was provided in the authentication phase. When PT wanted to modify SN's identity for privacy reasons, the identity modification phase was utilized. Moreover, the comparison outcome indicated that when analogized with the other protocols, this protocol attained more privacy along with security features. Conversely, upon repeated usage, the one-way hash function may weaken the system's security.

Mengxia Shuai et al. [23] introduced an effective privacy-preserving authentication scheme by utilizing ECC for WBANs. The certificate-less authentication grounded on identity-based cryptography that made it apt for multi-server architecture without third-party participation was espoused in this approach. With '5' related authentication methodologies, security analysis along with comparisons demonstrated that not only the preferred security features but also the diminution of computation cost were offered by the privacy-preserving authentication method. However, it didn't consider the patient side operational together with communicational overhead.

Mahender Kumar and Satish Chand [24] introduced an Identity-Based Anonymous Authentication and Key Agreement (IBAAKA) in the cloud-assisted environment for WBAN. Setups, registration, and authentication were the three algorithms contained in the IBAAKA protocol. It guaranteed that in the registration phase, a user's identity

remains to hide except the network manager. The security evaluation displayed that the assumption developed IBAAKA protocol was protected also had the ability to attain necessary security properties under the random oracle model (ROM) together with computational Diffie-Hellman (CDH). The outcome comparison revealed that when correlated with the existent methods, this method had the least computation and comparable cost. But, in the BSN environment, the encryption operation was extremely expensive and not really considered a choice for providing message confidentiality.

Bhawna Narwal and Amar Kumar Mohapatra [25] presented a Secure and Anonymous Mutual Authentication scheme for WBANs (SAMAKA). Particularly, the entire security features required were conserved by the SAMAKA; in addition, it also prevents several security attacks as of an adversary. A secure along with anonymity-preserving authentication methodology was developed, which authenticated the Chief Node (CN) along with SN via Mid Node (MN); in addition, it approved on a session key securely by employing simple hash together with XOR operations. AVISPA tool, BAN Logic, together with RoR Model was utilized to validate the security of SAMAKA as of different adversarial attacks, to achieve authentication, along with to guarantee safe session key agreement. Furthermore, to spotlight the essential security features attained along with adversarial attacks prevented by the SAMAKA, an informal security evaluation was done. Lastly, a comparative performance evaluation exposed that superior performance along with promising outcomes was attained by the SAMAKA. Yet, the espousal of a security system was made extremely complex and challenging owing to the limited memory resources, battery power, and processing capabilities of the body SNs.

Bhawna Narwal and Amar Kumar Mohapatra [26] produced a Secured Energy-Efficient Mutual Authentication and Key Agreement methodology (SEEMAKA) for two-tier WBAN. Utilizing some hash invocations along with bitwise XOR operations, SEEMAKA attained desirable security properties along with prevented various security attacks; thus, satisfying the requirement for limited capable SN. Via sound informal analysis and utilizing automated validation of internet security protocols along with applications, the safety of SEEMAKA was assessed. BAN Logic was utilized for verifying the exactness of SEEMAKA. Betwixt SEEMAKA and other recent authentication schemes, a set of thorough relative analyses was conducted and the outcome marked that SEEMAKA attained superior efficiency concerning processing overhead, energy dissipation, along with security features. Alternatively, in this methodology, optimization of route selection along with the energy conservation goal was not précised.

M. Ayyadurai et. al [27] introduced Data Encryption and Signature-based Authentication protocol (DESA) approach for WBSNs to provide reciprocated authentication regarding signature verification ID. To provide protected communication with lower overheads, this model was constructed to make certain the sensed data's privacy within the WBSN entities. The encrypted message text labelled with the set of attributes was sent by the sender and to indicate node authentication, the signature ID was assigned properly. At the receiver end, the authorized signature ID was verified and the data was encrypted. Hence, when analogized with the existent techniques, higher security would be offered by the introduced DESSA method, which could bear various security attacks. The experiential outcomes displayed that an advanced performance was achieved by the scheme than the baseline techniques. Conversely, here, energy efficiency was not considered that in turn increased the Computation Time (CT) necessary for DT.

3 Proposed Methodology

Sensors, smart devices, and displays, which work flawlessly on the body, are produced by the enhancements in wearable devices over the past decennium. The WBSN is produced by inspiring the improvements in wireless lower-power sensors along with the rising demand for a moveable HCM system. SNs fitted in, on, or around the human body monitor the physiological signals; a collection of such SNs is mentioned as WBSN. Electrocardiogram (ECG), Blood Pressure (BP), Electromyogram (EMG), Pulse Oxygen Saturation (SpO2), et cetera are the various sensors along with sensor devices, which are amassed initially; then, to process, the data is transmitted to a sink node. In WBSN, one of the primary concerns is security along with privacy even though it provides numerous advantages in facilitating people's lives. Lesser security and authentication system was provided by wearable WBSN devices owing to the accessibility of constrained bandwidth resources along with computing capacities. In the advancement and employment of WBSNs, the foremost obstacle was the energy supply for SNs. Consequently, a novel authentication IDGS along with SECC methodologies were proposed here to conquer the aforementioned complications; thus, enhancing the WBSN's security together with EE. Figure 2 displays the proposed framework's structural design.

The work flow of the proposed secure DT in the WBSN system is explicated in Figure 2. Firstly, details of patients, who utilize the wireless sensors, were registered with the respective hospital; then, a unique registration number is offered to every patient. Next, by exploiting the NOBL-BOA optimization model, a GM is chosen from a group of SNs. After that, by employing the IEKMA clustering methodology, which enhances the system's EE, the GMs are clustered.

Then, with the aid of the IDGS protocol, message authentication is performed betwixt the GM and the BS. This validates whether the body sensor data is coming from an authorized node or not. To prevent attacks, the data is encrypted by employing the SECC encryption methodology after successful authentication. Lastly, to the doctor along with emergency services, the encrypted data is forwarded after being decrypted. Also, it was amassed in the data server.

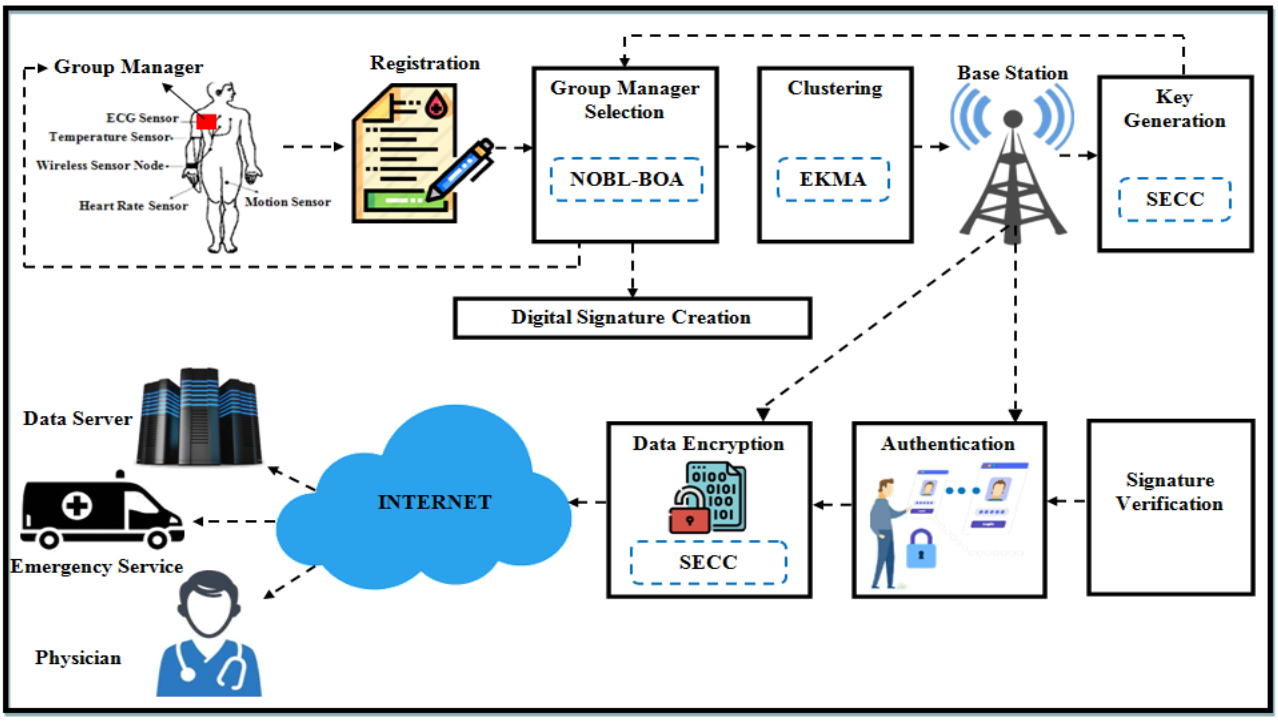

Figure 2. Structural design of the proposed system

3.1 Registration Phase

In this, firstly, patients using wireless sensors register their details with the respective hospital; after registration, they are provided with a unique registration number, which should be preserved confidential. To sense data like BP, temperature, heart rate, et cetera, various numbers of sensors are attached to the patient's body. Under the registration number, different IDs are included by these sensors. These sensors form a group and a group manager for this group is selected for efficient transmission of data. The number of sensors implanted on the patient body (s^i) is represented as,

$$s^i = s^1, s^2, \ldots\ldots, s^n. \tag{1}$$

In equation (1), n determines the number of sensor nodes placed on the human body.

3.2 GM Selection with NOBL-BOA

The Group Manager (GM) for a group of sensor nodes is selected based on the NOBL-BOA optimization technique. BAT-Optimization Algorithm (BOA) is a population-based optimization model inspired by the biological characteristics of food searching and predation behavior of bats. This algorithm consists of four main parameters, frequency, emission, constants, and emission rate. To detect the variation betwixt food and prey, echolocation is utilized by a BAT. A random uniform distribution methodology is utilized here to compute the maximum together with the minimum frequency range of BAT in updating its position. Likewise, regarding random walks, the BAT's local search is executed. A local optimum solution and a reduction in convergence rate may occur with such random distribution along with random walks. To gauge the bats' frequency range, the Min-Max normalization model is utilized; thus, conquering the aforementioned limitations. For the local search process, Opposition Based Learning (OBL) is employed. Besides, to enhance diversity together with to upgrade the produced solution, the OBL is utilized. These advancements in the traditional BOA are termed NOBL-BOA. The NOBL-BOA's optimization steps are explicated below.

Step 1: Let $s^i = s^1, s^2, \ldots, s^n$. (number of SNs) be the bat's initial population. Every single bat i comprises a definite position x^i with velocity v^i, along with frequency f^i. Every single BAT is assigned a uniform frequency betwixt $(f^{\min}, f^{\max})$ during optimization. When searching for prey, the bat's frequency is symbolized as,

$$f^i = f^{\min} + \varepsilon(f^{\max} - f^{\min}). \tag{2}$$

Where, the maximum and minimum frequency range is specified as $f^{\max}, f^{\min}$ and the normalized frequency range calculated by employing min-max normalization is signified as ε,

$$\varepsilon = \frac{f^i - f^{\min}}{f^{\max} - f^{\min}}. \tag{3}$$

Step 2: The velocity of the bat searching for prey at a time (t) is formulated as,

$$v_t^i = v_{t-1}^i + f^i(x_{t-1}^i - x''). \tag{4}$$

Here, the bat's flight speed at time ($t-1$) is defined as v_{t-1}^{i}, the bat's position at time ($t-1$) is proffered as x_{t-1}^{i} and the current best bat position is elucidated as x''.

Step 3: The Bats' position is expressed as,

$$x_t^i = x_{t-1}^i + v_t^i. \tag{5}$$

Step 4: Both the global and local search capacities, which are reliant on their parameters, are comprised in the BOA. Consequently, by choosing adaptive parameters, the balance betwixt the local and global search is obtained. The OBL is utilized to determine the local search strategy. It is measured as,

$$\hat{x} = f^{\min} + f^{\max} - x^{old} + \delta L_t^i. \tag{6}$$

Here, $f^{\min} = 0$ and $f^{\min} = 1$, the random number uniformly drawn in the range (0, 1) is exhibited as δ, the old position is specified as x^{old} and the average loudness of all bats at time (t) is notated as L_t^i. The criterion for bat moving towards the prey (X) is,

$$X = \begin{cases} p & \delta < L_t^i \\ \hat{x} & else \end{cases}. \tag{7}$$

Where, the bat's movement towards the prey (optimal solution) is specified as p. After that, the new solution is acquired; subsequently, to manage the exploration along with exploitation, the loudness and emission rates are updated.

Step 5: The loudness as well as emission rate are updated as,

$$L_{t+1}^i = \eta L_t^i. \tag{8}$$

$$e_{t+1}^i = e_0^i + \left\langle 1 - e^{-\psi t} \right\rangle. \tag{9}$$

Where, the constants are denoted as η and ψ in which $\eta, \psi > 0$, the emission rate at the time $t+1$ is specified as e_{t+1}^i and the emission rate's initial value is signified as e_0^i. At last, the global optimal solution (GM) attained is notated as S^k, the $k-th$ SN as of the set of SNs s^i is represented as k. Figure 2 exhibits the NOBL-BOA's pseudo-code.

3.3 Clustering by Means of IEKMA

Following the selection of GM, by computing the distance betwixt the BS and GM, they are clustered, which is executed by utilizing the IEKMA algorithm. Generally, the data is partitioned into a number of clusters via a K-Means Algorithm (KMA), which is a distance-centered clustering algorithm. Next, from the range of existing BSs, cluster centers are chosen randomly; then, the distance is gauged. The data is mapped into the least distance measure regarding the distance. Nevertheless, KMA relies on the initial cluster center estimation where the initial cluster centroids are selected randomly, which is pondered as the drawback of this methodology. The local optimum solution is brought about by this random selection. Therefore, to choose the cluster centers, Information Entropy (IE) is utilized here as shown in the Figure 3. The clustering accuracy is augmented by this initialization. The espousal of IE in the baseline KMA is renamed as IEKMA. Following are the steps involved in this phase.

Step 1: Let (G^j, G^1, G^2, ..., G^m) be the set of GMs where, the number of GMs in the hospital is denoted as m and ($B^k = B^1, B^2, B^N$) be the N number of available BSs (cluster centroids). Firstly, the number of clusters is gauged by the IEKMA.

Step 2: After that, by employing the IE equation, the cluster centroids are analyzed to measure the distance betwixt the GM and Cluster centroids. Regarding the relative frequencies, the probabilities are calculated in the IE. It is expressed as,

$$\tau = -\sum_{k \in N} p(B^k) \log_2 p(B^k). \tag{10}$$

Here, the IE is depicted as τ and the probability value is notated as $p(\circ)$. $(B^{\hat{k}})$ denotes the optimized centroid being computed.

Step 3: Next, to measure the distance betwixt GM and optimized cluster centroids, the Euclidean distance (d) is utilized. The Euclidean distance is determined as,

$$d(G^j, B^{\hat{k}}) = \left\langle \sum_{j=1}^{m} (B^k - G^j)^2 \right\rangle^{1/2}. \tag{11}$$

Step 4: To remit the data efficiently devoid of any loss, the GM is allocated to the closest BS (cluster centroids) with regards to the distance; also, it enhances the WBSN's lifetime. It is formulated as,

$$G^j = \begin{cases} 1 & \min\left\{ d(G^j, B^{\hat{k}}) \right\} \\ 0 & otherwise \end{cases}. \tag{12}$$

Where, the allocation of the GM to the specific BS is mentioned as 1, and 0 indicates that the GM is not allocated to that BS and is utilized for further process.

Step 5: The process is continued by re-computing the cluster centroids; gauging the distance betwixt GM and cluster centroids; allocating the GM to the minimum distance BS (cluster centroid). The process is continued until the cluster centers are not altered. Thus, the GMs are assigned to the closest BS in such a manner.

Pseudocode for NOBL-BOA

Input: Number of sensor nodes s^i

Output: General Manager S^k

Begin
Generate the initial bat population s^i
Characterize frequency f^i, velocity v^i at x^i
Initialize loudness L^i and emission rate e^i
While $t <$ max
  For each bat s^i **do**
    Fine-tune frequency f^i
    Keep posted $v_t^i = v_{t-1}^i + f^i\left(x_{t-1}^i - x''\right)$
    Update Bats' position x^i
    If $\varepsilon > e^i$
      Pick the best solution
      Compute local search using OBL
    End if
    If $\delta < L_t^i$
      Recognize the optimal solution
      Renew loudness using $L_{t+1}^i = \eta L_t^i$
      Revise emission rate e_{t+1}^i
    End if
  End for
  Rank the solution and obtain S^k
End while
End

Figure 3. Pseudo-code for NOBL-BOA

3.4 Authentication using ID-based Group Signature Model

Here, by employing the IDGS model, the message authentication betwixt the GM and the BS is performed. In this, the users' public key is permitted to be uniquely derived as of their identity by the ID-centric methodology; then, a group signature model permits its group member to sign a message on behalf of the group. To create a secret key for the GM regarding the group ID, a Trusted Authority (TA) is comprised in the IDGS methodology (here, BS is the TA). The secret key created is transmitted to the GM by the TA following the generation of the secret key. Afterwards, by deploying the generated keys, the GM executes a signature calculation on the message transmitted by one of its member nodes to sign a message; then, the message is forwarded to the BS. The signature verification is conducted by the BS. The BS accepts the message after successful verification; then, the message is encrypted for secure DT. In this, the SECC algorithm is deployed to generate the GM's public along with the private key. The IDGS's working process is explicated below.

Step 1: Initially, every single SN is registered to the BS and they are assigned a unique ID indicated as (x^h) where, h = 1, 2, ..., n and γ signify the GM's ID.

Step 2: Firstly, the TA creates its own public key, secret key and public system parameters. Subsequently, TA selects '2' prime numbers $A1$ and $A2$ where, $\frac{A1-1}{2}$ and $\frac{A2-1}{2}$ are smooth, odd, and co-prime. Consider, $B = A1 \cdot A2$ and choose '2' integers b, c such that,

$$bd \equiv 1 * \left|\varphi(B)\right|. \tag{13}$$

$$ce \equiv 1 * \left|\varphi(B)\right|. \tag{14}$$

Where, the secret key is mentioned as c, the public key is denoted as b and the public system parameters are pondered as d, e.

Step 3: After that, by utilizing the SECC model, the GM's secret along with the public key is calculated. The Elliptic Curve (EC) equation is notated as,

$$y^2 = x^3 + ax + b(\text{mod } p). \tag{15}$$

The public along with private keys are created after mapping the integers into the curve point. The TA's secret key c along with the GM's ID γ is utilized to produce the DM's private key (g^m).

$$g^m = c * \gamma * \left|\varphi(B)\right|. \tag{16}$$

Subsequently, the GM's public key (P^{gm}) is gauged as,

$$P^{gm} = g^m \cdot G. \tag{17}$$

Where, the generator point of the EC is notated as G.

Step 4: The TA sends P^{gm}, g^m, d, e to the GM after creating the keys. Similarly, by employing the TA's secret key along with the ID of every single biosensor, the keys for every single biosensor are generated by the TA.

Step 5: The TA computes the secret key (s^k) when a new member joins the group. It is computed as,

$$s^k = (ID^{new}) p^{gm} * \text{mod}(B) + x^h. \tag{18}$$

Where, the new member's ID is mentioned as D^{new}. Similarly, the public key parameter (k^p) is assessed by the GM as,

$$k^p = ID^{new} * \text{mod}(n). \tag{19}$$

(s^k, k^p) is the user membership certificate. Next, the keys are securely transmitted to every single biosensor by the GM. Hence, secret keys (s^k) and member certificate parameters (k^p) are possessed by the biosensor.

Step 6: By employing γ (GM ID), g^m (secret key of GM), together with d, e (public system parameters), group signature computation is performed by the GM on the message transmitted by one of its member nodes to sign a message M. The group signature is determined as,

$$Z = M^{g^m} * (P^{gk})^{d+2e-1+1} \text{mod}(B). \tag{20}$$

$$F = k^p (P^{gk})^{s^k+\gamma+r_1} * \left|B\right|. \tag{21}$$

$$H = k^p (P^{gk})^{r_2} \text{ mod}(B). \tag{22}$$

$$T = s^k h(M//Z) + r_1 h(M//Z). \tag{23}$$

In this, the random number is specified as r_1 & r_2 and the publically known hash function is signified as $h(\bullet)$.

Step 7: Verification is carried out at the BS (TA) following the generation of the group signatures. The valid group signature for the message M is elucidated by Z, F, H, T, to authenticate the signatures. The verification process is notated as,

$$H^{eh(M//Z)} * (k^p)^{eT} \equiv F^{eh(M//Z)} + r_1 h(M//Z). \tag{24}$$

The BS accepts the message after successful verification; then, encrypts the message for secure DT. The GM opens the signature to validate the signature provided by the biosensor regarding their unique IDS if the verification is unsuccessful.

3.5 Data Encryption via SECC

In the proposed secure DT in the WBSN methodology, data encryption through SECC is the last step. To thwart attacks, the data is encrypted following signature verification. Regarding SECC, data encryption is conducted. In ECC, which is an asymmetric cryptographic methodology, every single user possesses a public along with private keys. For data encryption together with decryption, these keys are utilized. In the traditional ECC, a modification is done by appending the BS's secret key during encryption, in addition, subtracting the BS's secret key with the decrypted message during decryption, to provide additional security in the proposed methodology. This introduction of the BS's secret key in the general ECC is renamed as SECC.

Step 1: Let, the message transmitted as of the BS to the cloud server be M. Firstly, by utilizing the GM's public key (P^{gk}), the message is encrypted. It is signified as,

$$\varsigma^1 = \lambda \times P^{gk}. \tag{25}$$

$$\varsigma^2 = M + \varsigma^1 + c. \tag{26}$$

Here, the cipher text of GM is specified as ς^1, ς^2, the random positive integer selected by the GM is signified as λ and the BS's secret key is proffered as c. Now, the cipher texts are forwarded to the receiver gateway.

Step 2: By utilizing the receiver node's private key (u^r), data is decrypted on the receiver side. It is given as,

$$M = \varsigma^2 - u^r \times \varsigma^1 - c. \tag{27}$$

In such a manner, devoid of any loss in information, the sensitive patient data is securely forwarded to the doctor. The message authentication is offered by the IDGS technique; the message is encrypted by the SECC, which prevents attacks during DT. Furthermore, the efficient usage of clustering by allocating the shortest path betwixt the GM and the BS augments the network lifetime along with mitigates data loss. Section 4 elucidates the experiential outcomes of the proposed methodology.

3.6 Security Analysis

We now examine the proposed scheme's security and show that it satisfies certain security criteria.

Theorem 1: As demonstrated in [28], The proposed scheme can be proved secure in the random oracle model, assuming the CDH problem is hard.

Theorem 1: The suggested technique may be shown secure in the random oracle model, presuming the CDH problem is difficult, as shown in [28].

Proof of Theorem 1: the probability that the challenger solves the CDH problem is

$$ProC \geq \frac{\partial}{9, nQ_1, nQ_2}. \quad \textbf{(28)}$$

In [29], ∂ is a non-negligible probability that an adversary can win the game, where nQ_1 and nQ_2 denote the number of Q_2 and Q_2 queries, respectively. As a result, the challenger can solve the CDH problem with a non-zero *ProC*. Due to the difficulty of the CDH problem, the proposed scheme is secure under the random oracle model.

Theorem 2: The Message integrity and source authentication are both possible with the proposed scheme.

Proof of Theorem 2: The identity-based group signature model that was used in this study is existentially unforgeable against attacks using adaptive selective identity and adaptive chosen message [28]. As a result, attackers are unable to access network services by pretending to be a genuine user, and only valid users can be authenticated by sensor nodes. Additionally, hackers are unable to change broadcast messages or inject fake broadcast messages into the network. In order to accomplish message integrity and source authentication, the proposed approach is successful.

4 Result and Discussion

Here, the proposed technique's performance is evaluated by comparing the outcomes with the existing baseline techniques. The analysis is made regarding some of the performance metrics. The work is executed in JAVA. The superiority comparisons are detailed below.

4.1 Symbols and Descriptions

Table 1 illustrates the detailed descriptions of the symbols utilized in the proposed techniques.

4.2 Performance Assessment of Proposed SECC

Utilizing Encryption Time (ET), Decryption Time (DT), and Security Level (SL), the outcome of the SECC approach that is wielded for data encryption along with decryption is estimated. Rivest-Shamir-Adleman (RSA), ECC, Diffie-Hellman, and Elgamal are the prevailing approaches wielded for the comparison of the SECC as given in the Table 2. The graphical illustration of the ET taken to encrypt the input message by the SECC is given below.

Table 1. Symbols and their description

Symbols	Description
s^i	Group of SNs
n	Number of SNs
x^i, v^i, f^i	Position, velocity, and frequency of bats
$f^{\max}, f^{\min}$	Maximum and minimum frequency
ε	Normalized frequency
t	Time
v^i_{t-1}	Flight speed of bat at time $(t-1)$
x^i_{t-1}	Position of bat at time $(t-1)$
x'', x^{old}	Best position of bat, old position of bat
δ	Random number (0, 1)
L^i_t	Average loudness of bat
X	Condition for bat moving towards prey
P	Movement of bat towards prey
η, ψ	Constants
e^i_{t+1}	Emission rate at time $(t-1)$
e^i_0	Initial value of emission rate
S^k	GM
B^k	BS
τ	IE
d	Euclidean distance
x^h	Unique Id of SNs
c, b, d, e	Secret key, public key and public system parameters
g^m	Private key of GM
γ	Group manager ID
D^{new}	ID of new member
k^p	Public key parameter
M	Message
Z, F, H, T	Group signature for message
P^{gk}	GMs' public key
ς^1, ς^2	Cipher texts
c	Secret key of the BS
u^r	Receiver nodes' private key
λ	Random positive integer selected by GM

Table 2. Tabulation for ET, DT and SL

Techniques	Encryption time (ms)	Decryption time (ms)	Security level (%)
Proposed SECC	2976	3470	96.923
ECC	3807	3896	94.748
RSA	4318	4598	92.125
Elagamal	5193	4588	91.852
Diffie-Hellman	5927	5536	89.794

The ET of the proposed approach along with the prevailing approach is exhibited in Figure 4. Time taken by the encryption algorithm to produce a ciphertext from the plain text is known as ET. When the system takes lesser time, better performance is acquired. Hence, the ET taken by the SECC is 2976ms. Alternatively, the prevailing approaches have an ET of 3807ms, 4318ms, 5193ms, and 5927ms in ECC, RSA, Elgamal, and Diffie-Hellman respectively. The SECC has a lesser ET when comparing the values of the prevailing technique; thus, it performs better than other prevailing methods. In Figure 5, the DT comparison is evaluated.

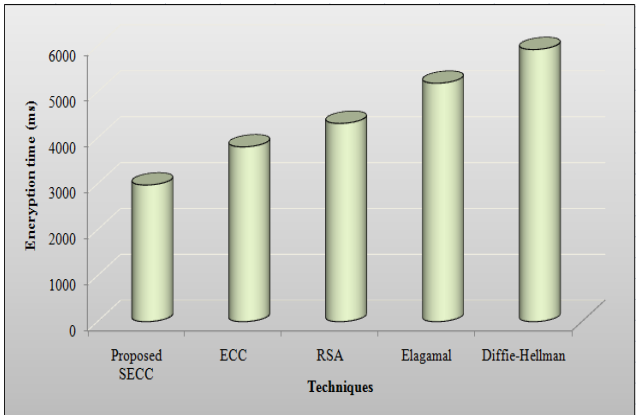

Figure 4. ET comparison of proposed SECC

The proposed along with the existing algorithms' DT is displayed in Figure 5. The time taken to transmute the altered data into its original form is mentioned as DT. At this juncture, to decrypt the encrypted data, the proposed framework needs 3470ms. However, compared to the proposed methodology the conventional ECC needs 3896ms, which is 426ms higher. Similarly, when analogized to the proposed model, other prevailing approaches take a longer time. Hence, it is clear that compared to other state-of-the-art techniques, the proposed approach is enhanced. The proposed works' graphical representation achieved SL is given below.

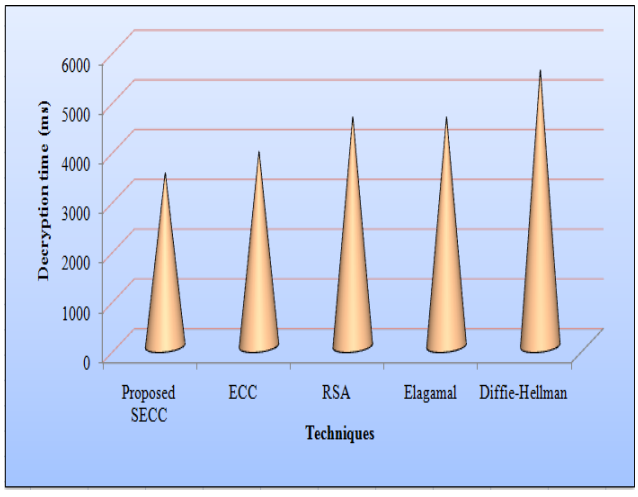

Figure 5. DT assessment of proposed SECC with existing ECC, RSA, Elgamal, and Diffie-Hellman

The SL achieved by the proposed system is analogized with the prevailing methodologies in Figure 6. The SL acquired by the conventional ECC algorithm is 94.748%. Conversely, the SECC achieves 96.923% security which is larger compared to the prevailing ECC, by including the secret of the BS in the general ECC for enhancing security. Moreover, the lower SL is attained by other prevailing approaches like RSA (92.125%), Elgamal (91.852%), and Diffie-Hellman (89.794%). The proposed technique achieves higher outcomes when analogized with the prevailing techniques. Thus, it is obvious that compared to other state-of-art techniques, the proposed technique is much better.

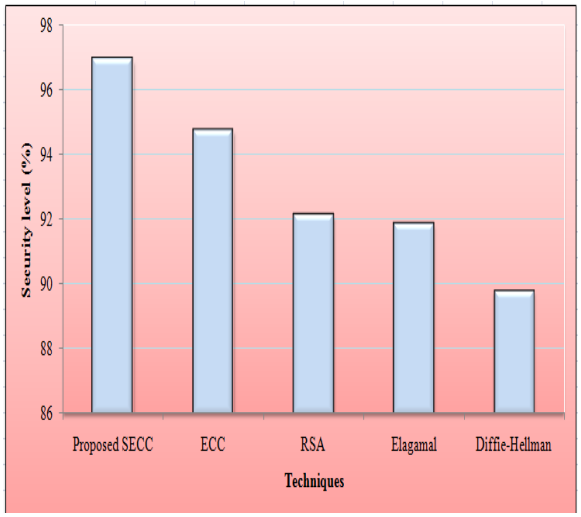

Figure 6. SL analysis of proposed SECC

4.3 Superiority Measurement of Proposed Clustering Technique

Regarding the clustering time, the IEKMA clustering approach's performance, which is deployed to cluster the GM centered on the nearest BS, is examined. With the prevailing Fuzzy C Means (FCM) technique, K-Means Algorithm (KMA), along with K-Medoid, the outcomes are compared. In Table 3, the outcomes are tabulated.

Table 3. Clustering time of proposed IEKMA and existing KMA, FCM and K-Medoid

Techniques	Clustering time (ms)
Proposed IEKMA	1247
KMA	1595
FCM	1984
K-Medoid	2004

The time taken by the IEKMA technique to group the GM is 1247ms, which is extremely low as specified in Table 3. The proposed method's improved performance is illustrated by the lower clustering time. Meantime, the clustering time of a few of the prevailing clustering techniques is compared to validate the proposed methodology's performance. However, comparing the proposed technique, the prevailing methods like KMA, FCM, and K-Medoid achieve a higher clustering time of 1595ms, 1984ms, and 2004ms respectively. Thus, it is obvious that the proposed IEKMA attains enhanced outcomes owing to the alterations made in the KMA.

Table 4. Tabulation for comparison of Average Delay (AD)

Techniques	Delay in ms Number of Nodes				
	20	40	60	80	100
Proposed IDGS	0.23	0.36	0.59	0.19	1.02
SAMAKA	0.63	0.75	0.88	1.34	1.48
IBAAKA	0.84	0.92	0.94	1.171	1.2
DESA	1.03	1.32	1.76	1.96	2.01
SEEMAKA	1.21	1.68	1.79	1.96	2.14

Table 5. Tabulation for energy consumption

Techniques	Energy consumption (joules) Number of nodes				
	20	40	60	80	100
Proposed IDGS	3322.25	3273.36	4005.36	4333.24	4022.25
SAMAKA	3815.95	4001.29	4152.32	4525.32	5015.95
IBAAKA	3911.26	4143.68	4267.34	5132.85	5411.26
DESA	4216.64	4921.14	5169.25	5672.26	5875.26
SEEMAKA	4819.17	5122.24	5472.63	5651.32	6119.17

Table 6. Tabulation for key mismatch ratio

Techniques	Key mismatch ratio Number of nodes				
	20	40	60	80	100
Proposed IDGS	0.154	0.162	0.232	0.273	0.368
SAMAKA	0.161	0.191	0.241	0.332	0.375
IBAAKA	0.197	0.212	0.265	0.347	0.439
DESA	0.202	0.246	0.307	0.361	0.405
SEEMAKA	0.233	0.251	0.327	0.383	0.469

Table 7. Tabulation for memory usages (Bits)

Techniques	Memory usage (bits) Number of nodes				
	20	40	60	80	100
Proposed IDGS	177	194	214	273	308
SAMAKA	192	213	261	291	341
IBAAKA	201	233	302	329	362
DESA	234	273	338	382	414
SEEMAKA	263	319	392	401	423

Table 8. Tabulation for packet delivery rate (Kbps)

Techniques	Packet delivery rate (Kbps) Number of nodes				
	20	40	60	80	100
Proposed IDGS	191	289	385	481	578
SAMAKA	187	244	331	377	472
IBAAKA	176	231	328	364	361
DESA	164	189	255	281	359
SEEMAKA	158	164	220	258	281

4.4 Performance Estimation of Proposed IDGS Authentication Framework

Here, in the IDGS scheme, the effectiveness is evaluated by comparing its outputs like Average Delay (AD), Energy Consumption (EC), key mismatch ratio, memory usage, Packet Delivery Rate (PDR), computation cost, and CT with the output of the prevailing SAMAKA [25], IBAAKA Protocol [24], Data Encryption and Signature-based Authentication protocol (DESA) [27], SEEMAKA [26] techniques.

The AD of the proposed along with the prevailing SEEMAKA, DESA, IBAAKA, along SAMAKA approaches are examined in Figure 7. The time variation betwixt the packets received at present to packets received formerly is signified by the AD as given in the Table 4. When the number of nodes increases, the AD augments. The time difference taken by the proposed framework is increased for the number of 20 to 100 nodes as, 0.23ms to 1.02ms, while the elevations in the time difference taken by the prevailing techniques are 0.63ms to 1.48ms, 0.84ms to 1.2 ms, 1.03ms to 2.21ms, and 1.21ms to 2.14ms. Thus, the examination showed that compared to the prevailing methods, the proposed method's AD is lower.

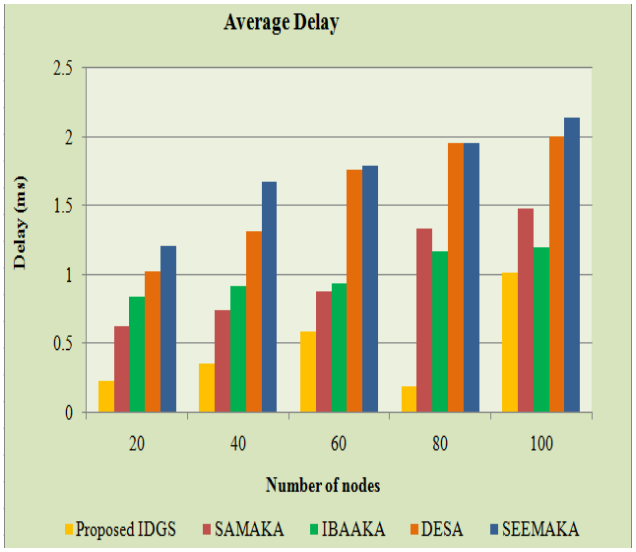

Figure 7. AD of the proposed and existing techniques

The quantity of energy consumed by the proposed along with prevailing approaches is demonstrated in Figure 8. To assess the proposed approach, EC is the main parameter since it shows the particular level of energy consumed by the nodes during the process of DT as given in the Table 5. The EC of the proposed methodology for the maximum of 100 nodes is 4022.25J. The EC of the prevailing techniques SAMAKA (5015.95J), IBAAKA (5411.26J), DESA (5875.26J), and SEEMAKA (6119.17) is higher than the proposed approach. The proposed framework provides a lesser EC value also for the remaining number of nodes. Hence, the examination conveyed that for a rising number of nodes, the proposed IDGS scheme requires very little energy.

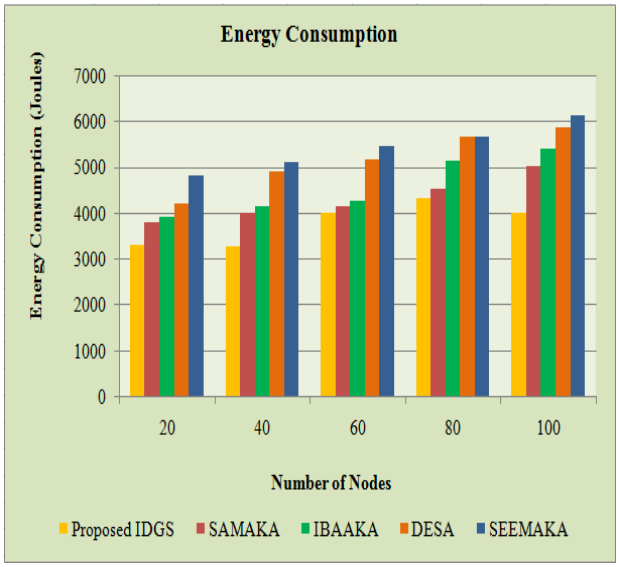

Figure 8. Performance evaluation by means of EC

In Figure 9, the proposed along with the prevailing approaches' key mismatch ratio is evaluated. The ratio between different numbers of bits in the secret keys with the total number of key bits produced for signature verification is specified as a key mismatch as given in the Table 6. Since the key mismatch ratio recognizes the false private key that is generated by the malicious nodes, it should be less for the enhanced performance. In this aspect, the proposed methodology's key mismatch ratio is differed as 0.154, 0.162, 0.232, and 0.273, along with 0.398 for 20 nodes, 40 nodes, 60 nodes, 80 nodes, and 100 nodes respectively. When analogized to the prevailing approaches low mismatch ratio is obtained by the proposed methodology, which is highly efficient with strong private keys.

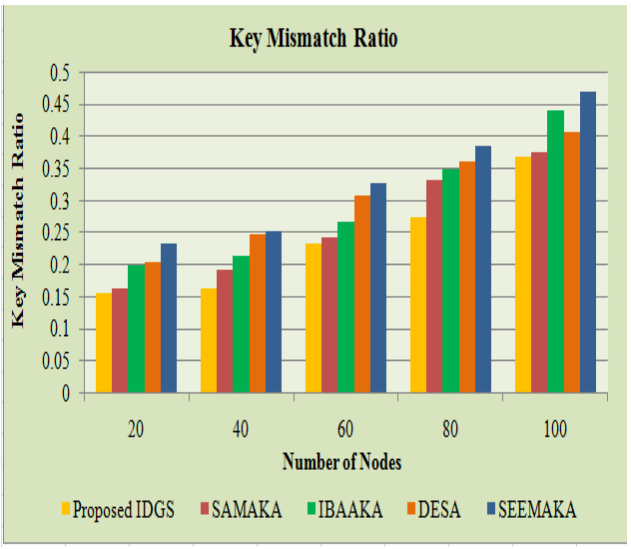

Figure 9. Key mismatch ratio analysis of proposed technique

Regarding memory usage, the proposed along with prevailing methods' performance is depicted in Figure 10 as given in the Table 7. The amount of memory necessary

to store the data is termed memory usage as given in the table. By examining the above figure, for the number of 20 to 100 nodes, the memory desired by the proposed technique is 177bits, 194bits, 214 bits, 273 bits, 308 bits respectively. With the number of nodes, the memory usage of the proposed mechanism is raised, but the raising level is not exceeded compared to the prevailing methods. The proposed IDGS's efficiency is established from this examination.

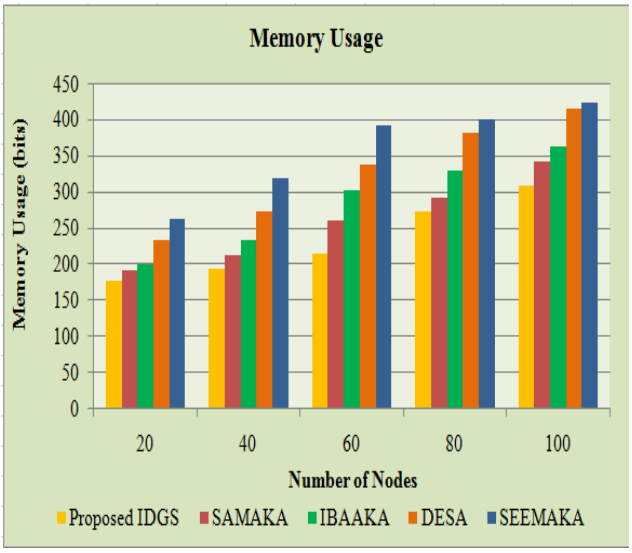

Figure 10. Superiority measure based on Memory usage of the proposed and existing techniques

Regarding PDR, the prevailing along with the proposed method's performance is exhibited in Figure 11. The number of packets reached successfully to the receiver node is pointed out by it as given in the Table 8. The PDR by the proposed method is 191kbps for the minimum number of nodes, while the PDR is 578kbps for a maximum number of nodes. However, the prevailing approaches have a lower PDR for all nodes. Thus, the proposed methodology is superior to the prevailing methodologies.

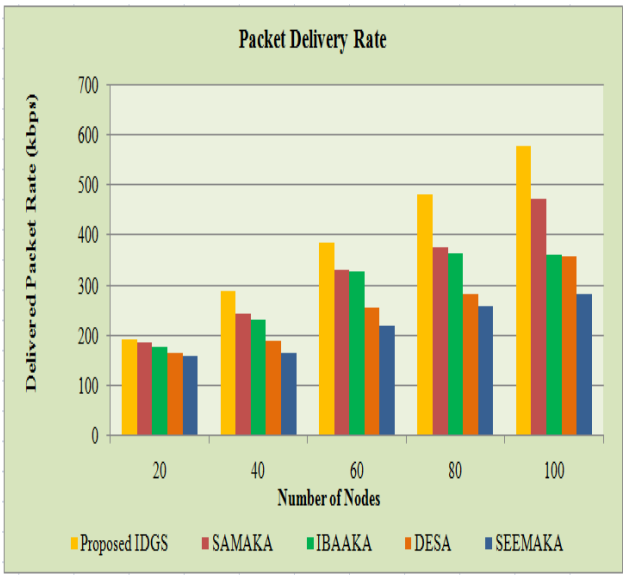

Figure 11. Comparison of PDR of proposed IDGS and existing SAMAKA, IBAAKA, DESA and SEEMAKA

The proposed along with existing methods' computation cost is examined in Table 9. The time taken by the system to generate the group signatures is termed as computational cost. For the proposed model the computation cost is 4.1 ms, while the prevailing methods attain the computation cost of 19.1 ms, 8.23ms, 5.13ms, and 12.30ms for SAMAKA, SEEMAKA, IBAAKA, and DESA respectively. From this examination, the proposed framework's lower computation cost specifies that compared to the prevailing approaches, the IDGS scheme has much-enhanced computation efficiency.

Table 9. Tabulation of computation cost of the proposed and existing techniques

Methods	Computation cost
Proposed IDGS	4.1
IBAAKA	5.13
SEEMAKA	8.23
DESA	12.3
SAMAKA	19.1

The computation time of the proposed along with prevailing approaches are compared in Figure 12. 1.12ms is the computation time of the proposed method. However, the computation time of the prevailing approaches are 1.88ms, 2.02ms, 2.21ms, and 2.84ms which are higher than the proposed approaches. Hence, from the analysis, it is clear that the proposed methodology has better performance than the prevailing approaches.

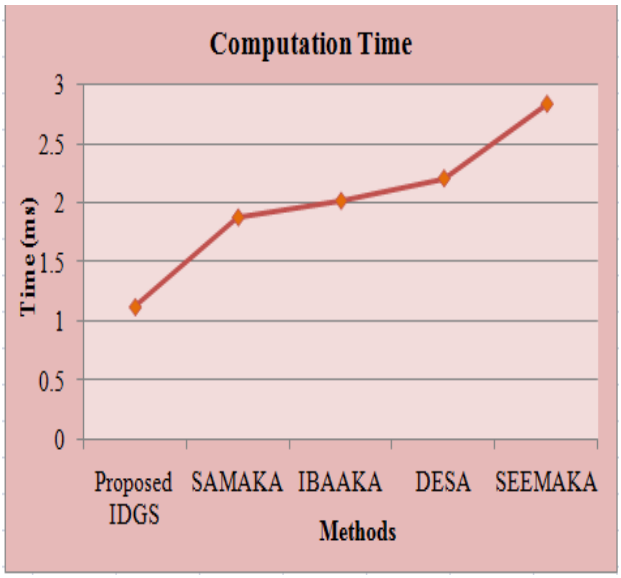

Figure 12. Performance evaluation based on computation time

5 Conclusion

Here, by employing a novel IDGS along with SECC methodology, an energy-efficient secure DT is WBSN is proposed. In this, for message authentication, the IDGS model is utilized; likewise, for the secure transmission of patient medical data, the SECC methodology is deployed. The

clustering mechanism is utilized here to enhance EE. Lastly, the experiential outcomes are analogized with conventional authentication along with privacy-preserving methodologies. The outcomes displayed that an SL of 96.923% is achieved by the IDGS model. Similarly, the computation cost and energy consumed by the IDGS methodology are 4.1ms and 4022.25J, respectively. The proposed methodology's key mismatch ratio is 0.154. A better performance was exhibited with the lowest value of mismatch ratio. Hence, it is revealed that the proposed framework is highly effectual in securing along with authenticating DT in the WBSN. This work will be enhanced by pondering privacy along with security utilizing advanced authentication together with authorization methodologies in the upcoming future.

References

[1] P. T. Kalaivaani, R. Krishnamoorthi, Design and implementation of low power bio signal sensors for wireless body sensing network applications, *Microprocessors and Microsystems*, Vol. 79, Article No. 103271, November, 2020.

[2] C. Rameshkumar, T. Ganeshkumar, A Novel of Survey: In Healthcare System for Wireless Body-Area Network, *International Conference on Applications of Computational Methods in Manufacturing and Product Design*, Springer, 2022, pp. 591-609.

[3] A. R. Bhangwar, A. Ahmed, U. A. Khan, T. Saba, K. Almustafa, K. Haseeb, N. Islam, WETRP weight-based energy & temperature aware routing protocol for wireless body sensor networks, *IEEE Access*, Vol. 7, pp. 87987-87995, June, 2019.

[4] A. K. Pandey, N. Gupta, An energy efficient distributed queuing random access (EE-DQRA) MAC protocol for wireless body sensor networks, *Wireless Networks*, Vol. 26, No. 4, pp. 2875-2889, May, 2020.

[5] P. Kasyoka, M. Kimwele, S. M. Angolo, Towards an efficient certificateless access control scheme for wireless body area networks, *Wireless Personal Communications*, Vol. 115, No. 2, pp. 1257-1275, November, 2020.

[6] A. Sivasangari, S. Bhowal, R. Subhashini, Secure encryption in wireless body sensor networks, *International Conference on Emerging Technologies in Data Mining and Information Security*, Vol. 814, Springer, 2019, pp. 679-686.

[7] F. T. Zuhra, K. B. A. Bakar, A. A. Arain, U. A. Khan, A. R. Bhangwar, MIQOS-RP: multi-constraint intra-ban, qos-aware routing protocol for wireless body sensor networks, *IEEE Access*, Vol. 8, pp. 99880-99888, May, 2020.

[8] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. Islam, D. Giri, A robust authentication and access control protocol for securing wireless healthcare sensor networks, *Journal of Information Security and Applications*, Vol. 52, pp. 1-14, June, 2020.

[9] J. D. Rao, K. Sridevi, Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy, *Materials Today Proceedings*, Vol. 45, No. 2, pp. 1498-1501, 2021.

[10] M. Shuai, L. Xiong, C. Wang, N. Yu, Lightweight and privacy-preserving authentication scheme with the resilience of desynchronization attacks for WBANs, *IET Information Security*, Vol. 14, No. 4, pp. 380-390, July, 2020.

[11] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, E. M. Mohamed, A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks, *IEEE Access*, Vol. 8, pp. 131397-131413, July, 2020.

[12] A. Joshi, A. K. Mohapatra, Authentication protocols for wireless body area network with key management approach, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 22, No. 2, pp. 219-240, March, 2019.

[13] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, M. A. Doostari, A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT, *Computer Networks*, Vol. 177, Article No. 107333, August, 2020.

[14] J. Zhang, Q. Zhang, Z. Li, X. Lu, Y. Gan, A lightweight and secure anonymous user authentication protocol for wireless body area networks, *Security and Communication Networks*, Vol. 2021, Article No. 4939589, July, 2021.

[15] L. Li, L. Liu, H. Peng, Y. Yang, S. Cheng, Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks, *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 3212-3227, April, 2019.

[16] S. R. H. Remu, Md. O. Faruque, R. Ferdous, Md. M. Arifeen, S. Sakib, S. M. S. Reza, Naive bayes based trust management model for wireless body area networks, *Proceedings of the 5th international conference on computing advancement*, Dhaka, Bangladesh, 2020, pp. 1-4.

[17] A. Sammoud, M. A. Chalouf, O. Hamdi, N. Montavont, A. Bouallegue, A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis, *Computers and Security*, Vol. 96, Article No. 101838, September, 2020.

[18] J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, J. Lin, A logistic mapping-based encryption scheme for wireless body area networks, *Future Generation Computer Systems*, Vol. 110, pp. 57-67, September, 2020.

[19] K. Chatterjee, an improved authentication protocol for wireless body sensor networks applied in healthcare applications, *Wireless Personal Communications*, Vol. 111, No. 4, pp. 2605-2623, April, 2020.

[20] S. Jegadeesan, M. Azees, R. Babu, U. Subramaniam, J. D. Almakhles, EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs), *IEEE Access*, Vol. 8, pp. 48576-48586, March, 2020.

[21] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, A. Mosavi, A lightweight genetic based algorithm for data security in wireless body area networks, *IEEE Access*, Vol. 8, pp. 183460-183469, October, 2020.

[22] H. Ryu, H. Kim, Privacy-preserving authentication protocol for wireless body area networks in healthcare applications, *Healthcare*, Vol. 9, Article No. 1114, September, 2021.
[23] M. Shuai, B. Liu, N. Yu, L. Xiong, C. Wang, Efficient and privacy-preserving authentication scheme for wireless body area networks, *Journal of Information Security and Applications*, Vol. 52, Article No. 102499, June, 2020.
[24] M. Kumar, S. Chand, A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network, *IEEE Systems Journal*, Vol. 15, No. 2, pp. 2779-2786, June, 2021.
[25] B. Narwal, A. K. Mohapatra, SAMAKA: secure and anonymous mutual authentication and key agreement scheme for wireless body area networks, *Arabian Journal for Science and Engineering*, Vol. 46, No. 9, pp. 9197-9219, September, 2021.
[26] B. Narwal, A. K. Mohapatra, SEEMAKA: secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks, *Wireless Personal Communications*, Vol. 113, No. 4, pp. 1985-2008, August, 2020.
[27] M. Ayyadurai, S. Varalakshmi, K. Chokkanathan, K. S. Kumar, Signature based key authentication protocol for wireless body sensor networks, *European Journal of Molecular & Clinical Medicine*, Vol. 7, No. 3, pp. 5563-5572, August, 2020.
[28] J. Subramani, A. Maria, R. B. Neelakandan, A. S. Rajasekaran, Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification, *Communications*, Vol. 15, No. 9, pp. 1187-1197, June, 2021.
[29] J. Katz, J. Loss, M. Rosenberg, Boosting the security of blind signature schemes, *International Conference on the Theory and Application of Cryptology and Information Security*, *Springer*, Vol. 13093, 2021, pp. 468-492.

Biographies

C. Ramesh Kumar is currently working as an Assistant Professor at Galgotias University. He is pursuing his Ph.D degree in Computing Science and Engineering at Galgotias University, Uttar Pradesh, India. His research interests include network security, wireless body area network, wireless sensor network

T. Ganesh Kumar received his Ph.D degree from the Computer Science and Engineering at Manonmaniam Sundaranar University, Tirunelveli, India. He is currently working as an Associate Professor in the School of Computing Science & Engineering at Galgotias University, Delhi NCR, India. His research interest includes Computer Networks, Remote Sensing and Medical Imaging.

A. Hemlathadhevi received the Ph.D. degree in Computer Science and Engineering at St Peter's University, Tamil Nadu, India. At present, working as an Associate Professor in the Department of Computer Science and Engineering at Panimalar Engineering College, Chennai, India. Her research interest includes network security and cloud computing security.

D. R. Thirupurasundari received the Ph.D. degree in Computer Science and Engineering at Shri Venkateshwara University, Gajraula, India. At present, working as an Associate Professor in the Department of Computer Science and Engineering at Bharath Institute of Higher Education and Research, Chennai, India. Her research interest includes network security and IOTs.