sensors

MDPI

Article

Enabling Secure Communication in Wireless Body Area Networks with Heterogeneous Authentication Scheme

Insaf Ullah [1], Muhammad Asghar Khan [1], Ako Muhammad Abdullah [2,3], Fazal Noor [4], Nisreen Innab [5] and Chien-Ming Chen [6,*]

1 Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan
2 Computer Science Department, College of Basic Education, University of Sulaimani, Sulaimaniyah 00964, Kurdistan Region, Iraq
3 Department of Information Technology, University College of Goizha, Sulaimaniyah 00964, Kurdistan Region, Iraq
4 Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia
5 Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, P.O. Box 71666, Riyadh 11597, Saudi Arabia
6 College of Computer Science and Technology, Shandong University of Science and Technology, Qingdao 266590, China
* Correspondence: chienmingchen@ieee.org

Abstract: Thanks to the widespread availability of Fifth Generation (5G) wireless connectivity, it is now possible to provide preventative or proactive healthcare services from any location and at any time. As a result of this technological improvement, Wireless Body Area Networks (WBANs) have emerged as a new study of research in the field of healthcare in recent years. WBANs, on the one hand, intend to gather and monitor data from the human body and its surroundings; on the other hand, biomedical devices and sensors interact through an open wireless channel, making them exposed to a range of cyber threats. However, WBANs are a heterogeneous-based system; heterogeneous cryptography is necessary, in which the transmitter and receiver can employ different types of public key cryptography. This article proposes an improved and efficient heterogeneous authentication scheme with a conditional privacy-preserving strategy that provides secure communication in WBANs. In the proposed scheme, we employed certificateless cryptography on the client side and Identity-Based Cryptography on the receiver side. The proposed scheme employs Hyperelliptic Curve Cryptography (HECC), a more advanced variation of Elliptic Curve Cryptography (ECC). HECC achieves the same level of security with a smaller key size and a more efficient approach than its counterpart methods. The proposed scheme not only meets the security and privacy standards of WBANs but also enhances efficiency in terms of computation and communication costs, according to the findings of the security and performance analysis.

Keywords: WBANs; Fifth Generation (5G); Hyperelliptic Curve Cryptography (HECC); heterogeneous cryptography; authentications

Citation: Ullah, I.; Khan, M.A.; Abdullah, A.M.; Noor, F.; Innab, N.; Chen, C.-M. Enabling Secure Communication in Wireless Body Area Networks with Heterogeneous Authentication Scheme. *Sensors* **2023**, *23*, 1121. https://doi.org/10.3390/s23031121

Academic Editor: Antonio Guerrieri

Received: 16 November 2022
Revised: 11 January 2023
Accepted: 14 January 2023
Published: 18 January 2023

1. Introduction

WBANs (Wireless Body Area Networks) are a collection of medical devices and software applications that collect, analyze, and communicate the physiological data of patients [1,2]. WBANs have recently received more attention as a result of recent technological breakthroughs in the fields of electronics, sensors, and wireless communication technologies. Due to the wide spread availability of 5G wireless technology, patients can now obtain preventative or proactive healthcare treatments from any location and at any time. Blood pressure, heart rate, body temperature, respiratory rate, electrocardiogram, patient posture, breathing rate, and other signals can all be gathered, analyzed, and shared in real time between both the patient's own electronic devices and the medical practitioner [3–7].

WBANs can also provide information on patient care settings, room conditions, laboratory shift timings, treatment durations, and staff-to-patient ratios. This information can be saved as an electronic health record in the health information system, which will be accessible to medical experts with a single click whenever the patient visits the hospital. Figure 1 depicts the general architecture of WBANs, in which sensor nodes gather and transfer real-time physiological data from patients to an AP and a typical smart medical service.

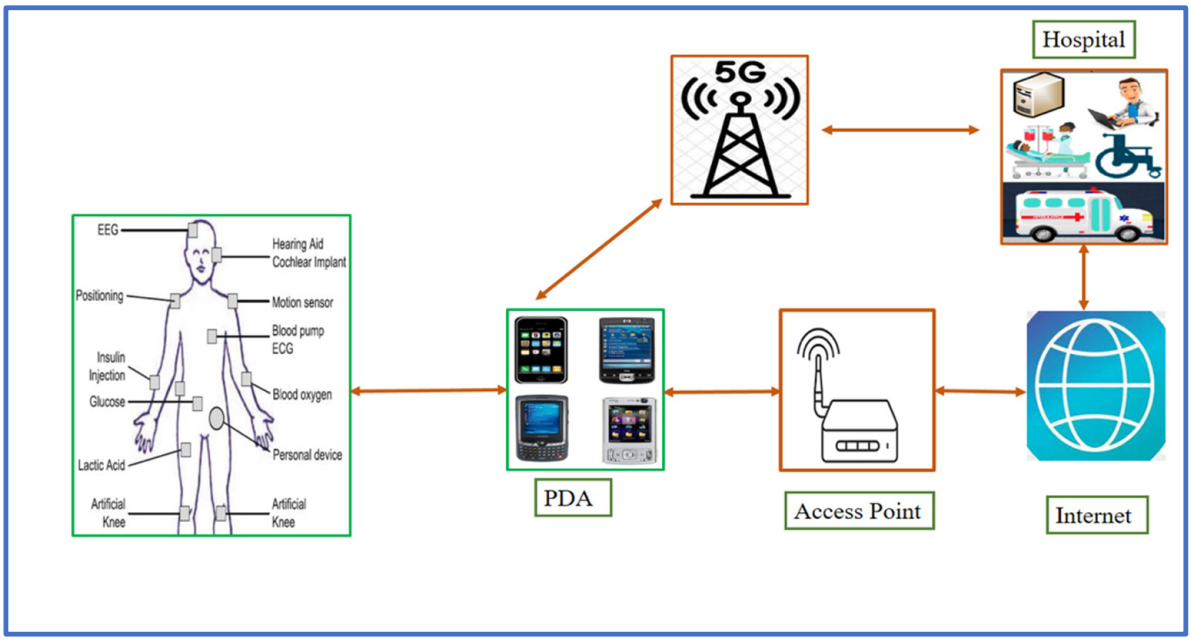

Figure 1. Sample Architecture of WBANs.

Because a considerable number of interactions between biomedical sensors and devices occur via the Internet, security and privacy concerns over sensitive patient data have arisen in WBANs [8]. An intruder, for example, may intercept a communication connection between biomedical devices and sensors in order to steal or manipulate patient health data. As a result, authentication mechanisms are essential to ensure secure communication in WBANs, as well as the privacy of patients' health-related information. Unfortunately, since most WBANs devices have limited processing and storage capacity, they are unable to execute traditional authentication mechanisms that require complex cryptographic computations, rendering them ineffective for WBANs. As a result, most public key cryptosystems published in the literature require a large number of computations, making them unsuitable for WBAN implementation.

Authentication in cryptography is accomplished by the digital signature procedure, which can be utilized for secure communication in WBANs [9,10]. A shared key is typically used to secure not just authentication and privacy but also confidentiality, integrity, and non-repudiation [11,12]. Identity-Based Cryptography (IBC) and Public Key Infrastructure (PKI) are the two most used ways for validating public keys in public-key cryptosystems. The CA specifies the public keys with the certificates as a participant. On the other hand, PKI systems include downsides such as certificate lifetimes, distribution, and storage concerns. IBC is instead promoted as a means to lower the expense of managing public keys [13]. When it comes to the cost of private key escrow issues, the trustworthy Private Key Generator (PKG) has firsthand knowledge of the participants' private keys [14,15]. Finally, the key escrow issue in authentication schemes can be addressed by combining a certificateless cryptosystem with a signature strategy.

Although public key cryptosystems are suited for a homogeneous environment, WBANs are a heterogeneous-based system; hence, heterogeneous cryptography is required. The transmitter and receiver in heterogeneous cryptography may use various forms

of public key cryptography. In some cases, for example, the sender belongs to IBC, and the receivers use PKI, or the sender uses PKI, and the receivers use IBC. Furthermore, it is possible that the sender uses a certificateless cryptosystem and the receivers use IBC or that the sender uses a certificateless cryptosystem and the receivers use PKI. As a result, in the following Figures 2 and 3, we show the functioning capacity of each of these cryptosystems one by one. Figure 2 shows how we give IBC to the PKI cryptosystem, which includes a Wearable Sensor Device (WSD) injected into the patient's body, a Trusted Authority (TA), and Application Providers (AP). The process starts when WSD communicate their identities to TA, who then generates the public and private keys for WSD and sends them via a secure network. Following this, WSD may construct the authentication message and transmit it to AP; AP will then give their public key to TA, who will then generate a certificate based on that public key and publicly proclaim it.

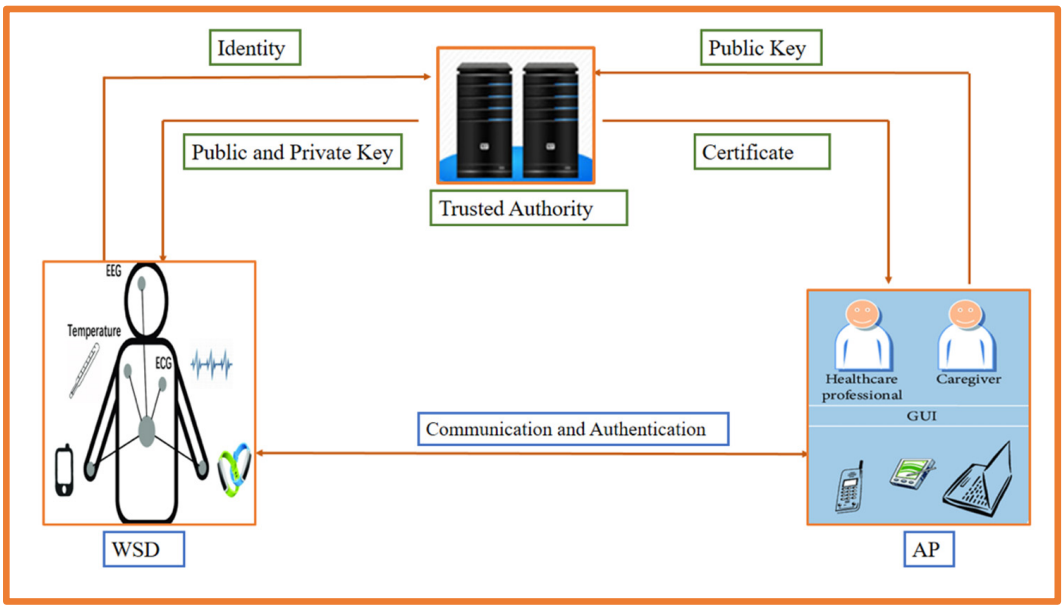

Figure 2. Heterogeneous cryptography (IBC to PKI or PKI to IBC).

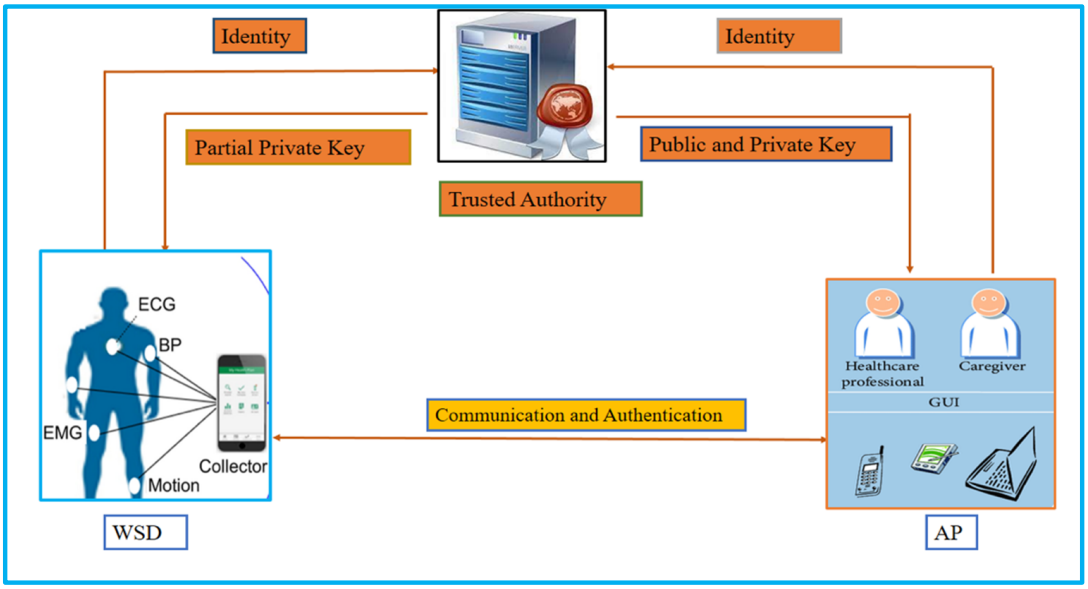

Figure 3. Heterogeneous cryptography (certificateless to IBC).

In addition, if we regard AP as a transmitter and WSD as a receiver in Figure 2, the PKI to IBC heterogeneous cryptosystem will be represented. Furthermore, we depict the certificateless cryptosystem to IBC in Figure 3, where WSD belongs to certificateless cryptography, and AP uses IBC. TA will produce a partial private key for WSD and transmit it through a secure channel after receiving identification from WSD and AP. TA will also generate a private key for AP and send it via a private network after receiving identity from WSD and AP. After that, the WSD and the AP may communicate and authenticate with each other.

Figure 4 depicts certificateless to PKI cryptography, with WSD belonging to certificateless cryptography and AP using PKI. TA will construct the partial private key for WSD and transmit it via a secure channel after receiving the identification from WSD and the public key from AP. TA will also create the certificate for AP and send it over to a public network. After that, the WSD and the AP may communicate and authenticate with each other.

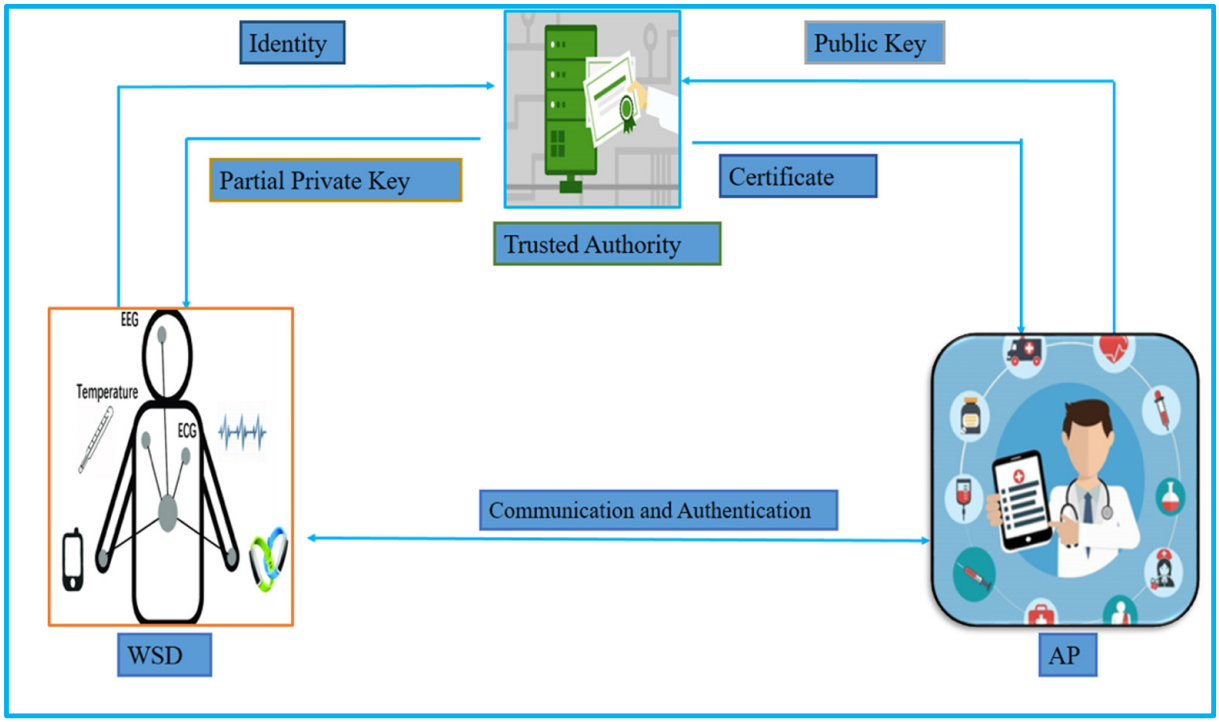

Figure 4. Heterogeneous cryptography (certificateless to PKI).

In this article, we propose an authentication scheme in heterogeneous settings (certificateless to IBC) based on the discussion above. We considered Hyperelliptic Curve Cryptography (HECC) to create the proposed scheme, which uses just 80-bit keys to give the same level of security in preventing cyber-attacks [16]. As a result, for WBAN devices with limited resources, HECC would be a better option. The following are some of the key contributions of the undertaken research work:

1. We propose a heterogeneous authentication scheme for WBANs that uses the HECC approach, which makes our scheme computationally efficient.
2. Informal security analysis has been used to evaluate the proposed scheme's ability to withstand different attacks. The results support the proposed scheme's resiliency.
3. Finally, in terms of computation and communication costs, we compare the proposed scheme to existing equivalent schemes. The result demonstrates that our approach surpasses its competitors.

Structure of the Paper

The following is how the rest of the article is organized. The related work is detailed in Section 2. The network model is provided in Section 3, followed by the proposed scheme in Section 4. Sections 5 and 6 contains a security analysis. Section 7 provides a performance evaluation with existing approaches. Concluding remarks are provided in Section 8.

2. Related Work

This section covers the existing solutions that have been used to overcome the security and privacy challenges of WBANs that use authentication mechanisms. In 2014, Chen et al. [16] proposed an authentication scheme for medical data exchange in the cloud environment to secure patients' health information. According to Chiou et al. [17], the approach developed by Chen et al. [16] could not ensure patient confidentiality or message authentication. In [17], the authors improved the privacy authentication process in the cloud health environment.

In 2016, Li et al. [18] introduced a network-based electronic medical authentication scheme that includes two-factor authentication using the user's password and smart card. He et al. [19] proposed an authentication scheme that is better suited to the setup of telemedicine information systems on mobile devices with minimal battery consumption. Wei et al. [20] observed that this protocol is vulnerable to password attacks; they proposed an improved authentication protocol for telemedicine information systems and showed that it fits the security criteria of two-factor authentication. Wu et al. [21] introduced a lightweight two-factor medical authentication approach in 2018, claiming that their protocol is secure; however, after further investigation, it was shown that their protocol could not successfully resist perfect forward security.

In 2016, Wu et al. [22] proposed a novel anonymous authentication scheme for WBANs and demonstrated that it is secure in a random oracle model. The proposed scheme, on the other hand, was based on bilinear pairing, which entails computationally intensive operations. He et al. [23] proposed a provable security anonymous authentication scheme for WBAN. The proposed scheme [23], on the other hand, comprises a bilinear pairing-based operation, which is a computationally expensive operation. In 2018, Ji et al. [24] proposed a certificateless conditional privacy-preserving authentication technique for WBAN in a big data environment. The proposed technique allows for batch authentication of multiple clients, considerably reducing the service provider's computing overhead. The proposed scheme supports common security aspects such as user anonymity, unlinkability, mutual authentication, traceability, and forward secrecy. On the basis of assessing the most recently presented certificateless authentication scheme for WBANs, Xie et al. [25] proposed an improved and efficient certificateless authentication scheme with conditional privacy-preserving. However, the proposed scheme was based on elliptic curve cryptography, which is not that suitable for WBAN devices.

Liao et al. [26] proposed a certificateless authentication scheme for WBAN, in which they used the concept of online and offline signature methods. However, the proposed scheme failed to provide real-time communication due to the use of bilinear pairing that needs extra machine time and bandwidth space.

Recently, Li et al. [27] proposed a certificateless authentication with the help of an elliptic curve; however, the proposed scheme failed to provide real-time communication due to the use of an elliptic curve that needs extra machine time and bandwidth space.

The schemes outlined above rely on cryptographic techniques such as ECC and bilinear pairing and have high computation and communication costs. On the other hand, the proposed scheme is based on the concept of HECC, which is a more refined variant of ECC. It provides the same amount of security as other methods but with a smaller key size.

3. Network Model

Figure 5 depicts the proposed network's working flow, in which we considered three main entities that are client, Application Provider (AP), and Key Generation Center (KGC), respectively. The role of each entity is explained as follows.

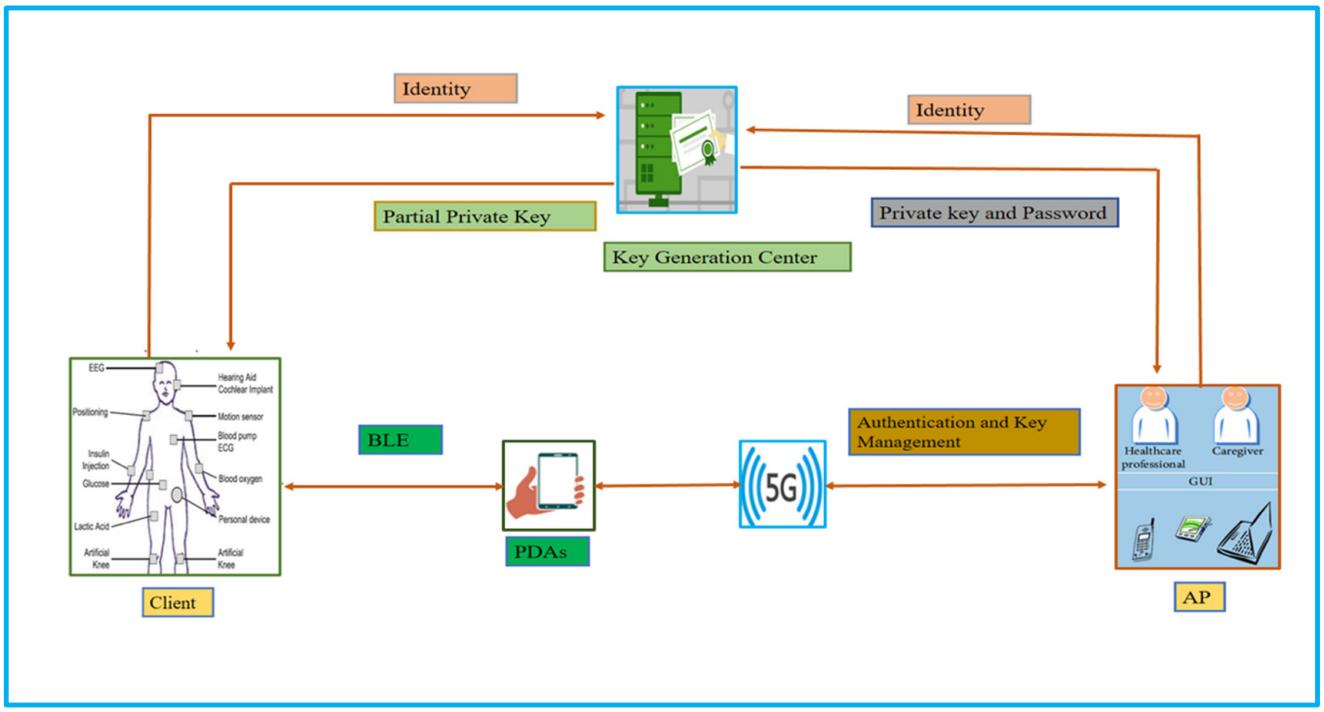

Figure 5. Proposed heterogeneous authentication and key management scheme.

3.1. Client

The client is the sensors placed in the human body, and the work of these sensors is to collect health-related data from the human body. The client sends a request along with their identity for the partial private key to KGC, then by using a secure channel, KGC sends a partial private key to the client.

Further, the collected data, along with a partial private key, is sent by the client through Bluetooth Low Energy (BLE) to PDAs. With the help of the client, PDAs first generate a signature, secret key, public parameter, cipher text, and hash value. Then PDAs will send the hash value, public parameter, ciphertext, and signature to AP through 5G technology.

3.2. Application Provider (AP)

This entity sends a request along with its identity to KGC, then the KGC generates and sends a private key to AP through a secure channel. Therefore, upon receiving the hash value, public parameter, ciphertext, and signature, AP first verifies the signature, recovers the secret key, and uses the secret key to recover a message from the ciphertext.

3.3. Key Generation Center (KGC)

This entity is responsible for generating the partial private key for the client and the private key for AP.

4. Proposed Conditional Privacy-Preserving Authentication Scheme for WBAN

In this section, we first provide Table 1, which includes acronyms used in the article and symbols utilized in the new algorithm. The five stages of our proposed conditional privacy-preserving authentication scheme for WBAN are described [24]:

Table 1. Acronyms and symbols used in this paper.

No	Symbol/Acronym	Descriptions
1	WBAN	Represent Wireless Body Area Network
2	KGC	Used for Key Generation Center
3	$H_a{}^1, H_a{}^2, H_a{}^3, H_a{}^4$	Represents four hash functions and their capability as it is irreversible
4	α	Used for the master public key of KGC
5	$\mathscr{k}$	Used for the master secret key of KGC
6	AP	Represents Application Provider
7	(η, Y)	Represents the public key pair of Application Provider
8	$(\varphi, \mathfrak{T})$	Represents the secret key pair of Application Provider
9	$Client_{PW}$	Represents the password for client
10	$Client_{RID}$	Represents the real identity for client
11	$Client_{PID}$	Represents the pseudo identity for client
12	$\oplus$	Used for the encryption and decryption function
13	E_K	Encryption by utilizing the secret key K
14	E_K	Shared secret key which can be used for encryption and decryption of medical data
15	T_{limit}	It is used for to define the limit of time of session
16	$\boldsymbol{A_{out}}$	Represents the attacking role of outsider attacker
17	$\boldsymbol{A_{insd}}$	Represents the attacking role of insider attacker
18	MIRACL	Represents Multi-precision Integer and Rational Arithmetic
19	HEMUL	Used for Hyper elliptic curve divisor multiplication
20	T_{exp}	Represents the time required for sin gle exponentials
21	T_{mp}	Represents the time required for single bilinear pairing multiplication
22	T_{ecmp}	The time required for sin gle elliptic curve multiplication
23	T_{hecmp}	Time required for sin gle hyper elliptic curve multiplication
24	T_p	Time required for sin gle bilinear pairing operations
25	b_C	Represents the bits required for ciphertext
26	b_G	Represents the bits required for bilinear parameter
27	b_T	Rpresents the bits required for timestamp
28	b_q	Used for bits required for elliptic curve parameter
29	b_n	bits required for hyper elliptic curve parameter
30	b_h	It is used for bits required for hash value
31	HECC	Represents Hyperelliptic Curve Cryptography
32	PKG	Represents Private Key Generator
33	PKI	Represents Public Key Infrastructure
34	IBC	Used for Identity-Based Cryptography
35	ECG	Used to represent electrocardiogram
36	5G	Used to represent Fifth-Generation
37	ECC	Used to represent Elliptic Curve Cryptography

4.1. Setup

The KGC performs the following sub initializations:
It chooses a hyper elliptic curve of genus 2 with 80 bits parameter size;

It also chooses the hash functions, i.e., $(H_a{}^1, H_a{}^2, H_a{}^3, H_a{}^4)$, and its capability as it is irreversible;

Then, it selects $\hbar$ randomly from the finite group of hyper elliptic curve and computes $\alpha = \hbar.\mathcal{D}$ and set α as the master public key and $\hbar$ as the secret key;

Exempt α, the KGC published all the above-discussed parameters in a network;

For AP, it selects $\varphi, \mathfrak{T}$ randomly from the finite group of hyper elliptic curve, calculates $\eta = \varphi\,.\mathcal{D}$, $Y = \mathfrak{T}\,.\mathcal{D}$ and sets (η, Y) as the public key and $(\varphi, \mathfrak{T})$ as the secret key of AP.

4.2. Pseudo Identity Generation

A client can select σ randomly from the finite group of hyper elliptic curve and compute $\mathfrak{S} = \sigma.\mathcal{D}$, and by using a secure network, it sends $(\mathfrak{S},\ Client_{RID}, Client_{PW})$ to the KGC, where $Client_{RID}$ is the identity of the client, and $Client_{PW}$ denotes the password of the client. Upon reception $(\mathfrak{S},\ Client_{RID}, Client_{PW})$, the KGC can select θ randomly from the finite group of hyper elliptic curve and compute $\mathfrak{h} = \theta.\mathcal{D}$, $\mathcal{E} = H_a{}^1(Client_{RID}) \oplus H_a{}^1(Client_{PW})$, $\ell = H_a{}^2(\hbar.\mathfrak{S}, T_{limit}, \mathfrak{h})$, $Client_{PID} = Client_{RID} \oplus \ell$, $\mathcal{J} = H_a{}^3(Client_{PID}, \mathfrak{S}, \mathfrak{h}, T_{limit})$, and $\Omega = \theta + \hbar.\mathcal{J}$, respectively. Then, KGC saves $(Client_{PID}, \mathfrak{S}, \mathfrak{h}, T_{limit}, \Omega, \mathcal{E})$ in the memory of the controller. Finally, the client can set (Ω, σ) as their private key and $(\mathfrak{S}, \mathfrak{h})$ as their public key.

4.3. Mutual Authentication and Secrete Key Management

A client can select χ randomly from the finite group of hyper elliptic curve and compute $\mathcal{Q} = \chi.\mathcal{D}$, $K = \chi.\eta$, $r = H_a{}^3(\ \mathcal{Q}.\mathfrak{S}, T_{limit}, \mathfrak{h}, Client_{PID})$, $S = \varphi + \mathfrak{T} + r.\chi$, and send $(\mathcal{Q}, r,\ S)$ to AP.

When AP receives the triple $(\mathcal{Q}, r,\ S)$ then it performs the following step for the verification of the signature received from the client and generation of the secret key.

It computes $S.\mathcal{D} = \mathrm{Y} + \eta + \mathrm{r}.\mathcal{Q}$ if it is qualified, then the client mutually authenticates with AP.

Then AP generates the secret key as $K = \mathcal{Q}.\varphi$ and when it receives an encrypted message as $C = E_K(medical\ data)$ from the client, it performs the decryption process on the same secret key.

4.4. Password Change Phase

This phase is the same as the password change process in [1].

4.5. Correctness

Here, AP can generate the secret key and verify the signature as follows:

$K = \mathcal{Q}.\varphi = \mathcal{Q}.\varphi = \chi.\mathcal{D}.\varphi = \chi.\eta$, hence proved;

$S.\mathcal{D} = \mathrm{Y} + \eta + \mathrm{r}.\mathcal{Q} = (\varphi + \mathfrak{T} + r.\chi).\mathcal{D} = (\varphi.\mathcal{D} + \mathfrak{T}.\mathcal{D} + r.\chi.\mathcal{D}) = (\mathrm{Y} + \eta + \mathrm{r}.\mathcal{D})$, hence proved.

5. Formal Security Analysis

In this section, the formal analysis for our proposed scheme is performed through the widely accepted ROR oracle model during the section, i.e., "4.3. Mutual Authentication and Secrete Key Management" between client and AP [28]. In Theorem 1, we proved that our designed scheme is safeguarded regarding derivations of the secret key ($K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$) from both type of attacker, i.e., $A_{insd/out} = (A_{out}, A_{insd})$, which are shared between the client and AP. Furthermore, $A_{insd/out}$ has full access to the following queries:

Execute Query: With the help of this query, $A_{insd/out}$ can eavesdrop on all the transmitted messages between the client and AP.

Corrupt Device Query: With the help of this query, $A_{insd/out}$ can physically extract the parameters stored in the device that belongs to the client or AP.

Reveal Query: With the help of this query, $A_{insd/out}$ has access to a disclosed session key between the client and AP.

Test Query: With the help of this query, $A_{insd/out}$ can verify whether the generated session key is a random or real one.

Theorem 1. *In this theorem, we prove that our scheme is a secret key that is secure from $A_{insd/out}$, which can execute itself in a polynomial time (Pol_{tm}). Suppose Q_{hqry}, $|Hash_{space}|$, and $Adv_{A_{insd/out}}hecdlp\ (Pol_{tm})$ denotes the hash query, space for hash value, and advantage of breaking the hardiness of $(hecdlp)$ for $A_{insd/out}$, respectively, then $Adv_{A_{insd/out}}hecdlp\ (Pol_{tm}) \leq \frac{{Q_{hqry}}^2}{|Hash_{space}|} + 2Adv_{A_{insd/out}}hecdlp\ (Pol_{tm})$.*

Proof. In this section, we made three games (${Game_1}^{A_{insd/out}}$, ${Game_2}^{A_{insd/out}}$, ${Game_3}^{A_{insd/out}}$), and their explanations are followed. □

${Game_1}^{A_{insd/out}}$: By using this game, $A_{insd/out}$ can launch an actual attack on the proposed scheme and guess a random bit (rdm_{bits}), so we can obtain the following equation:

$$Adv_{A_{insd/out}}hecdlp\ (Pol_{tm}) = |2Adv_{{A_{insd/out,Game_1}}^{A_{insd/out}}}\ proposed\ scheme\ (Pol_{tm}) - 1| \quad (1)$$

${Game_2}^{A_{insd/out}}$: By using the execute query in this game, $A_{insd/out}$ can eavesdrop all the transmitted messages ($(\mathcal{Q}, r,\ S)$, (C)). Then, the attacker $A_{insd/out}$ can try to make the secret shared key ($K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$). Furthermore, $A_{insd/out}$ needs to execute Reveal Query and Test Query to check whether the newly computed secret key is original or fake. Suppose their available outsider attacker (A_{out}) who is trying to generate $K = \chi.\eta$ and decrypt (C). Suppose in our proposed scheme, A_{out} has no access to the master secret key ($\hbar$) and has the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{out} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{out} failed because, in these two equations, χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem $(hecdlp)$. Suppose their available insider attacker (A_{insd}) is trying to generate $K = \chi.\eta$ and decrypt (C). Suppose in our proposed scheme, A_{insd} has access to the master secret key ($\hbar$) and does not have the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{insd} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{insd} failed because in these two equations χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem. Thus, we can obtain the following equation.

$$Adv_{{A_{insd/out,Game2}}^{A_{insd/out}}}\ proposed\ scheme = Adv_{{A_{insd/out,Game1}}^{A_{insd/out}}}\ proposed\ scheme \quad (2)$$

${Game_3}^{A_{insd/out}}$: By using the Corrupt Device Query, in this game $A_{insd/out}$ can derive the session key ($K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$) by computing a hard problem such as $hecdlp$. The session key can be revealed in two ways, as follows: (1) Suppose in our proposed scheme, A_{out} has no access to the master secret key ($\hbar$) and has the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{out} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{out} failed because in these two equations χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem $(hecdlp)$. (2) Suppose their available insider attacker (A_{insd}) who is trying to generate $K = \chi.\eta$ and decrypt (C). Suppose in our proposed scheme, A_{insd} has access to the master secret key ($\hbar$) and does not have the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{insd} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{insd} failed because in these two equations, χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem. Moreover, the other credentials are protected through a hash function that is $r = {H_a}^3(\ \mathcal{Q}.\mathfrak{S}, T_{limit}, \mathfrak{h}, Client_{PID})$,

so it is not possible for an attacker to recover these credentials because of the irreversible property of the hash function. Therefore, we can obtain the following equation:

$$\begin{aligned} |Adv_{A_{\frac{insd}{out},Game2}{}^{A_{\frac{insd}{out}}}} proposed\ scheme - Adv_{A_{\frac{insd}{out},Game3}{}^{A_{\frac{insd}{out}}}} proposed\ scheme| \\ \leq \frac{Q_{hqry}{}^2}{2|Hash_{space}|} + Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}) \end{aligned} \tag{3}$$

It is important to note that $A_{insd/out}$ is the only one who asks the queries; therefore, $A_{insd/out}$ must predict bits properly to win the game $Game_3{}^{A_{insd/out}}$. Therefore, we can obtain the following equation.

$$Adv_{A_{insd/out,Game2}{}^{A_{insd/out}}} proposed\ scheme = \frac{1}{2}. \tag{4}$$

From Equation (1), we can obtain the following result.

$$\begin{aligned} \tfrac{1}{2} Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}) = \\ |2Adv_{A_{insd/out,Game_1}{}^{A_{insd/out}}} proposed\ scheme\ (Pol_{tm}) - \tfrac{1}{2}| \end{aligned} \tag{5}$$

Then, by using Equations (2)–(4) with the help of triangular inequality, we can make the following results from Equation (5).

$$\begin{aligned} \tfrac{1}{2} Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}) = |Adv_{A_{\frac{insd}{out},Game1}{}^{A_{\frac{insd}{out}}}} proposed\ scheme - \\ Adv_{A_{\frac{insd}{out},Game3}{}^{A_{\frac{insd}{out}}}} proposed\ scheme\ | = \\ Adv_{A_{\frac{insd}{out},Game2}{}^{A_{\frac{insd}{out}}}} proposed\ scheme - \\ Adv_{A_{\frac{insd}{out},Game3}{}^{A_{\frac{insd}{out}}}} proposed\ scheme\ | \leq \frac{Q_{hqry}{}^2}{2|Hash_{space}|} + \\ Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}) \end{aligned} \tag{6}$$

By multiplying 2 by both sides of Equation (6), we can obtain the following result:

$$Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}) \leq \frac{Q_{hqry}{}^2}{|Hash_{space}|} + 2Adv_{A_{insd/out}} hecdlp\ (Pol_{tm}). \tag{7}$$

6. Informal Security Analysis

The security analysis of the new scheme is based on the hard problem called hyper elliptic curve discrete logarithm problem, in which both types of attacker (A_{out} and A_{insd}) trying to extract the unknown value, such as A from $B = A.D$. We consider two types of attacker, A_{out} and A_{insd}; furthermore, A_{out} is an outsider attacker who can try to steal information or destroy the forge ability and modify the medical data without having access to the master secret in a Dolev–Yao model channel. The A_{insd} is the insider attacker who can try to steal information or destroy the forge ability and modify the medical data with access to master secret in a Dolev–Yao model channel. Hence, in the following sub phases, we illustrate the security analysis of our proposed scheme on the basis of a hyper elliptic curve discrete logarithm problem.

6.1. Confidentiality against A_{out}

Suppose there is an available outsider attacker (A_{out}) who is trying to generate $K = \chi.\eta$ and decrypt (C). Suppose, in our proposed scheme, A_{out} has no access to the master secret key ($\hbar$) and has the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{out} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{out} failed because, in these two equations, χ and φ are not known

to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem (hecdlp).

6.2. Confidentiality against A_{insd}

Suppose their available insider attacker (A_{insd}) who is trying to generate $K = \chi.\eta$ and decrypt (C). Suppose in our proposed scheme, A_{insd} has access to the master secret key ($\hbar$) and does not have the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{insd} can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{insd} failed because in these two equations χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem.

6.3. Unforgeability against A_{out}

Suppose their available outsider attacker (A_{out}) who is trying to generate $S = \varphi + \mathfrak{T} + r.\chi$ with the intention of making a forged signature. Suppose in our proposed scheme, A_{out} has no access to the master secret key ($\hbar$) and has the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{out} can extract the original value of S by utilizing $S = \varphi + \mathfrak{T} + r.\chi$; here, A_{out} failed because, in this equation, χ, φ, and $\mathfrak{T}$ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem three times.

6.4. Unforgeability against A_{insd}

Suppose their available insider attacker (A_{insd}) who is trying to generate $S = \varphi + \mathfrak{T} + r.\chi$ with the intention of making a forged signature. Suppose in our proposed scheme, A_{insd} has access to a master secret key ($\hbar$) and does not have the capacity to replace the public key of the user. Therefore, in the proposed scheme, A_{insd} can extract the original value of S by utilizing $S = \varphi + \mathfrak{T} + r.\chi$; here, A_{insd} failed because, in this equation, χ, φ, and $\mathfrak{T}$ are not known to him and also equals to find the solution for hyper elliptic curve discrete logarithm problem three times.

6.5. Anonymity

In the proposed scheme, the client send $(\mathcal{Q}, r,\ S)$ to AP through an open network, where $S = \varphi + \mathfrak{T} + r.\chi$, $\mathcal{Q} = \chi.\mathcal{D}$, and $r = {H_a}^3(\ \mathcal{Q}.\mathfrak{S}, T_{limit}, \mathfrak{h}, Client_{PID})$. In this triple $(\mathcal{Q}, r,\ S)$, the client does not use any of its own or AP real identity, so we can say that our proposed scheme intelligently provides anonymity property.

6.6. Mutual Authentication

In the proposed scheme, the client can generate a signature $S = \varphi + \mathfrak{T} + r.\chi$, and send $(\mathcal{Q}, r,\ S)$ to AP. When AP receives the triple $(\mathcal{Q}, r,\ S)$ it then performs the following step for the verification of the signature received from AP and generation of the secret key. It computes $S.\mathcal{D} = \mathrm{Y} + \eta + \mathrm{r}.\mathcal{Q}$ if it is qualified, then the client mutually authenticates with AP.

6.7. Modification Attack

In the proposed scheme, A_{out} and A_{insd} cannot modify the ciphertext because it is protected through a secret key $K = \chi.\eta$, so they can extract the original value of the secret key by utilizing $K = \chi.\eta$ and $K = \mathcal{Q}.\varphi$; here, A_{insd} and A_{out} failed because, in these two equations, χ and φ are not known to them and also equals to find the solution for hyper elliptic curve discrete logarithm problem.

6.8. Session Key Establishment

In the proposed scheme, A client can select χ randomly from the finite group of hyper elliptic curve and compute $= \chi.\mathcal{D}$, $K = \chi.\eta$, $r = {H_a}^3(\ \mathcal{Q}.\mathfrak{S}, T_{limit}, \mathfrak{h}, Client_{PID})$, $S = \varphi + \mathfrak{T} + r.\chi$, and send $(\mathcal{Q}, r,\ S)$ to the client. When the client receives the triple $(\mathcal{Q}, r,\ S)$

then it performs the following step for the verification of the signature received from APR and generation of the secret key. It computes $S.\mathcal{D} = \mathrm{Y} + \eta + \mathrm{r}.\mathcal{Q}$ if it is qualified, then the client mutually authenticates with AP, then generate the secret key as $K = \mathcal{Q}.\varphi$.

6.9. Impersonation Attack

In the proposed scheme, A_{out} and A_{insd} cannot generate the original signature as $S = \varphi + \mathrm{T} + r.\chi$. Suppose, in the proposed scheme, A_{out} and A_{insd} can extract the original value of S by utilizing $S = \varphi + \mathrm{T} + r.\chi$; here, A_{out} and A_{insd} failed because, in this equation χ, φ, and T are not known to him and also equals to find the solution for the hyper elliptic curve discrete logarithm problem three times.

7. Performance Evaluation

This section compares the proposed scheme to other relevant schemes in terms of computation and communication costs. The detailed comparative analysis regarding computation cost and communication between the proposed scheme and those of Wu et al. [22], He et al. [23], Ji et al. [24], and Xie et al. [25] are given in the following Sections 7.1 and 7.2.

7.1. Computation Cost

The proposed scheme is compared to the relevant schemes published by Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27] in this section. The comparison is made in terms of the cost of computation. The key findings from the computation cost comparison are summarized in Table 2. To assess the proposed scheme's performance in terms of computation cost, we employed the Multi-precision Integer and Rational Arithmetic (MIRACL) C Library [29]. The library runs a large number of tests, up to 1000, on basic cryptographic operations. The simulations are run on a machine with a 2.0 GHz Intel Core i7-4510U CPU, 8 GB RAM, and Windows 7 [30]. Because of its smaller key size of 80 bits, the HEMUL is anticipated to take 0.48 milliseconds [31,32]. The comparisons are provided in Table 2, which reveals that the proposed scheme is substantially more cost-effective in terms of computation. The computational cost comparisons in milliseconds are also provided in Table 3, which is then illustrated in Figure 6 and clearly indicates that the proposed scheme is efficient by Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27].

Table 2. Computational cost comparisons.

Schemes	Sender Cost	Receiver Cost	Total Cost
Wu et al. [22]	$2T_{exp} + 3T_{mp}$	$2T_{exp} + 3T_{mp} + 1T_p$	$4T_{exp} + 4T_{mp} + 1T_p$
He et al. [23]	$4T_{mp}$	$1T_p + 4T_{mp}$	$1T_p + 8T_{mp}$
Ji et al. [24]	$3T_{ecmp}$	$3T_{ecmp}$	$6T_{ecmp}$
Xie et al. [25]	$3T_{ecmp}$	$3T_{ecmp}$	$6T_{ecmp}$
Liao et al. [26]	$4T_{mp} + T_{exp}$	$2T_{exp} + 5T_p$	$2T_{exp} + 4T_{mp} + 5T_p$
Li et al. [27]	$3T_{ecmp}$	$4T_{ecmp}$	$7T_{ecmp}$
Proposed Scheme	$3T_{hecmp}$	$3T_{hecmp}$	$6T_{hecmp}$

Note: T_{exp} = Time required for single exponentials = 1.25 ms, T_{mp} = Time required for single bilinear pairing multiplication = 4.31 ms, T_{ecmp} = Time required for single elliptic curve multiplication = 0.97, T_{hecmp} = Time required for single hyper elliptic curve multiplication = 0.48, and T_p = Time required for single bilinear pairing operations = 14.90.

Table 3. Computational cost comparisons in milliseconds.

Schemes	Sender Cost	Receiver Cost	Total Cost
Wu et al. [22]	$2 * 1.25 + 3 * 4.31 = 15.43$	$2 * 1.25 + 3 * 4.31 + 1 * 14.90 = 30.33$	45.76
He et al. [23]	$4 * 4.31 = 17.24$	$1 * 14.90 + 4 * 4.31 = 32.14$	49.38
Ji et al. [24]	$3 * 0.97 = 2.91$	$3 * 0.97 = 2.91$	5.82
Xie et al. [25]	$3 * 0.97 = 2.91$	$3 * 0.97 = 2.91$	5.82
Liao et al. [26]	$4 * 4.31 + 1.25 = 18.49$	$2 * 1.25 + 5 * 14.90 = 77$	$2 * 1.25 + 4 * 4.31 + 5 * 14.90 = 95.49$
Li et al. [27]	$3 * 0.97 = 2.91$	$4 * 0.97 = 3.88$	$7 * 0.97 = 6.79$
Proposed Scheme	$3 * 0.48 = 1.44$	$3 * 0.48 = 1.44$	2.88

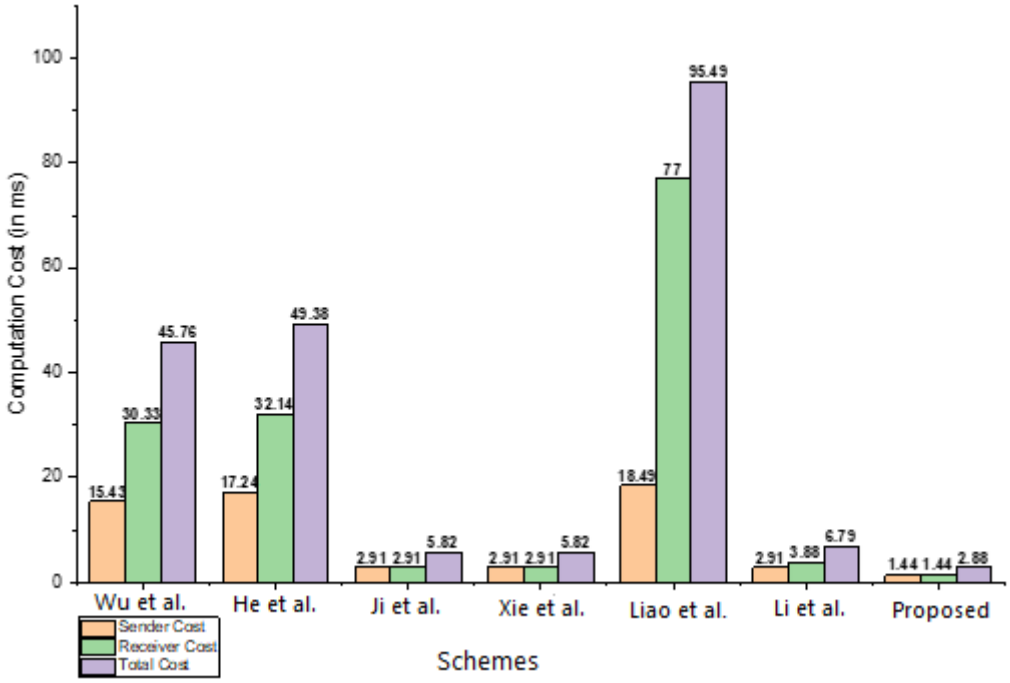

Figure 6. Computational cost comparison (in ms). Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27].

7.2. Communication Cost

The proposed scheme is compared to the relevant schemes published by Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27] in this section. The comparison is made in terms of the communication cost. The key findings from the communication cost comparison are summarized in Table 4. The results show that the proposed scheme is better in communication cost than the existing schemes, which is also illustrated in Figure 7 and clearly indicates that the proposed scheme is efficient from Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27].

Table 4. Communication cost comparisons.

Schemes	Sender Cost	Total Cost in Bits
Wu et al. [22]	$2b_C + 2b_G + 2b_T$	$2 * 1024 + 2 * 1024 + 2 * 34 = 4164$
He et al. [23]	$1b_C + 2b_G + 1b_T + 1b_h$	$1 * 1024 + 2 * 1024 + 1 * 34 + 1 * 256 = 3362$
Ji et al. [24]	$1b_C + 2b_q + 1b_T$	$1 * 1024 + 2 * 160 + 1 * 34 = 1378$
Xie et al. [25]	$1b_C + 4b_q + 2b_T$	$1 * 1024 + 4 * 160 + 2 * 34 = 1732$
Liao et al. [26]	$6b_G$	$6 * 1024 = 6144$
Li et al. [27]	$2b_C + 2b_q$	$2 * 1024 + 2 * 160 = 2368$
Proposed Scheme	$1b_C + 2b_h + 1b_h$	$1 * 1024 + 2 * 80 + 1 * 256 = 1440$

Note: b_C = bits required for ciphertext = 1024, b_G = bits required for bilinear parameter = 1024, b_T = bits required for timestamp = 34, b_q = bits required forelliptic curve parameter = 160, b_n = bits required for hyperelliptic curve parameter = 160, and b_h = bits required for hash value = 256.

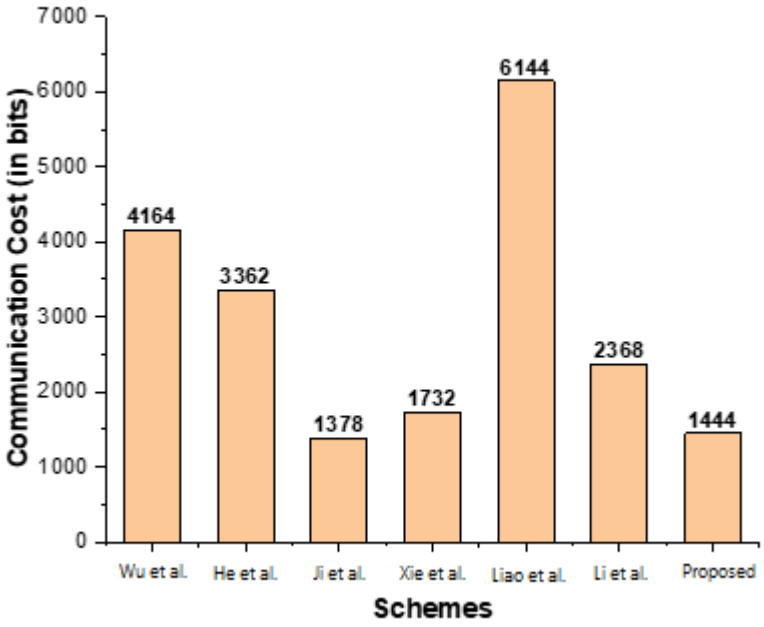

Figure 7. Communication cost comparison (in bits). Wu et al. [22], He et al. [23], Ji et al. [24], Xie et al. [25], Liao et al. [26], and Li et al. [27].

8. Conclusions

WBANs have recently received much attention as a result of recent technical developments in the fields of electronics, sensors, and wireless communication technologies, which allow patients to obtain preventative or proactive healthcare treatments from anywhere and at any time. Biomedical equipment, on the other hand, communicate regularly through an open wireless channel, making them vulnerable to a variety of cyber-attacks. In order to solve the security and privacy issues of WBAN, this article proposes an improved and efficient certificateless authentication scheme with a conditional privacy-preserving strategy. Hyperelliptic Curve Cryptography (HECC), a more sophisticated form of Elliptic Curve Cryptography, is used to build the proposed scheme (ECC). HECC offers the same degree of security while using a smaller key size, making it a more efficient solution than its alternatives. The proposed scheme, according to the comparative study, not only fulfills WBAN security and privacy criteria but also improves efficiency in terms of computation and communication costs.

In the future, we will propose a new heterogeneous authentication scheme in which the Key Generation Center can send the private key and partial private key through an open channel to the users without disclosing them to attackers.

Author Contributions: Conceptualization, I.U. and M.A.K.; Methodology, I.U., M.A.K., C.-M.C. and N.I.; Software, I.U., C.-M.C., M.A.K. and A.M.A.; Validation, A.M.A., F.N. and I.U.; Formal analysis, I.U. and M.A.K.; Investigation, I.U. and M.A.K.; Resources, F.N. and N.I., Data curation, M.A.K., I.U. and C.-M.C.; Writing—original draft preparation, A.M.A., I.U., M.A.K., F.N. and N.I.; Writing—review and editing, M.A.K., I.U. and C.-M.C.; Visualization, F.N.; Funds acquisitions, N.I.; Supervision, F.N. and M.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by AlMaarefa University, Riyadh, Saudi Arabia (TUMA-2021-57).

Data Availability Statement: Not applicable.

Acknowledgments: Nisreen Innab would like to express her gratitude to AlMaarefa University, Riyadh, Saudi Arabia, for providing funding (TUMA-2021-57) for this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Comert, C.; Kulhandjian, M.; Gul, O.M.; Touazi, A.; Ellement, C.; Kantarci, B.; D'Amours, C. Analysis of Augmentation Methods for RF Fingerprinting under Impaired Channels. In Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning (WiseML '22), San Antonio, TX, USA, 19 May 2022; pp. 3–8. [CrossRef]
2. Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Kumar, N.; Khan, M.A. An Anonymous Certificateless Signcryption Scheme for Internet of Health Things. *IEEE Access* **2021**, *9*, 101207–101216. [CrossRef]
3. Reus-Muns, G.; Jaisinghani, D.; Sankhe, K.; Chowdhury, K.R. Trust in 5G Open RANs through Machine Learning: RF Fingerprinting on the POWDER PAWR Platform. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
4. Yin, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
5. Khan, M.A.; Rehman, S.U.; Uddin, M.I.; Nisar, S.; Noor, F.; Alzahrani, A.; Ullah, I. An Online-Offline Certificateless Signature Scheme for Internet of Health Things. *J. Health Eng.* **2020**, *2020*, 6654063. [CrossRef]
6. Chen, C.M.; Chen, Z.; Kumari, S.; Lin, M.C. LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things. *Sensors* **2022**, *22*, 5401. [CrossRef]
7. Noor, F.; Kordy, T.A.; Alkhodre, A.B.; Benrhouma, O.; Nadeem, A.; Alzahrani, A. Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5986469. [CrossRef]
8. Lin, X.; Lu, R.; Shen, X.; Nemoto, Y.; Kato, N. Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems. *IEEE J. Sel. Areas Commun.* **2009**, *27*, 365–378. [CrossRef]
9. Chen, C.-M.; Li, Z.; Chaudhry, S.A.; Li, L. Attacks and Solutions for a Two-Factor Authentication Protocol for Wireless Body Area Networks. *Secur. Commun. Netw.* **2021**, *2021*, 3116593. [CrossRef]
10. Ullah, I.; Zeadally, S.; Amin, N.U.; Khan, M.A.; Khattak, H. Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN). *Microprocess. Microsyst.* **2021**, *81*, 103477. [CrossRef]
11. Chaudhry, S.A.; Irshad, A.; Yahya, K.; Kumar, N.; Alazab, M.; Bin Zikria, Y. Rotating behind Privacy: An Improved Lightweight Authentication Scheme for Cloud-based IoT Environment. *ACM Trans. Internet Technol.* **2021**, *21*, 78. [CrossRef]
12. Ali, Z.; Ghani, A.; Khan, I.; Chaudhry, S.A.; Islam, S.H.; Giri, D. A robust authentication and access control protocol for securing wireless healthcare sensor networks. *J. Inf. Secur. Appl.* **2020**, *52*, 102502. [CrossRef]
13. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 47–53. [CrossRef]
14. Kumar, P.; Kumari, S.; Sharma, V.; Sangaiah, A.K.; Wei, J.; Li, X. A certificateless aggregate signature scheme for healthcare wireless sensor network. *Sustain. Comput. Inform. Syst.* **2018**, *18*, 80–89. [CrossRef]
15. Kumar, P.; Kumari, S.; Sharma, V.; Li, X.; Sangaiah, A.K.; Islam, S.H. Secure CLS and CL-AS schemes designed for VANETs. *J. Supercomput.* **2018**, *75*, 3076–3098. [CrossRef]
16. Chen, C.-L.; Yang, T.-T.; Chiang, M.-L.; Shih, T.-F. A Privacy Authentication Scheme Based on Cloud for Medical Environment. *J. Med. Syst.* **2014**, *38*, 143. [CrossRef]
17. Chiou, S.-Y.; Ying, Z.; Liu, J. Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment. *J. Med. Syst.* **2016**, *40*, 101. [CrossRef] [PubMed]
18. Li, X.; Niu, J.; Karuppiah, M.; Kumari, S.; Wu, F. Secure and Efficient Two-Factor User Authentication Scheme with User Anonymity for Network Based E-Health Care Applications. *J. Med. Syst.* **2016**, *40*, 268. [CrossRef]
19. Debiao, H.; Jianhua, C.; Rui, Z. A More Secure Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* **2011**, *36*, 1989–1995. [CrossRef]
20. Wei, J.; Hu, X.; Liu, W. An Improved Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* **2012**, *36*, 3597–3604. [CrossRef]

21. Wu, F.; Li, X.; Sangaiah, A.K.; Xu, L.; Kumari, S.; Wu, L.; Shen, J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Gener. Comput. Syst.* **2018**, *82*, 727–737. [CrossRef]
22. Wu, L.; Zhang, Y.; Li, L.; Shen, J. Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks. *J. Med. Syst.* **2016**, *40*, 134. [CrossRef] [PubMed]
23. He, D.; Zeadally, S.; Kumar, N.; Lee, J.-H. Anonymous Authentication for Wireless Body Area Networks with Provable Security. *IEEE Syst. J.* **2017**, *11*, 2590–2601. [CrossRef]
24. Ji, S.; Gui, Z.; Zhou, T.; Yan, H.; Shen, J. An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services. *IEEE Access* **2018**, *6*, 69603–69611. [CrossRef]
25. Xie, Y.; Zhang, S.; Li, X.; Li, Y.; Chai, Y. *CasCP*: Efficient and Secure Certificateless Authentication Scheme for Wireless Body Area Networks with Conditional Privacy-Preserving. *Secur. Commun. Netw.* **2019**, *2019*, 5860286. [CrossRef]
26. Liao, Y.; Liu, Y.; Liang, Y.; Wu, Y.; Nie, X. Revisit of Certificateless Signature Scheme Used to Remote Authentication Schemes for Wireless Body Area Networks. *IEEE Internet Things J.* **2020**, *7*, 2160–2168. [CrossRef]
27. Li, C.; Xu, C. Efficient Anonymous Authentication for Wireless Body Area Networks. *IEEE Access* **2022**, *10*, 80015–80026. [CrossRef]
28. Bera, B.; Das, A.K.; Garg, S.; Piran, J.; Hossain, M.S. Access Control Protocol for Battlefield Surveillance in Drone-Assisted IoT Environment. *IEEE Internet Things J.* **2021**, *9*, 2708–2721. [CrossRef]
29. Shamus Sofware Ltd. Miracl Library. Available online: http://github.com/miracl/MIRACL (accessed on 21 August 2021).
30. Zhou, C.; Zhao, Z.; Zhou, W.; Mei, Y. Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings. *Secur. Commun. Netw.* **2017**, *2017*, 8405879. [CrossRef]
31. Khan, M.A.; Shah, H.; Rehman, S.U.; Kumar, N.; Ghazali, R.; Shehzad, D.; Ullah, I. Securing Internet of Drones With Identity-Based Proxy Signcryption. *IEEE Access* **2021**, *9*, 89133–89142. [CrossRef]
32. Khan, M.A.; Ullah, I.; Alsharif, M.H.; Alghtani, A.H.; Aly, A.A.; Chen, C.-M. An Efficient Certificate-Based Aggregate Signature Scheme for Internet of Drones. *Secur. Commun. Netw.* **2022**, *2022*, 9718580. [CrossRef]