How to Cite:
Kumar, C. R., Kumar, T. G., & Hemlathadhevi, A. (2022). A novel authentication scheme of identity based group signature algorithm for wireless body sensor network (WBSN). *International Journal of Health Sciences*, *6*(S1), 3448–3463. https://doi.org/10.53730/ijhs.v6nS1.5512

A Novel Authentication Scheme of Identity Based Group Signature Algorithm for Wireless Body Sensor Network (WBSN)

C. Ramesh Kumar
Research Scholar, School of Computing science and Engineering, Galgotias University, Greater Noida, UP, India
Email: c.ramesh@galgotiasuniversity.edu.in

T. Ganesh Kumar
Associate Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida, UP, India
Email: t.ganesh@galgotiasuniversity.edu.in

A. Hemlathadhevi
Associate Professor, Department of Computer Science & Engineering, Panimalar Engineering College, Chennai, Tamil Nadu, India
Email: hemlathadhevi@gmail.com

***Abstract*---**Wireless Body Sensor Network (WBSN) faces several security problems such as loss of information, access control and authentication. As WBSN collects vital information and operates in unfriendly environment, severe security mechanisms are needed in order to prevent the network from anonymous interactions, authentication is the initial steps towards providing security. An enhanced authentication scheme prevents the system from imposters effectively. In this paper, a novel authentication using identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. The proposed method employs identity-based group signature algorithm between biosensors and group manager (GM). An extensive set of experiments were carried out and the results are examined interms of computation cost and energy consumption.

***Keywords*---**Authentication, Group signature, Identity Based encryption, Biosensor, Group manager, WBSN.

***Corresponding author**: Kumar, C.R.; Email: c.ramesh@galgotiasuniversity.edu.in*
Manuscript submitted: 18 Jan 2022, Manuscript revised: 09 Feb 2022, Accepted for publication: 27 March 2022

Introduction

Wireless Sensor Networks (WSNs) are well-known and identify application in various IoT domains like armed forces, transportation, medicine, and so forth. In addition, Wireless Body Sensor Networks (WBSNs) is the extended version of WSNs that make use of wearable computing tools to process the applications. The remote healthcare observation of patient's health (Narwal & Mohapatra, 2021) is an instance of WBSN, where doctors often observe patient's health condition with no requirement of physically visiting the hospital. The provided affordability as well as simpler use of sensor nodes and inbuilt tools, WBSNs can be applied with minimum cost. While deploying WBSN, wearable sensors gather and transmit data for distant providers for immediate processing of data. Hence, WBSNs offer the additional objects for physicians to start spontaneous responses for deadly health conditions, like Sudden Infant Death Syndrome (SIDS). Fig. 1 depicts the method of cloud-based WBSNs.

Applying the wireless protocols like ZigBee (Latha & Vetrivelan, 2020) for transmitting data in WBSNs domains improve the communication facility for good experiment. Additionally, in medical sectors WBSNs is found in video streaming, data transmission, 3-Dimensional video, entertainment, such as games and social media. Power game-assisted techniques were presented to reduce the interaction disturbance for WBSNs which depends upon social network. The IEEE 802.15.6 wireless communication standard was created by the Institute of Electrical and Electronics Engineers to improve the measures of WBSNs. The primary purpose of this model is to set a high bar for low-power, short-range, and robust wireless communication around the human body. It can handle a broader range of data values in a variety of applications, including short-range and wireless communications.

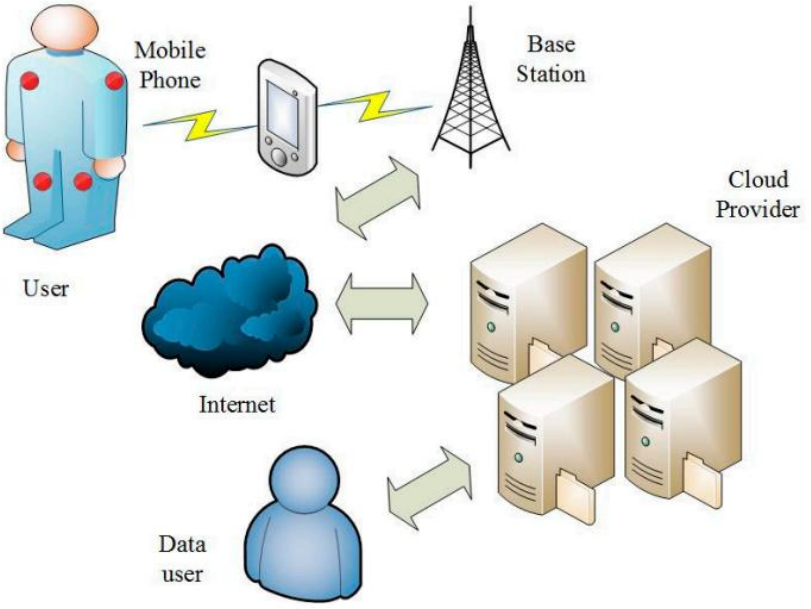

Figure 1. *Architecture of WBSN*

Here, WBSN is constrained with a problem of security level and privacy for given data. This method has the responsibility to offer data integrity as well as privacy, as the data can only be used by authorized users and not by any of the third parties. But, the resource limitations in WBSNs with respect to energy, storage, bandwidth potential, processing resources, and so on. The assured stability as well as data integrity in WBSN fields differs every time. IEEE 802.15.6 states 3 levels of security: The initial once is Level 0 which, is an unsafe communication; it is considered to be a minimum-security level in 802.15.6 that are lack of security measures. Secondly, Level 1 is an authorized approach, which denotes authority as well as concurrent encryption technique to attain maximum security goal in 802.15.6. These standards require all devices take part in transmitting data should be assured with effective security level. Moreover, a pre-defined Master Key (MK) is enabled in unicast communication; a Pairwise Temporal Key (PTK) has been produced for single application; a Group Temporal Key (GTK) is provided and distributed with respective group in case of multicast communication.

Security research in WBSNs: Generally, a communication method of WBSN could be portioned as 2 segments. The primary segment is present within a body communication, that implies a interaction among sensor nodes. As the alternate segment present external to body communication which denotes that, communication from gateway to another network applicants like service provider, remote observation as well as cloud servers. In order to compute the physiological data of clients in WBSNs, diverse inside-body authority approaches are presented (Kadel et al., 2018).

In (Ding et al., 2021), the inter-pulse duration of Electrocardiogram (ECG) as well as Photoplethysmogram (PPG) is applied to produce cryptographic keys for encryption and authentication. In (Venkatasubramanian et al., 2008), it is employed with frequency coefficients of ECG and PPG generate cryptographic keys. (You et al., 2018) implied a suggestion of a fuzzy vault that has been vastly employed in the application of field of biometric authorization. Then, a Physiological Signal Key Agreement technique (PSKA) depends upon fuzzy vault, which is presented in (Ding et al., 2021). But, the application of additional chaff points in PSKA model improves the processing expense. In (Miao et al., 2010), extended fuzzy vault models along with ECG signal were projected to enhance the working function. An improved fuzzy vault technique (Dodis et al., 2008) is proposed, which has been utilized for key generation on the basis of fingerprint.

In (Fotouhi et al., 2020), Biel et al. developed a method to apply the ECG signal for biometric integrity that requires producing a signal format to validate the similarity by a comparison. As the application of these constant templates, this model does not accomplish optimal security performance. In (Zhang et al., 2012), a method assisted on time differentiation ECG feature is presented for authenticity and to filter the authentic key. But, these models depend upon physiological attribute like accuracy, as the gathered signals are from similar individual which often deals with marginal variations. Additionally, a physiological signal is time-variant, permanent clock synchronizing is required which is more difficult to attain. Moreover, these methodologies meet compatibility problems while applied with various sensors, which often suffers from real-time shortcomings.

To resolve the certificate handling issue, (Shamir, 1985) applied a technique of identity based Public Key Cryptosystem (ID-based PKC). In ID-based PKC, a user's similarities like, name, email and mobile number, are the public keys. Hence, this data not require maintenance. According to the ID-based PKC, massive identity-oriented authentic approaches are presented (Jiang et al., 2013). But these models are not applicable for WBANs due to the inability to offer client anonymity and developed for client-server platform. In order to convince the security needs in WBANs, (Zia et al., 2020) deployed 2 ID based authentication techniques with the application of certificate-less signature module. Therefore, (Liu et al., 2012) noticed that Liu et al.'s framework could not support the stolen verifier-table attack. On the other hand, pointed that initial procedure is unable to offer anonymity. To enhance the security and effectiveness, Zhao projected an anonymous authenticity technique for WBANs. Thus, method could not provide real-time anonymity due to the customer's pseudo affinities are static measures and affect the customers. By using the increased security measurements, it is required to develop anonymous authentication approach to obtain real-time anonymity.

In this paper, a novel authentication using identity-based group signature (IBGS) protocol has been proposed to provide security to the WBSN. The proposed method employs identity-based group signature algorithm between biosensors and group manager (GM). An extensive set of experiments were carried out and the results are examined interms of computation cost and energy consumption.

Literature Review

WBAN is a multifaceted network of hub sensors used to detect and transmit information at various levels in real time. Sensor units collect critical data and send it to a medical center for further review. Sensor hubs fully meet the limits of quantity, memory and power. Information is the most important part of a patient's illness, so security and data protection are paramount. There are many killers who can undermine critical information about patient's health. The WBAN Data Security Study is a study conducted around 2017-2021. Many of the articles presented in the course provide a detailed discussion of these articles under consideration. There are a number of studies that have been developed to maintain data security in WBAN, and these experiments ensure that remote sensors work effectively on a variety of concepts. Many statistical techniques are considered for success problems such as failure failure, integration problems, and the use of data modification capabilities. The document is encrypted in various formats such as SHA (Secure Hashing Algorithm), AES (Advanced Encryption Standards), LEA (Easy Encryption Encryption).

A robust and reliable protocol for WBAN that focuses on what can be called sensors that are inserted into patients 'bodies to monitor their health (Sharma, 2020). The human body is connected to the Internet through mobile devices. Healthcare professionals use this data to treat patient diseases such as asthma, diabetes, coronary heart disease and bleeding.

The Security and Energy Protocol is used to use WBAN Advanced Encryption Security (AES) encryption and the SHA-1 hash function to provide BAN security.

SHA-I is challenging for WBAN, but the workload is reduced thanks to a chain hash protocol that uses Baker's Chaos Card for security (Vyas & Pal, 2019). Experts are well organized in terms of memory, computing power and bandwidth. The protocol generates a Baker chaos map for data separation, and this method is used to generate pseudo-random key streams.

Introduction of a lightweight secure communication system for PMS, with a focus on a secure patient monitoring system transportation system. The medical information of the patient is delivered to the gateway via a connected connection from the sensor to the body (Arfaoui et al., 2019). This article is dedicated to preventing data theft and ensuring that the key in the data can be identified by the appropriate user. Achievements in the Internet of Things (IoT) by those who bring smart systems, which have a wide range of health services. As a result, these systems put security and privacy at risk. The security system is low-power and resource-intensive. It starts a counter value, called the first value of a vector (IV), multiplied in a pseudo-random manner, using the AES-CTR method. Most counters employ an encryption algorithm like AES-128 bit, which uses a simple XOR function comparable to the CTR mechanism used in the XOR function.

To transport data over the network, WBAN requires basic and efficient resources. Many technologies have been required for security purposes, and this research paper focuses on integration by generating symmetric keys through a physical layer or a link containing the researched RSSI. This article presents an enterprise solution for improving the diversity and quantity of RSSI data to obtain an accurate image. The employment of different paths between a group of members and a group, or occasionally between two groups, to combine RSSI data with a plethora of overlapping multichannel information, boosting coherence and flexibility, is a critical breakthrough.

The WBAN is linked to the WSN WBAN, which is made up of small sensors that collect data from the human body and send it to a biomedical server via a network (Almuhaideb & Alqudaihi, 2020). The major purpose of the system is to ensure the security and confidentiality of network data. There are a variety of security systems available to ensure data security and avoid a variety of threats. This article goes through cryptography and some of the most essential encryption technologies for data security. Providing strong cryptography and protection of data from large volumes. Use cheating technology to achieve safe time and use accurate memory to think. The critical control protocol is built into the security application.

To make data transfer safer and more dependable, researchers are adopting secure hashing algorithms (SHA) and encryption technologies. It produces digital signatures throughout the hashing process to obtain patient data in a secure and correct manner (Ullah et al., 2019). This approach has been used to create an asymmetric key with two public keys and two private keys, lengthening and complicating the algorithms. WBAN data transfer with digital signatures, the created programme is based on a combination of multiple approaches to prevent data theft on WBAN using hard keys and digital signatures. Because of its public keyless keys, such as BNC, and the complete sensor node in encryption and decryption systems, this idea is particularly stable (Tan & Chung, 2019). BNC

records each data set using SK and sends it to all sensor nodes in the system using digital signatures.

In this paper, data was recorded using ECC and Diffie Hallman (DH). The need of keeping track of essential patient health data is so great that many different systems are utilized to keep track of it. As a result, the asymmetric ECC method is employed in this study (Jegadeesan et al., 2020). To achieve data security, DH is employed to generate keys in the system. Patients and doctors are two sorts of users, thus this article focuses on user authentication, which involves registering the correct Internet users in order to keep their personal information in a database, such as their fingers or palms. The ECC and DH algorithms are used to merge this biological data. It is transformed to binary before being assessed for various values such as 128, 192, and 256 bits. Both decryption encryption time and high processing time are taken into account while evaluating masseurs (Ren et al., 2019).

Data is transmitted via a network using WBAN technology, which is continually evolving. Taking good care of your data might be difficult (Lara et al., 2021). For data security, this article employed a three-way authentication mechanism with the ECC Programme. In the study, WBAN was also implemented utilizing star topology. There are two types of keys in asymmetric cryptography: public and private keys, which are mathematically coupled. There are two purposes in cryptography for achieving security: data authentication and patient authentication (Kumar & Chand, 2021). To encrypt and decrypt sensitive data, public and private keys are utilized.

Materials and Methods

This section defines about the models of an identity-based group-signature (IBGS) technique as given in the following. Fig. 2 shows the system architecture of the proposed model. The proposed model involves four main components, namely cloud server, Key generation center (KGC), User and Auditor.

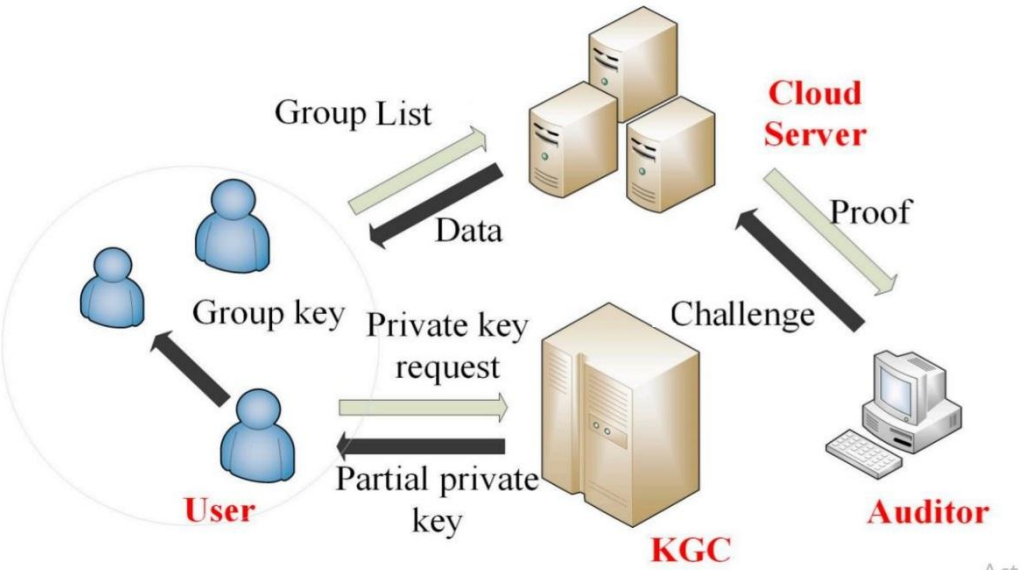

Figure 2. *System architecture of proposed model*

This model depends upon identity-based digital signature approach.
Definition 1: (Identity-based Group Signatures) It is an identity-based digital signature method is composed with 5 patterns given as follows:

- Setup: A technique, implemented by a Group Manager (GM), consumes an arbitrary security attribute l in the form of input and produces few system attributes as well as a master key. As a result, the system parameters are known by the primary group public key, while the master key is known by the group manager.
- Extract: The protocol from a GM and member. It has been considered that, interaction among a member as well as a GM is private and authorized. Consequently, a member is an authorized for this group. The outcome of a membership secret and a membership certificate. The member's secret is divided into two parts: the first is forwarded by a GM, and the second is chosen by the member himself, with two parts validated.
- Sign: A hypothetical model with group public key and membership secret as inputs, where a message m is the outcome of group signature of m.
- Verify: In terms of group public key, a model for introducing the time of reduced group signature of a message.
- Reveal: The given message is a valuable group signature, and it computes the similarity of the original author using a group public key and a group manager's master key.

A secure ID-based group signature model has to convince every features provided:

- Correctness: The VERIFY framework must approve any group signatures generated by a group member using the SIGN paradigm.
- Unforgeability: The Members of the group can sign communications in the presence of the underlying group.
- Anonymity: Finding the authentic signer of a letter when given a valuable

signature is impossible for everyone but a group manager.

- Unlinkability: Selecting two different effective signatures is handled by a similar group member who is more sophisticated.
- Excludability: A group member or a GM has the authority for signing instead of alternate group members.
- Traceability: A GM often finds the original signer for a valuable signature for disputes.

Setup

It is assumed to be a system generation method. A GM implements the procedures given as follows:

1) Select p, q, GP_1, GP_2.
2) Select 2 cryptographic hash functions:

$$H: \{0,1\}^* \mapsto GP_1, \quad (1)$$

$$H_1 : \{0,1\}^* \times GP_1 \mapsto GP_1. \quad (2)$$

3) Develop a bilinear function provided:

$$e: GP_1 \times GP_1 \mapsto GP_2. \quad (3)$$

4) Choose a generator unit $P \in GP_1$, hence $e(P,P)$ is a generator unit of GP_2.
5) Choose an integer a from Z_q^* as a secret key of GM; Fix $P_{pub} = aP$ as the PK in this group.
6) Assume the string $f \in \{0,1\}^*$ denotes a separate group member's identifier. The PK of this member is determined by GM as $Q_f = H(f)$.The practical identity of a few group members can be easily predicted by their email or IP address.
7) Suppose $\{0,1\}^*$ A message space is a collection of strings of various lengths.

Thus, a PK of this group is: $PK = \{P, P_{pub}, e(\cdot,\cdot), H, H_1\}$ The master key of GM is $SK = a$.

Extract

Assume a new member U_i requires being an authenticated member of this group. GM would interact with U_i by using secure channel:

1) U_i transmits its own identifier f_i to GM;
2) GM determines $sk_i = aQ_{f_i}$, and then forwards it to U_i.
3) U_i has a private value b_i and corresponding identifier f_i as its personal secret key as well as personal PK. Let $b_i f_i \equiv 1 \bmod \varphi(n)$, where n is a combination of 2 higher prime numbers.
4) U_i and GM are implements a Schnorr identifying protocol. Thus, GM attains a credential t_i that has been applied to find the membership ofU_i.
5) GM is composed with transcriptor: $trans = \{< f_i, t_i > |$ for all authenticated group member$U_{f_i}\}$. Therefore, the transcriptor is executed by GM.
6) As a result, U_i joins this group as an authenticated member. The credential is t_i, the personal secret key is $\{b_i, sk_i\}$; the personal PK is f_i, and

the personal secret key is $\{b_i, sk_i\}$;These data are recorded on a smart card that U_i.owns.

Sign

It is named as a generation technique of group-signatures. Let U_{f_i} is actual member of this group. Provided a message $m \in M$, to process the function:

1) Select random and uniform x from Z_q^* and sets $A = xP$.
2) Determine $B = x^{-1}sk_i + H_1(m, A)b_i$, where $x - 1$ implies the contrast of x in Z_q^*.

Thus, the group-signature on message m is $\{A, B, f_i\}$.

Veri

It is also a verification module on applied group-signatures. Provided a message m as well as alleged group-signature$\{A, B, f_i\}$, and different verifier holds a PK that validates the lifetime of group signature by performing the functions given below:

1) Determine $\alpha = e\left(f_i P_{pub}, Q_{f_i}\right)$;
2) Determine $\beta = e(A, f_i B)$;
3) Determine$\gamma = e\left(A, H(m, A)\right)$.

Finally, the verification method validates the equation:

$$\beta =^{?} \alpha\gamma \tag{4}$$

When the equality is present, then the verification approves: $\{A, B, f_i\}$ as a valuable group signature on message$m$; else, it has been eliminated. Besides, by using a group PK the verifier learns the signature emerging from a group; whereas, by applying personal PK the verifier understands that the signature has been produced by authentic members and not by an GM.

Reveal

This model can only be executed by a GM. As the message m and its own valid group-signature$\{A, B, f_i\}$, the GM seeks for tanscriptor of respective membership credentialt_i. With the application of Schnorr identifier and group membership credential, a GM accepts the practical similarity of group-member.

Remark 1: According to the SETUP technique, a model of various trust authorities is used to decide and build many GM in order to avoid the centralization of group members' identities into a single GM. GM's denial of service is no longer an issue.

Remark 2: The proposed protocol is a signature paradigm that allows each legitimate member to sign papers individually rather than as part of a group. If a protocol for a common signature technique is used, it means that each user can only sign papers.

Remark 3: The presented protocol is present in a setting of super singular elliptic curves whereas the setting of prime-order multiplicative subgroup of a definite application. Besides, a predefined curve does not apply the knowledge proof, and applied this kind of proof.

Results and Discussions

This section, a detailed computation cost analysis of diverse models takes place under varying number of messages. A comparative analysis is made with the Public Auditing with Privacy Protection (PAPP) and Certificateless public auditing (CPA) interms of computation cost and energy efficiency cost. Table 1 and Fig. 3 show the computational cost of our proposed method. Under the message count 1, it is shown that the proposed IBGS requires a minimum computation cost of 1s, whereas the PAPP and CPA models reaches to a maximum computation time of 2s and 4s respectively. Under the message count 10, it is shown that the proposed IBGS requires a minimum computation cost of 3s, whereas the PAPP and CPA models reaches to a maximum computation time of 5s and 8s respectively. Under the message count 20, it is shown that the proposed IBGS requires a minimum computation cost of 5s, whereas the PAPP and CPA models reaches to a maximum computation time of 8s and 10s respectively.

Table 1
Computational Cost (s) of our Proposed IBGS with Existing Methods

Number of Messages	IBGS	PAPP	CPA
1	1	2	4
10	3	5	8
20	5	8	10
30	9	12	16
40	11	15	22
50	14	17	27
60	18	22	29
70	21	24	36
80	25	27	42
90	29	31	47
100	32	34	52

Under the message count 30, it is shown that the proposed IBGS requires a minimum computation cost of 9s, whereas the PAPP and CPA models reaches to a maximum computation time of 12s and 16s respectively. Under the message count 40, it is shown that the proposed IBGS requires a minimum computation cost of 11s, whereas the PAPP and CPA models reaches to a maximum computation time of 15s and 22s respectively. Under the message count 50, it is shown that the proposed IBGS requires a minimum computation cost of 14s, whereas the PAPP and CPA models reaches to a maximum computation time of

17s and 27s respectively. Under the message count 60, it is shown that the proposed IBGS requires a minimum computation cost of 18s, whereas the PAPP and CPA models reaches to a maximum computation time of 22s and 29s respectively.

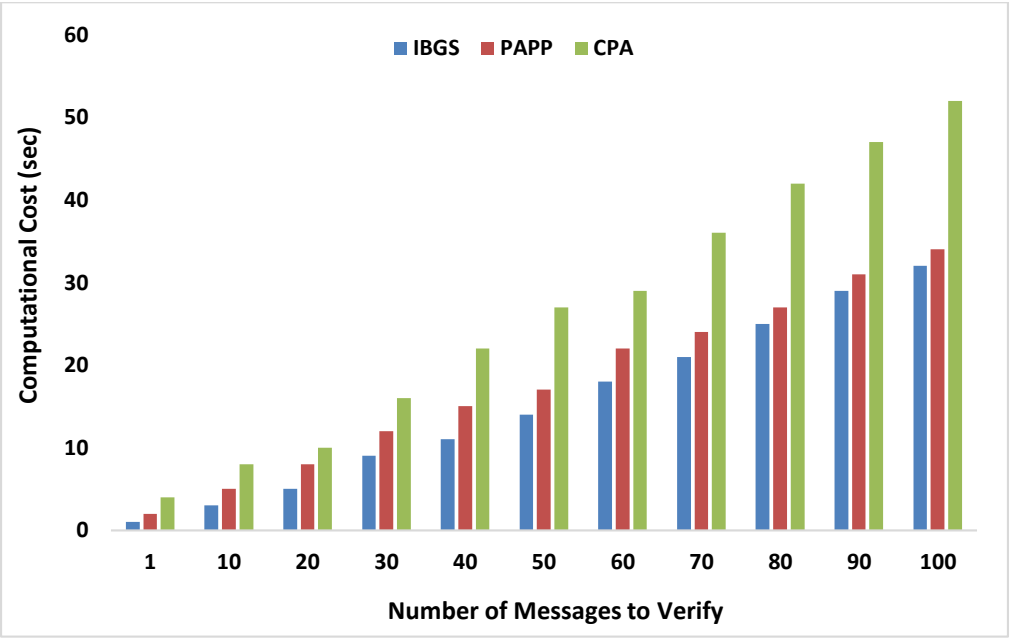

Figure 3. *Computation cost analysis*

Under the message count 70, it is shown that the proposed IBGS requires a minimum computation cost of 21s, whereas the PAPP and CPA models reaches to a maximum computation time of 24s and 36s respectively. Under the message count 80, it is shown that the proposed IBGS requires a minimum computation cost of 25s, whereas the PAPP and CPA models reaches to a maximum computation time of 27s and 42s respectively. Under the message count 90, it is shown that the proposed IBGS requires a minimum computation cost of 29s, whereas the PAPP and CPA models reaches to a maximum computation time of 31s and 47s respectively. Under the message count 100, it is shown that the proposed IBGS requires a minimum computation cost of 32s, whereas the PAPP and CPA models reaches to a maximum computation time of 34s and 52s respectively.

Table 2 and Fig. 4 show the energy consumption analysis of diverse models under varying message count. Under the existence of 1 message count, the IBGS model shows minimum energy consumption of 0.34J whereas the PAPP and CPA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of 1 message count, the IBGS model shows minimum energy consumption of 0.34J whereas the PAPP and CPA models require higher energy consumption of 0.89J and 1.43J respectively. Under the existence of 10 message count, the IBGS model shows minimum energy consumption of 0.76J whereas the PAPP and CPA models require higher energy consumption of 1.23J and 1.8J

respectively. Under the existence of 20 message count, the IBGS model shows minimum energy consumption of 0.91J whereas the PAPP and CPA models require higher energy consumption of 1.54J and 2.45J respectively.

Table 2
Energy Consumption of our Proposed IBGS with Existing Methods

Number of Messages	IBGS	PAPP	CPA
1	0.34	0.89	1.43
10	0.76	1.23	1.8
20	0.91	1.54	2.45
30	1.34	1.86	2.91
40	1.76	1.98	3.57
50	2.15	2.47	3.86
60	2.43	2.76	4.92
70	2.8	3.54	5.61
80	3.31	4.9	6.3
90	3.78	5.95	6.9
100	4.39	6.72	7.56

Under the existence of 30 message count, the IBGS model shows minimum energy consumption of 1.34J whereas the PAPP and CPA models require higher energy consumption of 1.86J and 2.91J respectively. Under the existence of 40 message count, the IBGS model shows minimum energy consumption of 1.76J whereas the PAPP and CPA models require higher energy consumption of 1.98J and 3.57J respectively. Under the existence of 50 message count, the IBGS model shows minimum energy consumption of 2.15J whereas the PAPP and CPA models require higher energy consumption of 2.47J and 3.86J respectively. Under the existence of 60 message count, the IBGS model shows minimum energy consumption of 2.43J whereas the PAPP and CPA models require higher energy consumption of 2.76J and 4.96J respectively.

Under the existence of 70 message count, the IBGS model shows minimum energy consumption of 2.8J whereas the PAPP and CPA models require higher energy consumption of 3.54J and 5.61J respectively. Under the existence of 80 message count, the IBGS model shows minimum energy consumption of 3.31J whereas the PAPP and CPA models require higher energy consumption of 4.9J and 6.3J respectively.

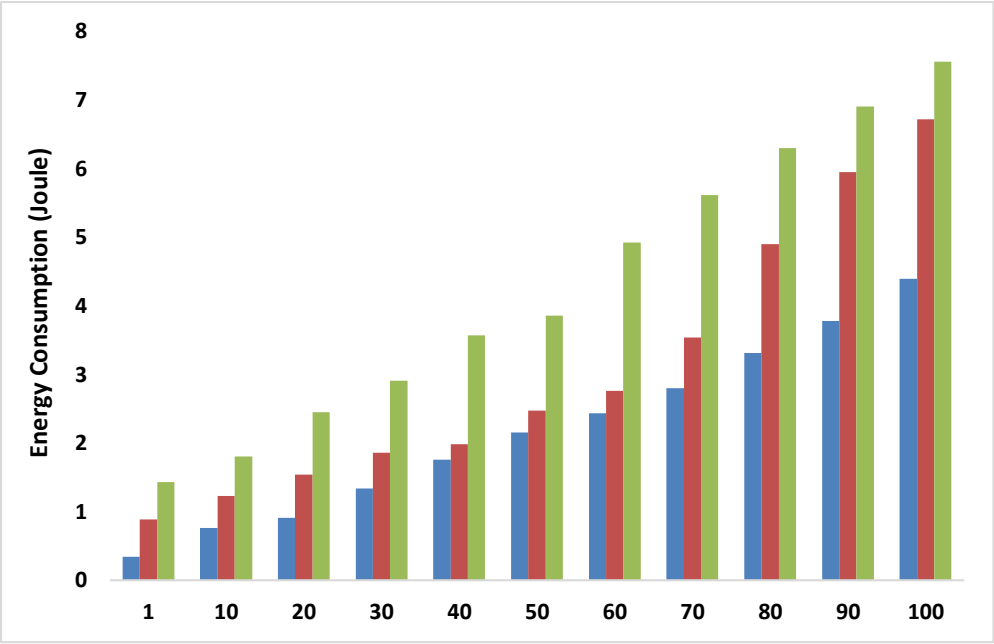

Figure 4. *Energy consumption analysis*

Under the existence of 90 message count, the IBGS model shows minimum energy consumption of 3.78J whereas the PAPP and CPA models require higher energy consumption of 5.95J and 6.9J respectively. Under the existence of 100 message count, the IBGS model shows minimum energy consumption of 4.39J whereas the PAPP and CPA models require higher energy consumption of 6.72J and 7.56J respectively.

Table 3 compares the security properties offered by the IBGS with existing models. It is shown that the IBPF model has offered maximum security properties over the compared methods except multi-user sharing.

Table 3
Comparison of the security properties of the Proposed IBGS with Existing Methods

Property	**IBGS**	**PAPP**	**CPA**
Public verifiability	1	1	1
Multi-user sharing	1	1	0
Revocability	1	1	N/A
Forward security	1	1	1
Privacy protection	1	1	0
Batch authentication	1	1	1

Proven security	1	1	1
Key replacement resistant	1	1	0
Unforgeability	1	0	0
Unlinkability	1	0	0
Exculpability	1	0	0
Traceability	1	0	0

Conclusion

WBSN is constrained with a problem of security level and privacy for given data. In this paper, a new authentication using IBGS protocol has been proposed to provide security to the WBSN. The proposed method employs identity-based group signature algorithm between biosensors and GM. An extensive set of experiments were carried out and the results are examined interms of computation cost and energy consumption under varying number of messages. Under the applied set of 100 messages, the proposed IBGS model achieves a minimum computation cost of 32s with least energy consumption of 4.39J.

Acknowledgments

We are grateful to two anonymous reviewers for their valuable comments on the earlier version of this paper.

References

Almuhaideb, A. M., & Alqudaihi, K. S. (2020). A Lightweight and Secure Anonymity Preserving Protocol for WBAN. *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.3025733

Arfaoui, A., Kribeche, A., & Senouci, S. M. (2019). Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. *Computer Networks*. https://doi.org/10.1016/j.comnet.2019.04.031

Ding, Y., Xu, H., Zhao, M., Liang, H., & Wang, Y. (2021). Group authentication and key distribution for sensors in wireless body area network. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/15501477211044338

Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. (2008). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*. https://doi.org/10.1137/060651380

Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks*. https://doi.org/10.1016/j.comnet.2020.107333

Jegadeesan, S., Azees, M., Ramesh Babu, N., Subramaniam, U., & Almakhles, J. D. (2020). EPAW: Efficient Privacy Preserving Anonymous Mutual

Authentication Scheme for Wireless Body Area Networks (WBANs). *IEEE Access*. https://doi.org/10.1109/ACCESS.2020.2977968

Jiang, Q., Ma, J., Ma, Z., & Li, G. (2013). A privacy enhanced authentication scheme for telecare medical information systems. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-012-9897-0

Kadel, R., Islam, N., Ahmed, K., & Halder, S. J. (2018). Opportunities and Challenges for Error Correction Scheme for Wireless Body Area Network—A Survey. *Journal of Sensor and Actuator Networks*. https://doi.org/10.3390/jsan8010001

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

Lara, E., Aguilar, L., & Garcia, J. A. (2021). Lightweight Authentication Protocol Using Self-Certified Public Keys for Wireless Body Area Networks in Health-Care Applications. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3084135

Latha, R., & Vetrivelan, P. (2020). Wireless body area network (WBAN)-based telemedicine for emergency care. *Sensors (Switzerland)*. https://doi.org/10.3390/s20072153

Liu, J., Zhang, Z., Sun, R., & Kwak, K. S. (2012). An efficient certificateless remote anonymous authentication scheme for wireless body area networks. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC.2012.6363786

Miao, F., Bao, S. Di, & Li, Y. (2010). A modified fuzzy vault scheme for biometrics-based body sensor networks security. *GLOBECOM - IEEE Global Telecommunications Conference*. https://doi.org/10.1109/GLOCOM.2010.5683998

Narwal, B., & Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. In *Journal of Systems Architecture*. https://doi.org/10.1016/j.sysarc.2020.101883

Ren, Y., Leng, Y., Zhu, F., Wang, J., & Kim, H. J. (2019). Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors (Switzerland)*. https://doi.org/10.3390/s19102395

Shamir, A. (1985). Identity-Based Cryptosystems and Signature Schemes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/3-540-39568-7_5

Sharma, R. (2020). An Intelligent Health Monitoring System based on Secure Distributed Routing in Wireless Body Area Networks. *International Journal of Advanced Trends in Computer Science and Engineering*. https://doi.org/10.30534/ijatcse/2020/138942020

Tan, H., & Chung, I. (2019). Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor. *IEEE Access*. https://doi.org/10.1109/ACCESS.2019.2948207

Ullah, I., Alomari, A., Amin, N. U., Khan, M. A., & Khaak, H. (2019). An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things. *Electronics (Switzerland)*. https://doi.org/10.3390/electronics8101171

Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S. (2008). EKG-based

key agreement in body sensor networks. *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFOCOM.2008.4544608

Vyas, A., & Pal, S. (2019). Preventing security and privacy attacks in WBANs. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. https://doi.org/10.1007/978-3-030-22277-2_8

You, L., Chen, Y., Yan, B., & Zhan, M. (2018). A novel location-based encryption model using fuzzy vault scheme. *Soft Computing*. https://doi.org/10.1007/s00500-017-2583-x

Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-cryptography and authentication in body area networks. *IEEE Transactions on Information Technology in Biomedicine*. https://doi.org/10.1109/TITB.2012.2206115

Zia, Y., Bashir, F., & Qureshi, K. N. (2020). Dynamic superframe adaptation using group-based media access control for handling traffic heterogeneity in wireless body area networks. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/1550147720949140