Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5986469, 14 pages
https://doi.org/10.1155/2021/5986469

Research Article

Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption

Fazal Noor, Turki A. Kordy, Ahmad B. Alkhodre, Oussama Benrhouma, Adnan Nadeem, and Ali Alzahrani

Department of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia

Correspondence should be addressed to Fazal Noor; mfnoor@gmail.com

Received 19 August 2021; Revised 7 September 2021; Accepted 9 September 2021; Published 7 October 2021

Academic Editor: Mohammed H. Alsharif

In the last few years, the wireless body area network (WBAN) has emerged as an appealing and viable option in the e-health application domain. WBAN technology is primarily used to offer continuous screening of health data to patients, independent of their location, time, or activity. A WBAN, on the other hand, is vulnerable to different cyberattacks due to the openness of the wireless environment and the privacy of people's physiological data. A highly efficient and secure cryptographic scheme that can fulfill the needs of resource-constrained WBAN sensors and devices is considered necessary. First, we take a look at the most up-to-date security solutions for WBANs. Then, we go through some of the underlying concerns and challenges with WBAN security. We propose a new framework called secure channel free certificateless signcryption scheme for WBANs based on a hyperelliptic curve that can meet security requirements such as confidentiality, anonymity, integrity, resistance against unauthorized users, unforgeability, public verifiability, forward secrecy, and antireplay attack, all of which can be achieved with low computation and communication costs. The computation cost of the proposed scheme is 3.36 ms, which is much better than its counterpart schemes.

1. Introduction

A Wireless Body Area Network (WBAN) is a revolutionary innovation that can deliver real-time preventative or proactive healthcare services at a lower cost [1]. Many low-power, intelligent, and tiny biomedical sensors are attached to, implanted in, or implanted around the human body in a WBAN without interfering with the individual's usual activities. Sensors continuously measure specific biological functions, such as temperature, blood pressure, heart rate, ElectroCardioGram (ECG), respiration, and others regardless of their current location or activity [2]. The physiological information collected is then transmitted over the wireless links to a remote processing unit without the need for complex and wired medical equipment. The ongoing miniaturization of sensors, actuators, and processors coupled with ubiquitous wireless connectivity has contributed to the emergence of WBANs. At the same time, advances in smartphones technology have also enhanced the mobility feature of WBAN technology. Today, WBAN can be connected through the Internet and other existing short-range wireless technologies (ZigBee, Bluetooth, Wi-Fi, and so on) and cellular networks. Wi-Fi may be considered the most favored options for wearable sensor nodes due to its low-cost and high-data-rate features [3].

As shown in Figure 1, the authors suggested a general communication architecture for a WBAN-based e-healthcare system [4]. A body control unit (BCU) and numerous wearable sensor/actuator nodes are included in the proposed design (e.g., a smartphone). Sensor nodes detect biological processes such as pulse, body temperature, blood pressure, glucose level, and electrocardiogram (ECG). According to the messages gathered from the sensors, actuators engage with a BCU (i.e., an insulin pump). The BCU collects biological data and sends it, together with the patient's profile, to a local/-remote medical server through networks. Medical staff offers medical treatments in a timely manner after obtaining and analyzing patient-related data. The BCU functions as a center node in a star topology in general. Additionally, sensor nodes

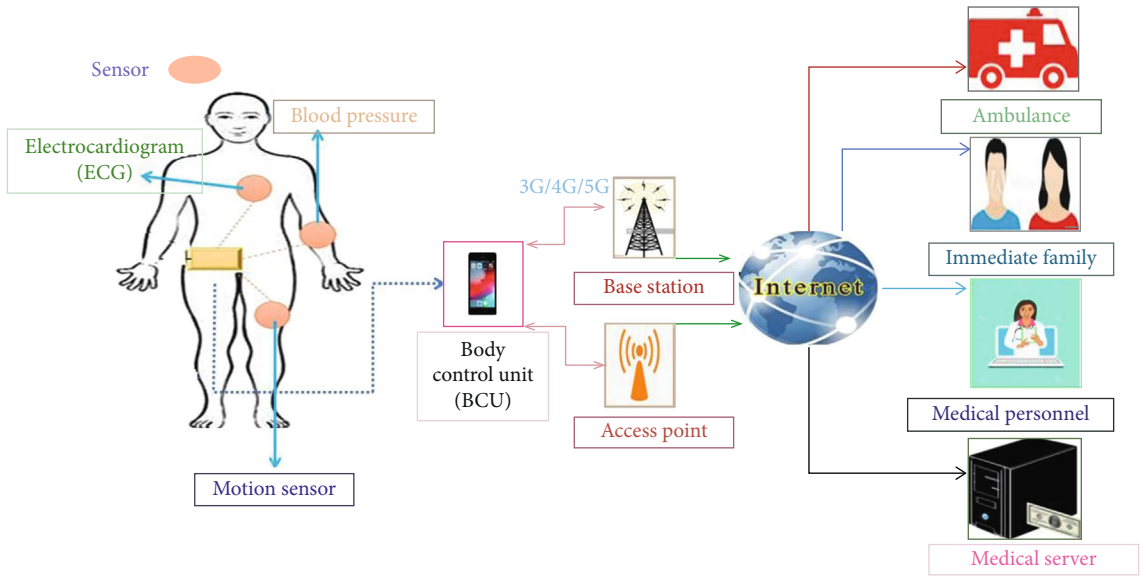

Figure 1: General architecture of a typical WBAN-based healthcare monitoring system [4].

upload data to a medical server or provide data directly to medical staff via the BCU. The medical personnel then issues the relevant instructions to the sensors via the BCU.

In a WBAN system, both patient-related information and medical messages are equally significant. WBAN, on the other hand, is vulnerable to a variety of cyberattacks owing to the open nature of wireless networks. As a result, to enable a safe WBAN system, an effective security architecture is necessary. Confidentiality and authentication are two key security problems in WBANs that must be addressed. Encryption and digital signatures, in general, are the answers to confidentiality and authenticity. The sign-then-encrypt technique is often employed when both procedures are required at the same time. Low-end WBAN sensor devices, on the other hand, have stringent constraints (such as limited on-board energy and processing resources) that prevent complicated cryptographic procedures. "Signcryption" [5] might be used to address these limitations. It is a public-key cryptosystem that performs both digital signature and encryption functions in a single logic step. It is far more efficient and cost-effective than the combination of encryption and digital signatures. Furthermore, it is considerably more suited for resource-constrained situations such as WBAN due to its reduced costs compared to techniques using signature followed by encryption.

As a result, a lightweight signcryption scheme that can fulfill the criteria of WBAN devices is required. Therefore, we offer a certificateless signcryption scheme in this paper. The scheme is based on the concept of a hyperelliptic curve and does not require a secure channel. The new scheme meets all of the previously specified security requirements while incurring low computation and communication costs, making it particularly appropriate for resource-constrained WBAN devices.

1.1. Signcryption for WBAN. Wireless body area network has received a lot of attention in the last decade especially as various technologies improve and devices keep getting smaller, more powerful, and cheaper. In a WBAN, different sensors are implanted in the human body for sensing and collecting data about different types of physiological information which are then sent to the application providers for further analysis and actions. As we have mentioned previously, communication takes place in the WBAN system while using an insecure network, i.e., the Internet, which requires two main security requirements, namely, authentication and confidentiality. Here, signcryption is the most suitable option because it combines both authentication and confidentiality in a single step, and it also requires low computational power making it suitable for resource-constrained devices such as sensors.

Figure 2 shows the generic signcryption model for WBAN which uses four entities, i.e., sensors, controller, trusted authority, and application providers. Normally, the trusted authority is a third party, which is responsible for providing the system parameters such as keys and certificates for different public-key cryptographic techniques. Sensor nodes are implanted into a person's body for sensing and collecting physiological data and then sending this data to the controller. Likewise, the controller applies the signcryption scheme to the data and transmits it to some application provider. Once the application provider receives the signcryption query, it verifies the authenticity of the sender. If the verification is successful, the application provider performs the decryption process and encrypts the requested data using some secret key (which is only known to the controller and the application provider) and sends it to the application provider. However, for access control, the same process can be repeated on the application provider side as shown in Figure 3. Here, the application provider generates the signcryption of the access control query by combining signature with encryption while using a single key pair in a single algorithm and transmits it to the controller. Once the controller receives the signcryption query, it verifies the

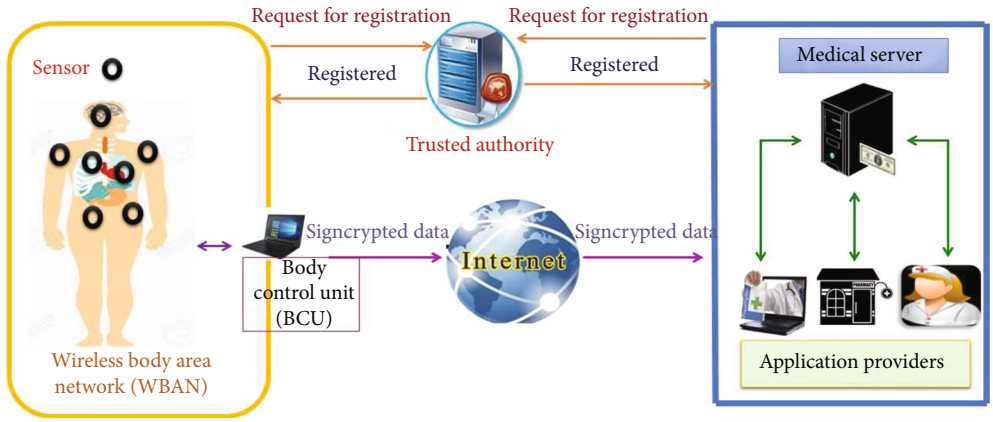

Figure 2: Signcryption performed by the controller.

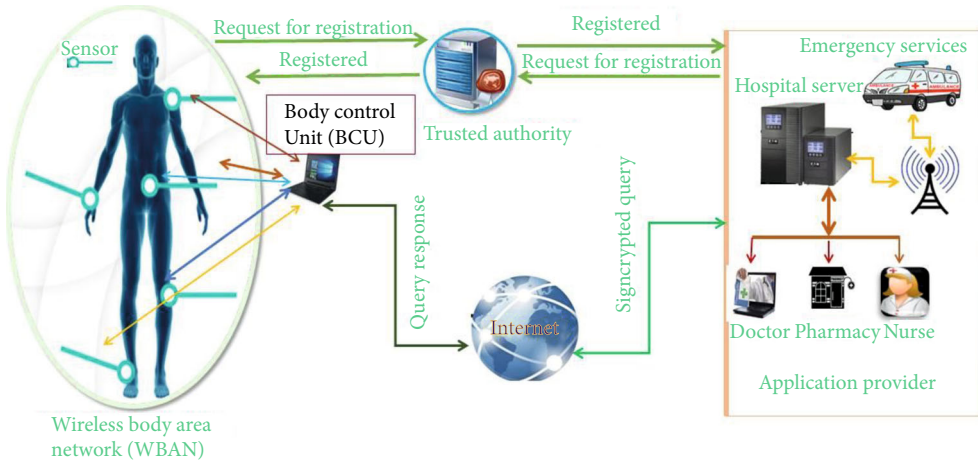

Figure 3: Signcryption performed by the application provider.

authenticity of the sender. If the verification is successful, the controller performs the decryption process and encrypts the requested data using some secret key (which is only known to the controller and the application provider) and sends it to the application provider.

1.2. Security Requirements for WBAN with Signcryption. In a WBAN, the communication process normally takes place through an open network. This means that the attacker can have unauthorized access to reveal the content of encrypted data, modify the original message, generate the forged signature, and so on. The basic security requirements for signcryption used in WBAN include (1) confidentiality: the attacker can compromise the confidentiality of the patient's sensitive data, if he/she gets access to the encryption or decryption keys. (2) Integrity: the attacker can modify the content of the original message only with the help of encryption or decryption keys. (3) Unauthorized access: the attacker can easily generate the authorized data access request if he/she has a valid digital signature. If the attacker cannot generate a valid then it is called an unauthorized access. (4) Unforgeability: the attacker can generate a forged signature as generated by the authorized user (I think that is what you mean here otherwise we mean the authorized user also generates a forged signature), if he/she gets access to the private key used for generating the digital signature. If the attacker fails to get access to this private key, then, it is called unforgeability. (5) Anonymity: the attacker can pretend to be the authorized user, if he/she can get the identity of the user from ciphertext. The inability of the attacker to access the users' identities is called anonymity. (6) Forward secrecy: the attacker cannot get access to the encryption/decryption keys, even, if he/she got access to the sender's private key. (7) Public verifiability: the attacker sends the false signcryption text instead of the authorized sender, and if it causes discrepancies between the sender and the receiver, then, the judge/third party can remove this dispute, which is called public verifiability. (8) Antireplay attack: the attacker cannot replay the existing messages if the sender and receiver use nonce and timestamp techniques for the freshness of messages.

1.3. Contributions of This Work. We summarize the main contributions of this work as follows:

(i) We present a comprehensive review of recently proposed signcryption schemes to improve security in the WBAN environment. To the best of our

knowledge, this is the first survey that focuses on signcryption for WBAN security

(ii) We identify the strengths and weaknesses of the previously proposed signcryption schemes for WBAN in terms of security requirements and their cost-efficiency

(iii) Based on the strengths and weaknesses identified for the past related works on signcryption schemes for WBAN, we propose a novel security architecture for the WBAN environment using secure channel free certificateless signcryption based on hyperelliptic curve. The new scheme satisfies all the security requirements identified earlier, and it incurs low computation and communication costs which make it particularly suitable for resource-constrained WBAN devices

The rest of the article is set out as follows. The related work is presented in Section 2, which also includes classification, security deficiencies, and cost requirements. The proposed scheme is provided in Section 3. In Section 4, we describe the construction of the proposed scheme. Section 5, on the other hand, provides the proposed scheme's security discussions. In addition, we discuss performance analysis in Section 6. The conclusion is presented in Section 7.

2. Related Works on Signcryption for WBAN

In this section, we review and analyze existing signcryption schemes for WBAN with respect to their research goals, security requirements, and computation and communication overheads. Amin et al. [6] proposed a hybrid key establishment technique for body area network (BANs) based on symmetric cryptography with signcryption. They make a cluster head selection with session key creation in one logical step and claimed reduced computation cost as well as communication overhead. They also claimed that their approach supports various security properties such as confidentiality, antireplay attack, integrity, and authentication. However, the scheme consumes high energy and increased bandwidth due to the elliptic curve cryptosystem (ECC). It suffers from certificate renewal and revocation problems. It does not support forward secrecy, public verifiability, mutual authentication, and nonrepudiation. Wang and Liu [7] proposed a ring signcryption method utilizing attribute-based cryptosystem for WBANs. The security hardiness and efficiency of this scheme are based on the computational Diffie-Hellman (CDH) assumption from bilinear pairing. Their method supports various security requirements, i.e., authenticity, nonrepudiation, and confidentiality. However, this method does not address the key escrow problem because the Hospital Authority (HA) performs the role of the Private Key Generation (PKG) center that generates the private keys for both the controller and data users (such as doctor, researchers, and emergency). Therefore, the HA can easily use the user's private key to forge the signature. Moreover, the scheme's efficiency is based on bilinear pairing which consumes high energy and uses high bandwidth. It does not support forward secrecy, public verifiability, mutual authentication, and antireplay attack.

Jothi and Srinivasan [8] proposed another method which combines the concept of attribute-based cryptosystem with ring signcryption. In this system, the sensors which are planted into the body use ant colony optimization with the concept of fuzzy ontology. They claimed better performance as compared to existing elliptic curve-based methods with respect to efficiency and feasibility. Further, their approach also supports various security services such as authentication, unforgeability, confidentiality, public verifiability, integrity, nonrepudiation, and forward secrecy. Unfortunately, this method suffers from two major weaknesses, i.e., the key escrow problem and private key distribution among users which needs a secure channel. Li and Hong [9] proposed a new signcryption method that uses the concept of certificateless cryptosystem (CC) with bilinear pairing. Further, they implemented this new method in WBANs and showed that it incurs low computation overhead and energy as compared to existing schemes for WBANs. Their approach supports authentication, confidentiality, nonrepudiation, public verifiability, integrity, and cipher-text authenticity. But this scheme suffers from a partial private key distribution among users which needs a secure channel. Additionally, since this method is based on bilinear pairing, it consumes high energy and increased network bandwidth. Iqbal et al. [10] proposed a new signcryption method with the public verifiability security requirement. They performed the cluster head selection process for this new method and claimed better efficiency due to the hyperelliptic curve, which is suitable for resource hungry environments of WBANs. Their proposed method supports security services such as confidentiality, integrity, forward secrecy, and authentication. However, the network model fails to provide a central authority and suffers from certificate renewal and revocations problems. Further, this work focuses mainly on the public verifiability security property while the authors fail to explain this property. Moreover, this scheme does not provide nonrepudiation, mutual authentication, and protection against replay attack.

Saeed et al. [11] proposed a new method for the Internet of things based on heterogeneous online/offline signcryption, in which the sensor nodes (sender) utilize the functionality of a certificateless infrastructure (CLI), and the server (receiver) utilizes the services of public key infrastructure (PKI). They proved the scheme security requirement using a random oracle model and showed that it satisfies security requirements such as authentication, nonrepudiation, integrity, and confidentiality. Furthermore, they applied the scheme in WBAN. However, due to CLI and PKI, this scheme suffers from secret key distribution, and the certificate revocation and management problem. It also suffers from high consumption of and network bandwidth because it uses bilinear pairing. Also, it does not support mutual authentication, forward secrecy, public verifiability, and protection against replay attack. Lu et al. [12] proposed a scheme for a social network-based mobile health care system that uses attribute-based signcryption. They used a four-party model to protect patients' sensitive information. The scheme provides traceability, privacy, unforgeability, and

correctness. Using encryption and digital signature in a single step, they claimed better performance efficiency. However, due to the PKG concept, this scheme suffers from private key distribution and the key escrow problem. The scheme does not support forward secrecy, public verifiability, nonrepudiation, mutual authentication, and protection against replay attack. Moreover, it has high power consumption and network bandwidth due to of the use of bilinear pairing. Li et al. [13] developed a novel method using certificateless signcryption, and then, they practically deployed this scheme for access control services in WBAN. This method supports several security requirements that include authenticity, integrity, confidentiality, nonrepudiation, and anonymity. They also compare their scheme with existing schemes and demonstrated better results in terms of energy consumption and computational cost. However, due to the CLI concept, this scheme suffers from the partial private key distribution problem and incurs high power consumption. The method does not support public verifiability, forward secrecy, and mutual authentication.

Prameela [14] proposed an improved scheme that uses certificateless signcryption with anonymous mutual authentication for access control in WBANs. They used a chaos baker map scheme with XOR operation and a one-way hash chain function for secure authentication. The experimental results obtained with the proposed scheme yielded better results compared with existing ones in terms of energy consumption, end-to-end delay, coverage time, packet delivery ratio, and throughput. The scheme supports confidentiality, mutual authentication, nonrepudiation, and integrity. Conversely, because of the use of CLI, this scheme suffers from partial private key distribution difficulties and high power consumption and network bandwidth because it uses bilinear pairing. This scheme does not support forward secrecy, public verifiability, and protection against replay attack. Omala et al. [15] proposed a keyword search technique for WBAN based on heterogeneous signcryption, in which the data owner uses the concept of CLI, while the server and receiver utilize the PKI functionality. This heterogeneous signcryption generates the mathematical structure of bilinear pairing. The scheme supports security services such as confidentiality, unforgeability, nonrepudiations, and authenticity. However, the scheme suffers and incurs high power consumption and communication costs due to bilinear pairing. It suffers from weaknesses such as it needs a secure channel for the data owner's partial private key distribution and PKI certificate management at the server and receiver side. It does not provide public verifiability, forward secrecy, and mutual authentication.

Omala et al. [16] proposed an access control technique for WBAN based on heterogeneous signcryption, in which the controller uses the concept of CLI, while application providers utilize the concept of identity-based cryptography (IBC). The scheme's cost and security efficiency are based on the mathematical structure of elliptic curve cryptography. The technique is cost-efficient and supports security services such as anonymity, confidentiality, unforgeability, nonrepudiations, and authenticity. However, the scheme also suffers from high computational and communication costs due to elliptic curve cryptosystem. It also needs a secure channel for the application provider's partial private key distribution. It also suffers from the key escrow problem at the controller side. It does not support public verifiability, forward secrecy, and mutual authentication. Gao et al. [17] proposed an elliptic curve-based technique for access control of WBAN by using a certificateless signcryption. They claimed better cost efficiency, for the technique supports security services such as confidentiality, unforgeability, nonrepudiation, and authenticity. However, the scheme also suffers from high computation and communication costs due to the elliptic curve cryptosystem. It also needs a secure channel for the partial private key distribution. The techniques do not support forward secrecy, public verifiability, and mutual authentications. Ullah et al. [18] proposed an energy-efficient access control technique for WBAN with IoT using certificate-based signcryption. The scheme's cost and security efficiency are based on the mathematical structure of hyperelliptic curve cryptography. The authors of this technique claimed better cost-efficiency. The scheme supports security services that include confidentiality, unforgeability, antireplay attack, integrity, public verifiability, and forward security. However, since the scheme requires certificate management, the scheme may not scale well when the number of devices in the network increases. The scheme does not support mutual authentication and anonymity properties. Iqbal et al. [19] proposed a new scheme for body sensor network. This scheme uses attribute-based signcryption with blockchain technology. The security and efficiency of this scheme are based on bilinear pairing. The scheme has better power consumption and low communication overheads. The scheme supports security requirements such as confidentiality and unforgeability. The scheme provides protection against antireplay and man-in-the-middle attacks. However, the scheme can be suffering from more computational and communication cost due to bilinear pairing. As with other approaches, the scheme needs a secure channel for partial private key distribution and certificate management due to CLI and PKI. The scheme does not support mutual authentication, anonymity, public verifiability, and forward secrecy. Xiong et al. [20] presented a heterogeneous signcryption method for WBANs that transitions from an identity-based cryptosystem to a public key infrastructure (PKI) with an equality test (HSCIP-ET). The technique enables the IBC system's sensors to encrypt critical data using the management center's public key in the PKI system before uploading it to the cloud server. Based on the discussions above, Table 1 summarizes the results of our review.

2.1. Classification of Signcryption Schemes for WBAN regarding Public Key Cryptography. In this section, we classified the existing signcryption schemes for WBAN such as asymmetric cryptosystems and mathematically hard problems. In Table 2, we summarize the contributed schemes on the basis of public key cryptosystems that are attribute based, PKI based, certificateless, certificate based, and heterogeneous, respectively. The schemes in [7, 8, 12, 19] realized on the concept of attribute-based signcryption, while schemes in [7, 8, 12] at the same time utilizes the concept

Table 1: Strengths and weaknesses of signcryption schemes for WBANs.

Goal(s) of research	Strengths	Weaknesses
[6]	(i) They make a cluster head selection with session key creation in one logical step (ii) Claimed for reduced computational cost as well as communication overhead (iii) Claimed for various security properties such as confidentiality, antireplay attack, integrity, and authentication	(i) Suffering from certificate renewal and revocations problems (ii) Suffered from greater consumption of computational power (iii) Suffered increased nature of bandwidth (iv) Suffer from the lack of forward secrecy, public verifiability, and nonrepudiation
[7]	(i) Claimed for better efficiency (ii) Claimed for various security requirements, i.e., authenticity, nonrepudiation, and confidentiality	(i) Failed to remove the key escrow problem (ii) Suffered from greater computational power (iii) Suffered from increased nature of bandwidth (iv) Lack of forward secrecy, public verifiability, and antireplay attack
[8]	(i) Claimed for better performance with respect to efficiency and feasibility (ii) Claimed for various security services that are authentication, unforgeability, confidentiality, public verifiability, integrity, nonrepudiation, and forward secrecy	(i) Suffering from the key escrow problem (ii) Suffering from private key distribution problem (iii) Lack of antireplay attack
[9]	(i) Claimed for minimum consumptions of computation and energy (ii) Claimed for security services such as authentication, confidentiality, nonrepudiation, public verifiability, integrity, and ciphertext authenticity	(i) Suffering from a partial private key distribution problem (ii) Undergone from larger consumption of computational power (iii) Suffering from bigger nature of bandwidth (iv) Lack of forward security property
[10]	(i) Claimed for better efficiency (ii) Claimed for confidentiality, integrity, forward secrecy, and authentication	(i) Failing to provide the role of central authority (ii) Suffering from certificate renewal and revocations problems (iii) Suffered from public verifiability security property (iv) Lacking from nonrepudiation, and antireplay attack
[11]	(i) They prove the scheme security requirement using a random oracle model (ii) Claimed for security property such as authentication, nonrepudiation, integrity, and confidentiality	(i) Suffering from secret key distribution (ii) Suffering from certificate revocation and management problem (iii) Undergo from larger consumption of computational power (iv) Suffering from the bigger nature of bandwidth (v) Lack of forward secrecy, public verifiability, and antireplay attack
[12]	(i) Claimed for a number of analysis, i.e., traceability, privacy, unforgeability, and correctness (ii) Using encryption and digital signature in a single step (iii) Claimed for better performance regarding efficiency	(i) Suffering from private key distribution and the key escrow problem. (ii) Undergo from larger consumption of computational power (iii) Suffering from bigger nature of bandwidth (iv) Lack of forward secrecy, public verifiability, nonrepudiation, and antireplay attack
[13]	(i) Claimed for a series of security requirements, i.e., authenticity, integrity, confidentiality, nonrepudiation, and anonymity (ii) Claimed for better results regarding energy consumption and computational cost	(i) Suffering from partial private key distribution problem (ii) Underwent from loftier consumption of computational power and a larger nature of bandwidth (iii) Lack of public verifiability and forward secrecy
[14]	(i) Claimed for better results compared with existing ones regarding energy consumption, end-to-end delay, coverage time, packet delivery ratio, and throughput (ii) Claimed for confidentiality, mutual authentication, non-repudiation, and integrity, authentication	(i) Undergo from partial private key distribution difficulties (ii) Suffering from snootier consumption of computational power and a larger nature of bandwidth (iii) Lack of forward secrecy, public verifiability, and antireplay attack

Table 1: Continued.

Goal(s) of research	Strengths	Weaknesses
[15]	(i) Claimed for better efficiency (computational and communication cost) (ii) Claimed for confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) Affected by needing the secure channel for the data owner partial private key distribution (iii) Suffering from certificate management at the server and receiver side (iv) Lack of public verifiability and forward secrecy
[16]	(i) Claimed for better cost-efficiency (ii) Claimed for security services that are anonymity, confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) Affected by requiring the secure channel for the application provider partial private key distribution (iii) Suffering from key escrow problem at the controller side (iv) Lack of public verifiability and forward secrecy
[17]	(i) Claimed for better cost-efficiency (ii) Claimed for security services that are confidentiality, unforgeability, nonrepudiations, and authenticity	(i) Suffering from more computational and communication cost (ii) It can be affected by requiring the secure channel for the partial private key distribution (iii) Lack of forward secrecy and public verifiability
[18]	(i) Claimed for better cost efficiency (ii) Claimed for security services that are confidentiality, unforgeability, antireplay attack, integrity, public verifiability, and forward security	(i) Affected by requiring the certificate management in a network which consists a large number of devices (ii) It can also be affected by the lack of anonymity property
[19]	(i) Claimed for better utilization of energy, computational consumptions, and with less communication overhead (ii) Claimed for the security requirements like confidentiality, unforgeability, antireplay attack, and resist for man-in-the-middle attack	(i) Suffering from more computational and communication cost (ii) Affected by needing the secure channel for partial private key distribution (iii) Suffering from certificate management (iv) Affected by the lack of public verifiability and forward secrecy security requirements

Table 2: Classification of signcryption schemes W.r.t to asymmetric cryptosystem.

Attribute-based signcryption techniques for WBAN	[7, 8, 12, 19]
Identity-based signcryption techniques for WBAN	[7, 8, 12]
PKI-based signcryption techniques for WBAN	[6, 10]
Certificateless signcryption techniques for WBAN	[9, 13, 14, 17]
Certificate-based signcryption techniques for WBAN	[18]
Heterogeneous signcryption techniques for WBAN	[11, 15, 16, 19]

Table 3: Classification on the basis of hard problems.

Bilinear pairing cryptosystem	[7, 9, 11–15, 19]
Elliptic curve cryptosystem	[16, 17]
Fuzzy-based cryptosystem	[8]
Hyperelliptic curve cryptosystem	[10, 18]

of identity-based cryptosystem, and scheme in [19] uses the heterogeneous cryptosystem method. The techniques presented in [6, 10] are realized on PKI-based cryptography. The schemes proposed in [9, 13, 14, 17] used the concept of certificateless signcryption technique. The technique used in [18] is based on certificate-based signcryption, and the schemes in [11, 15, 16, 19] are on the basis of heterogeneous signcryption techniques.

2.2. Classification of Signcryption Schemes for WBAN with respect to Cryptographic Hard Problems. In this section, we classified the existing signcryption schemes for WBAN on the basis of hard problems that are shown in Table 3. The schemes presented in [7, 9, 11–15, 19] are based on the concept of bilinear pairing, while the schemes provided in [16, 17] utilize the concept of elliptic curve cryptography. The scheme proposed in [8] used the Fuzzy-based cryptosystem, while the schemes contributed in [10, 18] use the notion of hyperelliptic curve cryptography.

2.3. Security Deficiencies in Signcryption Techniques for WBAN. In this phase, on the basis of our analysis that is presented in Table 1, where each technique has its own pros and cons and it is difficult to differentiate the superiority of each technique on others. Further, each of those has its own security limitations on the basis of security properties such as confidentiality, unforgeability, integrity, anonymity, nonrepudiations, forward secrecy, antireplay attack, public verifiability, and preventing from unauthorized access, respectively. The scheme presented in [6] has been suffering from the lack of forward secrecy, public verifiability, and nonrepudiation. The scheme in [7] has the diffenciencies of forward secrecy, public verifiability, and antireplay attack. The scheme in [8] can be affected by the lack of antireplay attack. The technique used in [9] has the limitations of not providing the forward security. The method used in [10] is suffering from the absence of nonrepudiation and antireplay attack. The mechanism used in [11] has been suffering from the absence of forward secrecy, public verifiability, and antireplay attack. The presented scheme in [12] does not provide the security properties such as forward secrecy, public verifiability, nonrepudiation, mutual authentication, and antireplay attack. The mechanism used in [13] can be suffered from the absence of public verifiability and forward secrecy. Due to the absence of forward secrecy, public verifiability, and antireplay attack, the scheme used in [14] can affect. During communication, the schemes used in [15–17, 19] can be affected by the absence of public verifiability, forward secrecy, and mutual authentication security properties. The scheme used in [18] is affected by the absence of mutual authentication property.

2.4. Cost Requirements of Signcryption Technique for WBAN. We divide the cost requirements into two subcategories, i.e., computational cost and communication overhead. First of all, we investigate the computational cost of the signcryption mechanisms for WBAN. The computational cost is normally calculated by using some major operations. In signcryption schemes for WBAN, discussed in Table 1, the well-known technique, which is used for the cost efficiency, is bilinear pairing, elliptic curve, and the hyperelliptic curve. According to the experimental results, which is discussed in [21], regarding the major operations, the single pairing operation takes 14.90 milliseconds (ms), single exponential operation takes 1.25 ms, single elliptic scalar multiplication consumes 0.97 ms, and according to [22–26], single hyperelliptic curve needs 0.48 ms, respectively. Thus, from Table 3, we can easily choose the best scheme on the basis of computational cost. Likewise, the schemes [7, 9, 11–15, 19] are based on bilinear pairing, which can be required 14.90 ms for single pairing operations; and the mechanisms used in [16, 17] are based on elliptic curve, which requires 0.97 ms, while the schemes of [10, 18] requiring 0.48 ms due to hyperelliptic curve. Based on the aforementioned discussion, we can conclude that the hyperelliptic curve is the most favorable option while designing signcryption scheme for WBAN. Further, for communication overhead, the assumption observed from [18] bilinear pairing, elliptic curve, and the hyperelliptic uses 1024 bits, 160 bits, and 80 bits key sizes, respectively. We can conclude that the hyperelliptic curve will be the best option in terms of communication overhead for such types of WBAN, which have a low bandwidth capacity.

3. Proposed Secured Channel Free Certificateless Signcryption for WBAN

From Table 1, it is very clear that all the existing signcryption schemes for WBAN are suffering from certain flaws such as key escrow, certificate management, and secure channel needs. Further, these schemes are also suffering from the lack of one or more security requirements, and some of the schemes are suffering from high computational communication cost. To remove the key escrow, certificate management, and the need of secure channel problem and to provide all the claimed security requirements as discussed in related work section (3) with low computational and communication cost, we proposed a new framework called secured channel free certificateless signcryption for WBAN. For this new scheme, we adopt the secured channel free concept from [27], certificateless signcryption from [13], and the security and efficiency of the particular scheme based on a hyperelliptic curve [18]. Here, the secure channel free means that this scheme does not require any secure channel for the distributions of partial private key among the participated users. In Figure 4, we show the flow of secured channel-free certificateless signcryption for WBAN. This new ecosystem contains four entities, i.e., the smart sensor nodes, controller, application provider, and key generation center (KGC), respectively. The following substeps can be more helpful while clarifying the working flow of this new ecosystem.

3.1. Key Generation Center. The key generation center generates the public parameter set, master private, and public key. Then, KGC published publicly the public parameter set and master public key. After this, upon receiving the identity from application provider and controller, KGC generates the pseudorandom partial private key (PRPPK) for each user and transmits it to each user through open network.

3.2. Application Providers. Application providers are the run time service providers (SP), i.e., doctors, nurses, smart pharmacy, and emergency services, which monitor the patient's condition. For the monitoring purpose, the SP can request for patient data, while for privacy and authorization, SP perform signcryption on access control query and then transmit it to the controller. For the signcryption process, the application providers first send his identity to KGC for accessing of PRPPK. The KGC then produces PRPPK and sends it to the application providers through open network. The application providers then extract the partial private key from the PRPPK and generate the full public and private key. Further, the application providers generate secret session key for the encryption of patient data. At the end, the application providers produce the signcryption on patient data by using all the aforementioned parameters and transmit it to the controller by using internet.

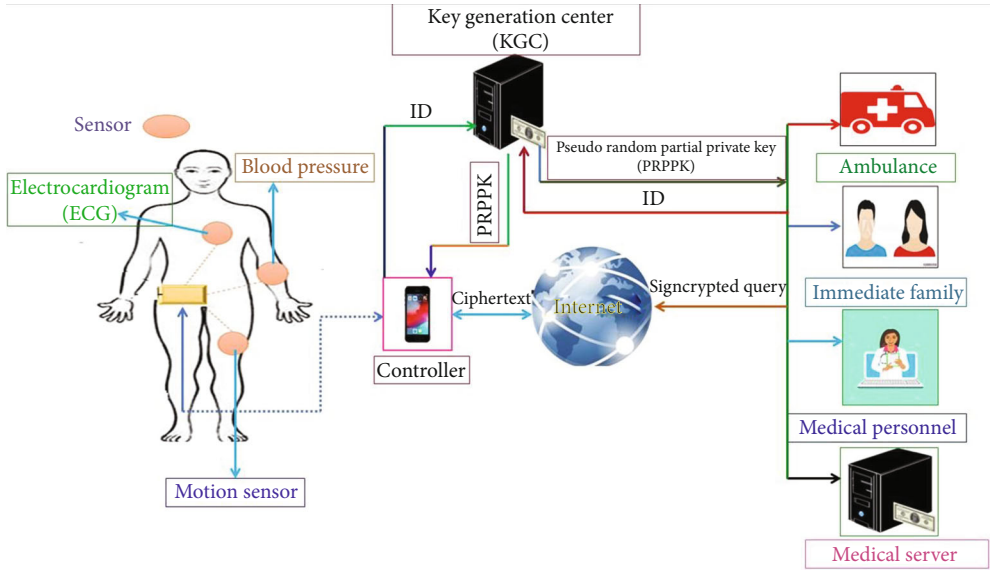

Figure 4: Secure channel free certificateless signcryption for WBAN.

Table 4: Symbols used in the proposed scheme.

S. no	Symbol	Description
1	KGC	Key generation center
2	$\mathscr{L}$	Selected input security parameter from hyperelliptic curve
3	$\mathcal{Q}$	It is a prime number with size $\mathcal{Q} \cong 2^{80}$
4	$F_{\mathcal{Q}}$	A finite field of its order is $\mathcal{Q}$
5	$\mathcal{H}\mathcal{E}^{\circ}C$	A hyperelliptic curve on $F_{\mathcal{Q}}$
6	D	A divisor from $F_{\mathcal{Q}}$
7	$\square$	Master private key of KGC
8	$W = \square.D$	Master public key of KGC
9	$\mathcal{H}_I$, $\mathcal{H}_{II}$, $\mathcal{H}_{III}$, and $\mathcal{H}_{IV}$	Four irreversible hash functions
10	Φ	Public parameter set
11	ID_s, ID_r	Identity of sender and receiver
12	U_s, U_r	Secret value of sender and receiver
13	$\mathcal{O}_s$, $\mathcal{O}_r$	Private key of sender and receiver
14	Y_s, Y_r	Public key of sender and receiver
15	G_r, R_r	Partial private key pair of receiver
16	G_s, R_s	Partial private key pair of sender
17	E_σ	Represents encryption through a secret key σ
18	D_σ	Represents decryption through a secret key σ
19	M	Eptimized plaintext
20	N_s	A fresh nonce which is used to safeguards replay attack
21	$\|\|$	Used for concatinations
22	Z^*_q	A group from hyper elliptic curve of order $\mathcal{Q}$

3.3. Smart Sensor Nodes. These are the small sensors, which are generally implanted within the patient's body for monitoring data regarding the nature of different diseases and then hand over to the controller on demand basis.

3.4. Controller. The controller is a smart device that can be a laptop, mobile phone, and personal digital assistant, etc., which is normally used to receive data from sensors and also the access control signcrypted query from application

Table 5: Computational cost comparisons on the basis of major operations.

Schemes	Signcryption	Unsigncryption	Total
Saeed et al. [11]	5 PBM + 1 E	1 PBM + 2 P	6 PBM + 1 E + 2 P
Lu et al. [12]	11 E + 2 PBM + 1P	6P + 1E	12 E + 2 PBM + 7P
Li et al. [13]	1 E + 4 PBM	2P + 1 E + 2 PBM	2P + 2 E + 6 PBM
Prameela [14]	2 E	3E	5E
Omala et al. [15]	3 PBM	3P + 1PBM	3P + 4PBM
Omala et al. [16]	3 ESM	3 ESM	6 ESM
Gao et al. [17]	3 ESM	4 ESM	7 ESM
Ullah et al. [18]	4 HEM	4 HEM	8 HEM
Iqbal et al. [19]	5 PBM + 1E	1 PBM + 2P	6 PBM + 1E + 2P
Proposed	4 HEM	3 HEM	7 HEM

Table 6: Comparative analysis in terms of ms.

Schemes	Signcryption	Unsigncryption	Total
Saeed et al. [11]	23.52	34.11	57.63
Lu et al. [12]	45.19	91.37	136.56
Li et al. [13]	19.21	40.39	59.6
Prameela [14]	3.94	5.91	9.85
Omala et al. [15]	12.93	49.01	61.94
Omala et al. [16]	2.91	2.91	5.82
Gao et al. [17]	2.91	3.88	6.79
Ullah et al. [18]	1.92	1.92	3.84
Iqbal et al. [19]	23.52	34.11	57.63
Proposed	1.92	1.44	3.36

Table 7: Computation cost improvement in percentage.

Schemes	Computation cost of (A)	Computation cost of (B)	Cost reduction (C)
Saeed et al. [11]	57.63	3.36	94.16
Lu et al. [12]	136.56	3.36	97.53
Li et al. [13]	59.6	3.36	94.36
Prameela [14]	9.85	3.36	65.88
Omala et al. [15]	61.94	3.36	94.57
Omala et al. [16]	5.82	3.36	42.26
Gao et al. [17]	6.79	3.36	50.51
Ullah et al. [18]	3.84	3.36	12.5
Iqbal et al. [19]	57.63	3.36	94.16

Percentage change: $C = (A - B/A) * 100$.

providers. In our case, on receipting the signcrypted query from application providers, the controller then performs the unsigncryption process on it and then verifies and decrypts it. For this process, the controller first sends his identity to the KGC for accessing of PRPPK. The KGC then produces PRPPK and sends it to the controller through open network. The controller extracts the partial private key from the PRPPK and generates the full public and private key. Further, the application providers recover the secret session key for the decryption of access control query. At the end, the controller performs the unsigncryption process upon the signcrypted access control query, if the verification process is done, then, controller decrypts the query and encrypts the requested patient data through secret key and send back to the application providers.

Note: this scheme provides the security services of confidentiality and integrity because it encrypts the patient data through secret key, which is only known to the application providers and the controller. It also resists against the unauthorized user access because if the attacker wants to access the data then he/she must generate a forged signature for it. Therefore, the controller does not generate the forged signature because for this purpose he/she must have the private key of application providers. Even if the private key of application providers/controller is known to the attacker, still this scheme has resisted against to break the confidentiality, because for encryption and decryption purpose, it uses the secret key, which means the new scheme provides the forward secrecy property. Further, this scheme hides the identity of the controller and application providers; it means that it cannot send the identity of the controller and application provider openly with ciphertext, which provides the anonymity property. It also used a technique for the discrepancy resolving among the application providers and controller, if happen, which is called public verifiability security requirement. The new scheme generates a fresh nonce, encrypts it, and sends along with every access control query for the resistance of replay attack. What is more in this new scheme, it is based on a hyperelliptic curve, which is the generalized form elliptic curve which provides the same level of security with 80 bits key in contrast to 160 bits key of elliptic curves. Thus, due to the hyperelliptic curve, our new scheme has the capacity of low computational cost and decrease communication overhead. If we look into the literature section of this paper, only two signcryption schemes [10, 18] for WBAN on the basis of the hyperelliptic curve are available, but the schemes in [10] have the limitations of failing to provide the role of central authority, suffering from certificate renewal and revocations problems, lacking of public verifiability, nonrepudiation, and antireplay attack. The scheme used in [18] can be affected by requiring the certificate

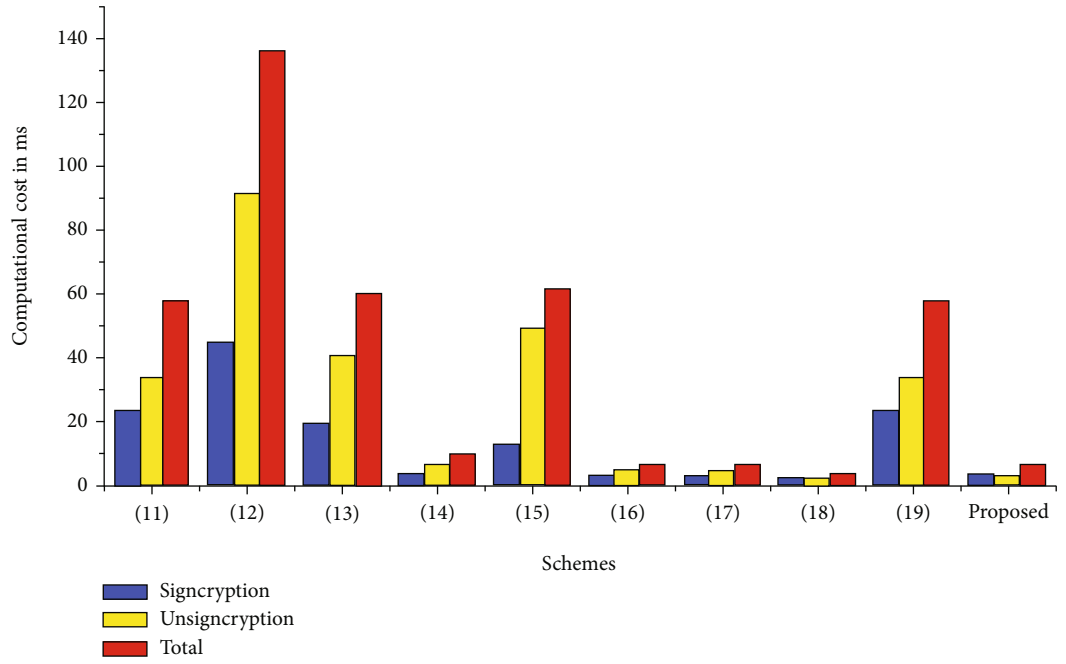

Figure 5: Computational cost.

Table 8: Communication cost improvement in percentage.

Schemes	Computation cost of (A)	Computation cost of (B)	Cost reduction (C)
Saeed et al. [11]	3072	1184	61.45
Lu et al. [12]	4096	1184	71.09
Li et al. [13]	4096	1184	71.09
Prameela [14]	3072	1184	61.45
Omala et al. [15]	3072	1184	61.45
Omala et al. [16]	1504	1184	21.27
Gao et al. [17]	1984	1184	40.32
Ullah et al. [18]	1184	1184	0
Iqbal et al. [19]	3072	1184	61.45

Percentage change: $C = (A - B/A) * 100$.

management in a network which consists a large number of devices, and it can also be affected by the lack of anonymity property. So, our scheme also removes all these disadvantages which are discussed above.

4. Constructions of the Proposed Scheme

It includes the substeps that are setup, actor key setting, actor partial private key setting, actor private key generation, actor public key setting, CLSC-signcrypt, and CL-unsigncrypt, respectively.

Here, first of all, we provide the symbols used in the proposed scheme in Table 4 and the whole process of the construction towards a new scheme in the following steps.

4.1. Setup. The setup phase is executed by KGC to make a system parameter set and master key. The following are the steps which show how to compose a system parameter set and master key.

(1) Given a security parameter $\mathscr{L}$, the KGC chooses a prime number $\mathscr{Q}$ and makes a finite field $F_{\mathscr{Q}}$, where its order is $\mathscr{Q}$ such that $\mathscr{Q} \cong 2^{80}$. Select a hyperelliptic curve $(\mathscr{H}\mathscr{E}^{\circ}C)$ on $F_{\mathscr{Q}}$ and pick a divisor D from $F_{\mathscr{Q}}$

(2) Uniformly select $\square \in Z^*_{\mathscr{q}}$ as the master private key and calculate its public key as $W = .D$, further, it saves $\square$ at his memory and enables W publicly to the network

(3) It also choice the hash functions that are $\mathscr{H}_{\mathrm{I}}$, $\mathscr{H}_{\mathrm{II}}$, $\mathscr{H}_{\mathrm{III}}$, and $\mathscr{H}_{\mathrm{IV}}$

(4) Produce parameter set $\wp = \{\mathscr{H}_{\mathrm{I}}, \mathscr{H}_{\mathrm{II}}, \mathscr{H}_{\mathrm{III}}, \mathscr{H}_{\mathrm{IV}}, \mathscr{Q}, \mathscr{H}\mathscr{E}^{\circ}C, F_{\mathscr{Q}}, W, D\}$ and publish it to the network

4.2. Actor Key Setting. An actor with ID_a uniformly chooses $U_a \in Z^*_{\mathscr{q}}$ as his/her secret value, calculates $V_a = U_a.D$, and sends (V_a, ID_a) to KGC.

4.3. Actor Partial Private Key Setting. After receipting (V_a, ID_a), the KGC then uniformly chooses $P_a \in Z^*_{\mathscr{q}}$, calculates $R_a = P_a.D$, calculates the pseudopartial private key $G_a = P_a + \square\mathscr{H}_I(V_a, R_a, ID_a) + \mathscr{H}_I(V_a.\square, ID_a)$, and sends (G_a, R_a) to an actor with ID_a utilizing an open network.

4.4. Actor Private Key Generation. After receipting (G_a, R_a), an actor with ID_a first verifies it by utilizing the equation $G_a.D = R_a + \mathscr{H}_I(V_a, R_a, ID_a).W + \mathscr{H}_I(U_a.W, ID_a).D$, if it is held, then it extracts the partial private key as $T_a = G_a - \mathscr{H}_I(U_a.W, \mathrm{ID}_a)$ and produces the private key as $\mathscr{O}_a = U_a + T_a$.

4.5. Actor Public Key Setting. An actor with ID_a computes his/her public key as $Y_a = V_a + R_a$ and sends it to the KGC through open network.

Table 9: Comparative analysis in terms of bits.

Schemes	Ciphertext size
Saeed et al. [11]	$\|m\| + 2\|G\|$
Lu et al. [12]	$\|m\| + 8\|G\|$
Li et al. [13]	$\|m\| + 3\|G\|$
Prameela [14]	$\|m\| + 2\|G\|$
Omala et al. [15]	$\|m\| + 2\|G\|$
Omala et al. [16]	$\|m\| + 3\|q\|$
Gao et al. [17]	$\|m\| + 6\|q\|$
Ullah et al. [18]	$\|m\| + 2\|n\|$
Iqbal et al. [19]	$\|m\| + 2\|G\|$
Proposed	$\|m\| + 2\|n\|$

4.6. CL-Signcrypt. With the sender and receiver identities $(\mathrm{ID_s}, \mathrm{ID_r})$ and a messages M, the sender performs the following steps by composing CGSWSC-signcrypt algorithm.

(1) Uniformly choose $\gamma \in Z^*_{\mathbb{Q}}$ and calculate $\beta = \gamma.D$

(2) Compute $\boldsymbol{d} = \gamma.(Y_\mathrm{r} + \mathscr{H}_\mathrm{I}(Y_\mathrm{r}, \mathrm{ID_r}).W)$ and $\eta = \mathscr{H}_\mathrm{II}(\beta, \mathrm{ID_r}, \delta)$

(3) Uniformly choose another number $\Phi \in Z^*_q$ and compute $\sigma = \mathscr{H}_\mathrm{III}(\beta, \Phi)$

(4) Generate the ciphertext as $\mathscr{K} = {}_\sigma(M[]\mathrm{N_s})$ and then calculate a digital signature as $\Delta = \mho_\mathrm{s} + \gamma.\varphi$, where $\varphi = \mathscr{H}_{IV}(M[]\mathrm{ID_s}, \beta, \Phi)$

(5) At the end, the sender transmits $\psi = (\Lambda, \Delta, \varphi, \beta)$ to the receiver

4.7. CL-Unsigncrypt. Upon receipting $\psi = (\Lambda, \Delta, \varphi, \beta)$, the receiver can verify it by composing the following steps.

(1) Calculate $\boldsymbol{d} = \mho_\mathrm{r}.\beta$ and $\eta = \mathscr{H}_\mathrm{II}(\beta, \mathrm{ID_r}, \delta)$

(2) Compute $\Phi = f(\eta)$ and calculate $\sigma = \mathscr{H}_\mathrm{III}(\beta, \Phi)$

(3) Recover the plain text as $(M[]N_\mathrm{s}) = D_\sigma(\Lambda)$ and compute $\varphi^{\exists} = \mathscr{H}_\mathrm{IV}(M[]\mathrm{ID_s}, \beta, \Phi)$

(4) Accept $(\mathrm{M}[]\mathrm{ID_s})$, if $\varphi^{\exists} = \boldsymbol{v}$ and $\Delta.D = Y_s + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\beta$ are holds

4.7.1. Correctness. Each actor with ID_a can verify the pseudopartial private key G_a by utilizing the following computations:

$$\begin{aligned} G_\mathrm{a}.D &= (R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}).W + \mathscr{H}_I(U_\mathrm{a}.W, \mathrm{ID_a}).D \\ &= G_\mathrm{a}.D = (P_\mathrm{a} + \square\mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}) \\ &\quad + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a})).D \\ &= (P_\mathrm{a}.D + \square.D\mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}) + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a}).D) \\ &= R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{a}, R_\mathrm{a}, \mathrm{ID_a}).W + \mathscr{H}_I(V_\mathrm{a}.\square, \mathrm{ID_a}).D). \end{aligned} \tag{1}$$

The receiver can verify the signature as if $\Delta.D = Y_s + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\ \beta$ is held.

$$\begin{aligned} &= \Delta.D = (\mho_\mathrm{s} + \gamma.\varphi).D = (U_\mathrm{s} + \mathrm{T_s} + \gamma.\varphi).D \\ &= (U_\mathrm{s} + G_\mathrm{s} - \mathscr{H}_I(U_\mathrm{s}.W, \mathrm{ID_s}) + \gamma.\varphi).D \\ &= (U_\mathrm{s} + G_\mathrm{s} - \mathscr{H}_I(U_\mathrm{s}.\square.\mathrm{D}, \mathrm{ID_s}) + \gamma.\varphi).D \\ &= (U_\mathrm{s} + P_\mathrm{s} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) + \mathscr{H}_I(V_\mathrm{s}.,\mathrm{ID_s}) \\ &\quad - \mathscr{H}_I(V_\mathrm{a}.,\mathrm{ID_s}) + \gamma.\varphi).D = (U_\mathrm{s} + P_\mathrm{s} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) \\ &\quad + \gamma.\varphi).D = (U_\mathrm{s}.D + P_\mathrm{s}.D + D\mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s}) + \gamma.D.\varphi) \\ &= (V_\mathrm{s} + R_\mathrm{a} + \mathscr{H}_I(V_\mathrm{s} + R_\mathrm{s}, \mathrm{ID_s})\mathrm{W} + \varphi.\beta \\ &= Y_\mathrm{s} + \mathscr{H}_\mathrm{I}(Y_\mathrm{s}, \mathrm{ID_s}).W + \varphi.\beta. \end{aligned} \tag{2}$$

5. Security Discussions

This scheme provides the security services of confidentiality and integrity because it encrypts the patient data through secret key, which is only known to the application providers and the controller. It also resists against the unauthorized user access because if the attacker wants to access the data then he/she must generate a forged signature for it. Therefore, the attacker does not generate the forged signature because for this purpose he/she must have the private key of application providers. Even if the private key of application providers/controller is known to the attacker, still this scheme has resisted against to break the confidentiality, because, for encryption and decryption purposes, it uses the secret key, which means the new scheme provides the forward secrecy property. Further, this scheme hides the identity of the controller and application providers; it means that it cannot send the identity of the controller and application provider openly with ciphertext, which provides the anonymity property. It also used a technique for the discrepancy resolving among the application providers and controller, if happen, which is called public verifiability security requirement. The new scheme generates a fresh nonce, encrypts it, and sends along with every access control query for the resistance of replay attack. What is more in this new scheme, it is based on a hyperelliptic curve, which is the generalized form elliptic curve which provides the same level of security with 80 bits key in contrast to 160 bits key of elliptic curves. Thus, due to the hyperelliptic curve, our new scheme has the capacity of low computational cost and decrease communication overhead. If we look into the literature section of this paper, only two signcryption schemes [10, 18] for WBAN on the basis of the hyperelliptic curve are available, but the schemes in [10] have the limitations of failing to provide the role of central authority, suffering from certificate renewal and revocations problems, lacking of public verifiability, nonrepudiation, and antireplay attack. The scheme used in [18] can be affected by requiring the certificate management in a network which consists a large number of devices, and it can also be affected by the lack of anonymity property. So, our scheme also removes all these disadvantages which are discussed above.

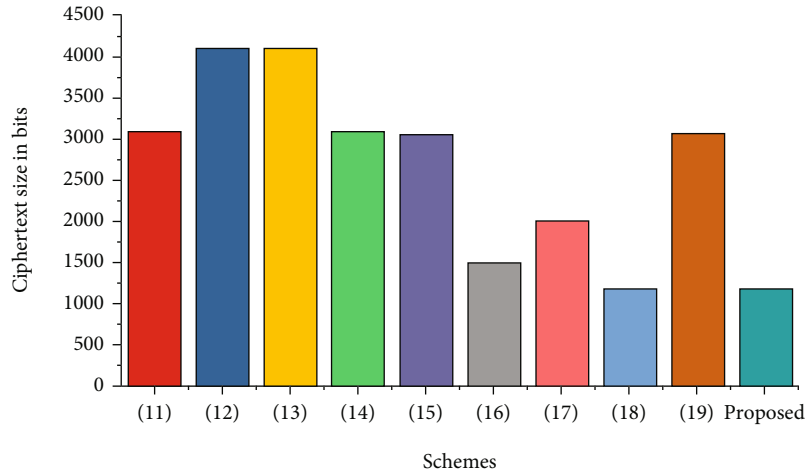

Figure 6: Communication cost.

6. Performance Analysis

This section includes performances analysis in terms of computational and communication costs.

6.1. Computational Cost. In Table 5, we give the computational cost comparison among our designed secure channel free certificateless signcryption and the existing ones, i.e., Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of major operations. We consider the major operation, i.e., bilinear pairing, pairing-based scalar multiplication, exponential, hyperelliptic divisor multiplication, and elliptic curve scalar multiplication in the proposed one and in Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19]. Further, P, PBM, E, HEM, and ESM signify one pairing operation, one pairing-based scalar multiplication operation, one exponential operation, one hyperelliptic curve divisor multiplication operation, and one elliptic curve scalar multiplication operation, respectively. Additionally, we create comparisons among the proposed one and Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of milliseconds (ms), which is shown in Table 6. We observed from [21] that the single ESM consumes 0.97 ms, P needs 14.90 ms, PBM consumes 4.31 ms, E needs 1.97 ms, and it is also assumed that HEM earnings consume 0.48 ms [22–26]. Moreover, a computation cost reduction is shown in Table 7 and Figure 5, respectively.

6.2. Communication Overhead. Sending additional bits along with the actual ciphertext is called communication overhead. If the additional bits are smaller in size, then, the communication will be fast; otherwise, delays will occur in communications. In this phase, we compare our designed CB-PS with existing ones, i.e., Saeed et al. [11], Lu et al. [12], Li et al. [13], Prameela [14], Omala et al. [15], Omala et al. [16], Gao et al. [17], Ullah et al. [18], and Iqbal et al. [19] on the basis of communication overhead as shown in Table 8. To make these comparisons, we suppose that $|H| \cong |ID| \cong |q| \cong 2160$ bits, $|h| \cong |ID| \cong |n| \cong 280$ bits, $|G|$, and $|\mathscr{mW}| \cong |\mathscr{m}| \cong 1024$ bits. Besides, a communication cost reduction is shown in Tables 9 and 8 and Figure 6, respectively.

7. Conclusion

A detailed review of the currently available signcryption schemes that might be used in the WBAN system is presented in this article. Then, each scheme is subjected to a critical review in terms of security requirements, as well as the need for computational and communication expenses. The research revealed that the majority of existing WBAN signcryption schemes failed to meet one or more security requirements, as well as had high computational and communication costs. Then, for WBAN applications, we presented a new framework called secure channel free certificateless signcryption scheme, which is based on the notion of a hyperelliptic curve. The proposed scheme removes all the limitations of existing signcryption schemes for WBAN, because it does not suffer from the certificate management problem, key escrow problem, and does not require any secure channel for the distribution of partial private key. In addition, the scheme is lightweight in terms of computational and communication costs. Furthermore, the new scheme has the capability of providing the security requirements, such as confidentiality, integrity, resist against the unauthorized user, unforgeability, public verifiability, forward secrecy, and antireplay attack, respectively. In the future, we are intended to apply the same scheme to the multimessage and multireceiver environment.

Data Availability

All data generated or analyzed during this study are included in this article.

Conflicts of Interest

The authors declare no conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] A. Meharouech, J. Elias, and A. Mehaoua, "Moving towards body-to-body sensor networks for ubiquitous applications: a survey," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, p. 27, 2019.

[2] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communication Surveys and Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[3] M. A. Khan, I. M. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)," *Drones*, vol. 3, no. 1, p. 16, 2019.

[4] Y. Chen and F. Zhao, "A hybrid half-duplex/full-duplex transmission scheme in relay-aided cellular networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, Article ID 795, 15 pages, 2017.

[5] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)," in *Annual international cryptology conference*, pp. 165–179, Berlin, Heidelberg, 1997.

[6] N. U. Amin, J. Iqbal, and A. R. Abbasi, "Secure key establishment and cluster head selection for body area networks based on signcryption," *Journal of Applied Environmental and Biological Sciences*, vol. 4, pp. 210–216, 2014.

[7] C. Wang and J. Liu, "Attribute-based ring signcryption scheme and its application in wireless body area networks," in *International Conference on Algorithms and Architectures for Parallel Processing*, pp. 521–530, Cham, 2015.

[8] A. Arul Jothi and B. Srinivasan, "Security analysis in body area networks using attribute-based ring signcryption scheme," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 13, no. 1, pp. 48–56, 2016.

[9] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389–5396, 2016.

[10] J. Iqbal, N. U. Amin, and A. I. Umar, "Nizamuddin, public verifiable signcryption and cluster head selection for body sensor networks," *Journal of Applied Environmental and Biological Sciences*, vol. 6, pp. 64–72, 2016.

[11] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "HOOSC: heterogeneous online/offline signcryption for the internet of things," *Wirel. Networks*, vol. 24, no. 8, pp. 3141–3160, 2018.

[12] Y. Lu, X. Wang, C. Hu, H. Li, and Y. Huo, "A traceable threshold attribute-based signcryption for mHealthcare social network," *International Journal of Sensor Networks*, vol. 26, no. 1, pp. 43–53, 2018.

[13] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 747–758, 2018.

[14] S. Prameela, "Enhanced certificateless security improved anonymous access control with obfuscated quality-aware confidential data discovery and dissemination protocol in WBAN," *International Journal of Pure and Applied Mathematics*, vol. 118, pp. 2627–2635, 2018.

[15] A. A. Omala, I. Ali, and F. Li, "Heterogeneous signcryption with keyword search for wireless body area network," *Security and Privacy*, vol. 1, no. 5, article e25, 2018.

[16] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, no. 6, p. 108, 2018.

[17] G. Gao, X. Peng, and L. Jin, "Efficient access control scheme with certificateless signcryption for wireless body area networks," *International Journal of Network Security*, vol. 21, pp. 428–437, 2019.

[18] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things," *Electronics*, vol. 8, no. 10, p. 1171, 2019.

[19] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[20] H. Xiong, Y. Hou, X. Huang, Y. Zhao, and C. -M. Chen, "Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs," *IEEE Systems Journal*, pp. 1–10, 2021.

[21] I. Ullah, N. U. Amin, J. Khan et al., "A novel provable secured signcryption scheme: a hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, 2019.

[22] M. Asghar Khan, I. Ullah, A. Alkhalifah et al., "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[23] M. A. Khan, I. Ullah, N. Kumar et al., "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4839–4851, 2021.

[24] M. A. Khan, I. Ullah, S. Nisar et al., "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, vol. 2020, Article ID 8861947, 15 pages, 2020.

[25] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[26] M. A. Khan, S. U. Rehman, M. I. Uddin et al., "An online-offline certificateless signature scheme for internet of health things," *Journal of Healthcare Engineering*, vol. 2020, Article ID 6654063, 10 pages, 2020.

[27] L. Pang, M. Kou, M. Wei, and H. Li, "Anonymous certificateless multi-receiver signcryption scheme without secure channel," *IEEE Access*, vol. 7, pp. 84091–84106, 2019.